RODO – GDPR

OCENA RYZYKA, OCENA SKUTKÓW NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Jakub Rzymowski

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

RODO – GDPR

OCENA RYZYKA, OCENA SKUTKÓW NARUSZENIA OCHRONY DANYCH OSOBOWYCH

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

RODO – GDPR

OCENA RYZYKA, OCENA SKUTKÓW NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Jakub Rzymowski

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO
Łódź 2023

Jakub Rzymowski (ORCID: 0000-0003-0538-8895) – Uniwersytet Łódzki
Wydział Prawa i Administracji, Katedra Europejskiego Prawa Gospodarczego
90-232 Łódź, ul. Kopcińskiego 8/12

RECENZENCI
Paweł Fajgielski, Adam Sulikowski

SKŁAD I ŁAMANIE
Jakub Rzymowski

PROJEKT OKŁADKI
Jakub Rzymowski, Monika Rawska

Wydrukowano z gotowych materiałów dostarczonych do Wydawnictwa UŁ

Wydane przez Wydawnictwo Uniwersytetu Łódzkiego
Wydanie I. W.10804.22.0.M

Ark. druk. 32,75

ISBN 978-83-8331-244-6
https://doi.org/10.18778/8331-244-6
Wydawnictwo Uniwersytetu Łódzkiego
90-237 Łódź, ul. Matejki 34A
www.wydawnictwo.uni.lodz.pl
e-mail: ksiegarnia@uni.lodz.pl
tel. 42 635 55 77

Spis treści

Wstęp

Wstęp

Wprowadzenie

Ciekawą myśl zawiera oxfordzki komentarz do RODO, a mianowicie, że nie należy zadawać pytania o to, czy administrator odnotuje naruszenie ochrony danych, ale należy pytać o to, kiedy będzie miało ono miejsce[1].

Ciekawą myśl wyraził również K. Wygoda, który stwierdza, że przed pojawieniem się RODO panowało *statyczne i formalne podejście do przetwarzania*, obecny zaś model jest proaktywny, prewencyjny, zindywidualizowany[2]. Model ten oparty na zindywidualizowanym podejściu do ryzyka naruszenia praw i wolności. Indywidualizacja jest wynikiem obowiązków: oceniania, szacowania, ustalania – nieważne, jakiej nazwy użyjemy – poziomu ryzyka u konkretnego administratora lub podmiotu przetwarzającego, w konkretnej sytuacji. Analogicznie wypowiada się P. Fajgielski, który stwierdza, że w przeciwieństwie do poprzedniej, szczegółowej, zawartej w ustawie i rozporządzeniu regulacji, na gruncie RODO *[...] wskazane są jedynie ogólne wymogi, w tym wymóg przeprowadzenia analizy ryzyka i doboru zabezpieczeń odpowiednich dla tego rodzaju ryzyka [...]*[3].

Uzupełnieniem tych myśli może być myśl D. Nowak, która pisze: *[...] wielkość organizacji nie determinuje poziomu wymaganej przez RODO zgodności*[4]. W tym samym duchu wypowiada się

---

[1] C. Burton, [w:] *The EU General Data Protection Regulation (GDPR). A Commentary.* Edited by Ch. Kuner, L.A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020, s. 631.

[2] K. Wygoda, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 354–355.

[3] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*. WKP 2018 – Komentarz. Kom. do art. 24.

[4] D. Nowak, *Podejście oparte na ryzyku w RODO w praktyce – wnioski po dwóch latach stosowania RODO*, [w:] *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*. pod. red. G. Sibigi. Dodatek specjalny do „Monitora Prawniczego" 2020, nr 23, s. 35.

Ch. Poszwiński, który pisze, że *Każdy podmiot […] niezależnie od tego, czy jest podmiotem prywatnym czy publicznym, powinien przeanalizować i oszacować ryzyko związane z przetwarzaniem danych osobowych*[5].

Są – najogólniej patrząc – dwie kategorie sytuacji, dwa rodzaje sytuacji, w których przedmiotem ustaleń jest ryzyko związane z przetwarzaniem danych osobowych.

– **Pierwsza** – ocena ryzyka przetwarzania przed przystąpieniem do przetwarzania, uzupełniana następnie oceną powtarzaną w sposób zależny od różnych kryteriów.
– **Druga** – ocena skutków naruszenia. Sytuacje z jednej, jak i z drugiej grupy mają związek z bezpieczeństwem danych osobowych.
– Uzupełniając **sytuację pierwszą**, mamy wtedy do czynienia z bezpieczeństwem ocenianym niejako z góry, ze świadomością możliwości naruszenia tegoż bezpieczeństwa i będącym skutkiem tej świadomości ocenianiem ryzyka i dostosowywaniem doń środków technicznych i organizacyjnych, które to środki mają na celu ochronę danych osobowych.
– Uzupełniając **sytuację drugą**, mamy wtedy do czynienia z bezpieczeństwem, a właściwie jego naruszeniem ocenianym niejako z dołu, po zdarzeniu, którego skutki administrator musi ocenić przez pryzmat zagrożenia dla praw i wolności osoby, której dane dotyczą i której dane przetwarza.

Niniejsza publikacja poświęcona jest bezpieczeństwu na gruncie RODO. Zagadnienia związane z bezpieczeństwem na gruncie RODO podzielić można na **trzy grupy**.

Pierwsza grupa zagadnień to zagadnienia związane z zapewnieniem bezpieczeństwa.

Druga grupa zagadnień to zagadnienia związane z działaniami, jakie powinny zostać podjęte przez administratora w sytuacji zaistnienia zjawisk, które godzą w bezpieczeństwo danych.

[5] Ch. Poszwiński, *Podejście oparte na ryzyku w procesie przetwarzania danych osobowych,* Wrocław 2021, s. 18.

Trzecia grupa to zagadnienia organizacyjne i związane z nimi zagadnienia dotyczące dokumentacji. Organizacja i dokumentowanie ochrony danych, czyli właśnie zagadnienia ze wskazanej tu grupy trzeciej, są ściśle związane z zagadnieniami grupy pierwszej, nie mogą być jednak – jak uważam – z nimi mylone.

Niniejsza książka poświęcona jest analizie podstawowych elementów modelu ochrony danych osobowych i ochrony praw i wolności osób, których dane dotyczą, który to model wynika z RODO. Już na wstępnym etapie rozważań zwracam uwagę na fakt, że konieczne jest odróżnienie ochrony danych osobowych od ochrony praw i wolności osób, których dane dotyczą. Ochrona danych osobowych to jedno, ochrona praw i wolności to drugie.

Administrator (danych osobowych) ma obowiązek chronić dane osobowe przed naruszeniem ochrony danych osobowych. Naruszenie ochrony danych osobowych zdefiniowane jest w art. 4 pkt 12 RODO.

Jeżeli naruszenie zaistnieje, to administrator ma obowiązek dokonać pewnej oceny, a to oceny skutków naruszenia i stosownie do jej wyników poinformować o naruszeniu PUODO[6] albo PUODO i osoby, których dane dotyczą, albo nikogo.

Jeżeli naruszenie zaistnieje, to administrator ma obowiązek dokonać oceny tego naruszenia. Administrator musi ocenić poziom ryzyka naruszenia praw i wolności osób, których dane dotyczą. Jeżeli poziom ryzyka naruszenia praw i wolności nie jest niski (powiedzmy, jest podstawowy) to administrator ma obowiązek poinformować PUODO. Jeżeli poziom ryzyka jest wysoki, to administrator ma obowiązek poinformować osoby, których dane dotyczą. Jednocześnie, jeżeli poziom ryzyka jest wysoki, to oczywiste jest, że nie jest on niski, a jedynie niski poziom ryzyka zwalnia z informowania PUODO. W takim razie, jeżeli poziom ryzyka jest wysoki, to administrator ma obowiązek poinformować również PUODO. Jeżeli poziom ryzyka jest niski, to administrator nie ma obowiązku informować kogokolwiek.

[6] PUODO – Prezes Urzędu Ochrony Danych Osobowych.

Zagadnienia związane z zapewnieniem bezpieczeństwa

Pierwsza grupa zagadnień, są to – jak piszę wyżej – zagadnienia związane z zapewnieniem bezpieczeństwa. Obowiązek ochrony danych osobowych administrator jest zobowiązany realizować w opisany poniżej sposób.

Najpierw administrator sporządza rejestr czynności przetwarzania danych osobowych, za które odpowiada. Z art. 30 ust. 5 RODO wynika, że nie każdy administrator ma obowiązek sporządzać rejestr czynności przetwarzania, jednak jeżeli administrator nie sporządzi takiego rejestru, to administrator taki będzie miał ogromny problem z przeprowadzeniem oceny ryzyka lub oceny skutków[7].

Następnie administrator dokonuje oceny ryzyka, jakie wiąże się z poszczególnymi czynnościami.

Ocena ryzyka powinna składać się z dwóch elementów, czyli dwóch ocen składowych.

Element 1 – ocena stopnia bezpieczeństwa (ocena, czy stopień bezpieczeństwa jest odpowiedni, ocena odpowiedniości stopnia bezpieczeństwa). (Art. 32 ust. 2 RODO)

Element 2 – ocena ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. (Art. 32 ust. 1 RODO)

Następnie administrator (danych osobowych) wdraża odpowiednie środki techniczne i organizacyjne. Celem wdrożenia tych środków jest zapewnienie stopnia bezpieczeństwa odpowiadającego ryzyku, którego poziom administrator (danych osobowych) ustalił w ocenie ryzyka. (Art. 32 ust. 1 RODO)

Następnie administrator opisuje wdrożone środki techniczne i organizacyjne w dokumencie noszącym tytuł: „ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO".

Następnie administrator poddaje środki techniczne i organizacyjne przeglądom i je uaktualnia.

Przepis RODO stanowi, że środki techniczne i organizacyjne *[...] są w razie potrzeby poddawane przeglądom i uaktualniane* (art. 24 ust. 1 RODO). Zwracam tu uwagę, że środki techniczne i organiza-

[7] Podobnie: E. Bielak-Jomaa, D. Lubasz, [w:] D. Lubasz red. n., *Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych*, Warszawa 2022, s. 45.

cyjne mają być poddawane przeglądom i uaktualnianiu „w razie potrzeby". Wspomnianą tu potrzebę można rozumieć dwojako.

Rozumienie pierwsze

Potrzeba uaktualnienia środków pojawia się, jeżeli pojawia się nowa czynność. Jeżeli pojawia się nowa czynność, to administrator powinien dokonać oceny ryzyka, ponieważ w poprzedniej, dokonanej przez niego ocenie ryzyku dana czynność nie była brana pod uwagę. Administrator dokonuje oceny ryzyka, a następnie – zależnie od wyników tej oceny – poddaje przeglądom, a zwłaszcza aktualizuje: środki techniczne i organizacyjne i oczywiście ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Rozumienie drugie

Potrzeba uaktualnienia środków pojawia się z czasem, bez pojawienia się nowej czynności. Czas płynie, zmieniają się realia technicznego otoczenia, w związku z tym może również ulec zmianie poziom ryzyka. W związku z tym administrator (danych osobowych) co jakiś czas dokonuje kolejnej oceny ryzyka, a potem kolejnej i kolejnej. Administrator może oceny prowadzić w układzie periodycznym (na przykład co pół roku, co rok, co dwa lata) lub w układzie ciągłym (kończy się ocena ryzyka ostatniej czynności z rejestru czynności przetwarzania danych osobowych, więc administrator przystępuje do oceny ryzyka pierwszej czynności, potem drugiej i tak do ostatniej i znowu).

Ocena skutków

Jeśli chodzi o ocenę ryzyka nowej planowanej czynności, to w RODO zawarto jeszcze jedno rozwiązanie dotyczące takiej oceny. Ocena taka nosi nazwę oceny skutków dla ochrony danych. W rzeczywistości taką ocenę należy wykonywać, jeżeli dana czynność została wskazana przez PUODO w Komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony[8]. Do takiego jednak wniosku droga jest długa i nieprosta.

Z art. 35 ust, 1 RODO wynika, że taka ocena powinna być wykonywana, jeżeli dana czynność może powodować wysokie ryzyko

[8] M.P. 2019 poz. 666. (Dalej: Komunikat PUODO)

naruszenia praw lub wolności osób fizycznych. Innymi słowy, jeżeli czynność może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to administrator ma obowiązek wykonać ocenę skutków dla ochrony danych.

Należy jednak zwrócić uwagę, że o tym, czy czynność może powodować wysokie ryzyko czy nie, można orzec dopiero po dokonaniu oceny tego ryzyka, tu nazwanej oceną skutków dla ochrony danych. Z tego wynika, że trzeba wykonać ocenę ryzyka, aby ustalić poziom tego ryzyka, aby w zależności od tego poziomu, dokonać oceny skutków dla ochrony danych. Ocena skutków dla ochrony danych składa się z dwóch elementów:
– oceny ryzyka i
– elementów dodatkowych.

Kiedy sobie to uświadomimy, to okazuje się, że administrator dokonuje oceny ryzyka po to, aby ustalić, czy ma obowiązek dokonać oceny ryzyka wzbogaconej o elementy dodatkowe. Nie ma podstaw, by sądzić, że wskazane tu dwie kolejne, następujące po sobie oceny ryzyka różnią się od siebie czymkolwiek prócz elementów dodatkowych, których obecność przekształca ocenę ryzyka w ocenę skutków. Wykonywanie dwóch ocen ryzyka, jednej tuż po drugiej jest absurdalne i jako takie powinno być odrzucone. Należy zatem przyjąć, że jeżeli administrator przewiduje, że będzie wykonywał nową czynność, to administrator powinien wykonać ocenę ryzyka. Jeżeli z tej oceny ryzyka będzie wynikało, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to powinien on przeprowadzić elementy dodatkowe, które różnią ocenę ryzyka od oceny skutków, a następnie powinien skonsultować się z PUODO, co wynika z art. 36 ust. 1 RODO.

Jednocześnie należy pamiętać, że administrator ma obowiązek wykonać ocenę skutków, jeżeli planowana przez niego czynność została ujęta przez PUODO w dokumencie, który na gruncie RODO nosi tytuł: „wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust. 1", a który w Polsce nosi tytuł: wskazany wyżej. Wynika to z art. 35 ust. 4 RODO.

Jak zatem widać, artykuł 35 ust. 4 RODO niejako odwraca sytuację. Ze względu na treść art. 35 ust 4 RODO, opisane powyżej na-

stępstwo czynności administratora związanych z ryzykiem, jakim może skutkować nowa czynność, wygląda jak poniżej.

– Najpierw administrator ustala, że będzie wykonywał nową czynność na danych osobowych.
– Następnie administrator sprawdza, czy czynność ta znajduje się w Komunikacie PUODO.
– Jeżeli czynność została wymieniona w Komunikacie PUODO, to administrator wykonuje ocenę skutków dla ochrony danych, czyli ocenę ryzyka wzbogaconą o elementy dodatkowe.
– Następnie, jeżeli z oceny skutków wynika, że przetwarzanie powodowałoby wysokie ryzyko, to administrator konsultuje się z organem nadzorczym

Nie wolno zapominać o sytuacji, w której administrator

– ustala, że będzie wykonywał nową czynność na danych osobowych, następnie administrator:
– sprawdza czy czynność ta została wymieniona w komunikacie
– i ustala, że czynność nie została tam wymieniona.

Jeżeli czynność nie została wymieniona w Komunikacie PUODO, to administrator nie wykonuje oceny skutków, jednak nadal jest to nowa czynność. Jest to czynność, wobec której administrator nie wykonał oceny ryzyka, ponieważ jest to czynność nowa i po prostu nie miał ku temu okazji, kiedy ostatnio ocenę ryzyka wykonywał. W takiej sytuacji administrator, który nie wykonuje oceny skutków, powinien po prostu wykonać ocenę ryzyka i dopiero po jej wykonaniu, przystąpić do czynności, uprzednio dostosowawszy środki techniczne i organizacyjne do ryzyka spowodowanego nową, właśnie ocenioną czynnością.

Analiza przepisów nakazuje sądzić – na co wskazałem wyżej – że istotnym elementem oceny skutków jest ocena ryzyka. Nie ma powodu, by administrator wykonywał ocenę ryzyka, która jest częścią oceny skutków, inaczej niż wykonuje on ocenę ryzyka, o której mowa w art. 32 ust. 1 RODO.

Zagadnienia związane z działaniami, jakie powinny zostać podjęte przez administratora w sytuacji zaistnienia zjawisk, które godzą w bezpieczeństwo danych

Druga grupa zagadnień to zagadnienia związane z działaniami, jakie powinny zostać podjęte przez administratora w sytuacji zaistnienia zjawisk, które godzą w bezpieczeństwo danych. Działania te wynikają z art. 33 RODO i z art. 34 RODO.

Obydwa wskazane przepisy dotyczą sytuacji, w której zachodzi zjawisko o nazwie „naruszenie ochrony danych osobowych".

Naruszenie ochrony danych osobowych zdefiniowane jest w art. 4 pkt 12 RODO. Omawiam je w niniejszej książce w podrozdziale (*1. Art. 33 ust. 1. Analiza*), więc poniżej prezentuję rzecz jedynie skrótowo.

– Zachodzi zdarzenie, które może być naruszeniem.
– Administrator (danych osobowych) ocenia, czy zdarzenie jest naruszeniem ochrony danych osobowych.
– Jeżeli zdarzenie jest naruszeniem ochrony danych osobowych, to administrator (danych osobowych) przystępuje do oceny ryzyka naruszenia praw i (sic!) wolności osób fizycznych.
– Jeżeli ryzyko naruszenia praw i wolności osób fizycznych jest niskie, to administrator (danych osobowych) nikogo nie informuje o naruszeniu ochrony danych.
– Jeżeli ryzyko naruszenia praw i wolności osób fizycznych nie jest niskie i nie jest wysokie, to administrator zgłasza naruszenie organowi nadzorczemu – PUODO. (Art. 33 ust. 1 RODO). Ryzyko, które nie jest niskie i nie jest wysokie i do którego odnosi się art. 33 RODO, nie posiada na gruncie RODO odpowiedniej dla niego nazwy. Podkreślam, że ryzyko, o którym tu mowa, jest ryzykiem, którego poziom mieści się między ryzykiem o niskim poziomie i ryzykiem o wysokim poziomie i jednocześnie nie przyjmuje poziomu niskiego ani poziomu wysokiego. Jednocześnie ryzyko to nie jest niższe niż niskie i jest wyższe niż niskie i nie jest wyższe niż wysokie i jest niższe niż wysokie. Jest to ryzyko, jakie najlepiej chyba określa nazwa: „ryzyko podstawowe". Nazwa nie jest tu istotna, jednak warto się jakąś posługiwać, pozwala to bowiem na uniknięcie opisowego charakteryzowania tego poziomu ryzyka.
– Jeżeli ryzyko naruszenia praw i wolności osób fizycznych jest lub może być wysokie, to administrator zawiadamia osobę, której dane

dotyczą o naruszeniu ochrony danych. Jednocześnie administrator zgłasza naruszenie organowi nadzorczemu, a czyni tak, ponieważ jeżeli ryzyko jest lub może być wysokie, to nie jest ono niskie, a jedynie niskie ryzyko zwalnia administratora ze zgłoszenia naruszenia organowi nadzorczemu.

Zagadnienia organizacyjne i związane z nimi zagadnienia dotyczące dokumentacji

Organizacja i dokumentowanie ochrony danych osobowych są ściśle związane z zagadnieniami grupy pierwszej, nie mogą być jednak – jak uważam – z nimi mylone.

Zasygnalizowane powyżej zjawiska pociągają za sobą konieczność wdrożenia przez administratora pewnych rozwiązań organizacyjnych oraz stworzenia i przechowywania przez administratora związanej z realizacją przepisów dokumentacji. Ogólny obowiązek dokumentowania realizacji wszelkich realizowanych obowiązków, który spoczywa na administratorze, wynika z art. 5 ust. 2 RODO, a dokładniej, z zawartej w tym przepisie zasady rozliczalności. Szerzej piszę o tym w książce[9] poświęconej m.in. zasadom w RODO oraz w książce poświęconej dokumentacji przygotowywanej na gruncie RODO[10], więc poniżej jedynie skrótowo.

– Administrator (danych osobowych) powinien wytworzyć i przechowywać dokument o nazwie „rejestr czynności przetwarzania danych osobowych" (art. 30 ust. 1 RODO). Jeżeli administrator (danych osobowych) nie ma obowiązku tworzenia takiego rejestru, to i tak powinien zestawić wykonywane czynności tak, by móc to zestawienie wykorzystać przy okazji wykonywania oceny ryzyka. Tworzenie rejestru opisuję w innej książce[11], wydanej nieco wcześniej. W RODO nie znajdziemy nic o wspomnianym tu przeze mnie zestawieniu wykonywanych czynności, jeżeli jednak administrator,

[9] J. Rzymowski, *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*, Łódź 2020, s. 303–317.

[10] J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*, Kraków 2019, s. 9–10.

[11] Ibidem, s. 31–56.

który nie robi rejestru, nie wykona również takiego zestawienia, to tym samym wykonanie u takiego administratora oceny ryzyka, oceny skutków, ewentualnej oceny ryzyka nowej czynności, w sytuacji, kiedy nie jest wykonywana ocena skutków, może być bardzo trudne. Nie jest niemożliwe, ale staje się trudne.

– Administrator (danych osobowych) powinien wytworzyć i przechowywać dokument oceny stopnia bezpieczeństwa przetwarzania danych osobowych (art. 32 ust. 2 RODO). Ocena stopnia bezpieczeństwa przetwarzania danych osobowych jest konieczna do wykonania przed wykonaniem oceny ryzyka naruszenia praw i wolności osób fizycznych.
– Administrator (danych osobowych) powinien wytworzyć i przechowywać dokument oceny ryzyka naruszenia praw i wolności (art. 32 ust. 1 RODO).
– Administrator (danych osobowych) powinien wytworzyć i przechowywać ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 30 ust. 1 lit. g RODO).
– Jeżeli ma miejsce naruszenie ochrony danych osobowych zdefiniowane w art. 4 pkt 12 RODO, to administrator (danych osobowych) powinien wytworzyć i przechowywać dokument, z którego wynika, że administrator dokonał oceny ryzyka naruszenia praw i wolności. Od poziomu tego ryzyka uzależnione jest, czy administrator zgłasza naruszenie organowi nadzorczemu, czy nie oraz czy informuje o naruszeniu osoby, których dane dotyczą. I podobnie jak w rozważaniu powyżej – udokumentowanie dokonania oceny jest potrzebne po to, by móc skontrolować, czy administrator wykonał obowiązki odpowiednio do poziomu ryzyka.
– Administrator (danych osobowych) powinien wytworzyć i przechowywać dokument, z którego wynika, kiedy stwierdzono naruszenie. Obowiązek ten wynika z art. 33 ust. 1 RODO. Z przepisu tego wynika, że administrator powinien zgłosić naruszenie organowi nadzorczemu *w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia*. Utrwalenie momentu stwierdzenia naruszenia jest konieczne, by administrator, jak również ewentualnie kontroler, mogli stwierdzić, czy obowiązek zgłoszenia został zrealizowany we wskazanym w przepisie terminie. Konieczność udokumentowania naruszenia wynika również z art. 33 ust. 5 RODO, z którego

wynika obowiązek dokumentowania naruszeń, niezależnie od poziomu ryzyka naruszenia praw i wolności wynikającego z tych naruszeń.
– Jeżeli miało miejsce naruszenie ochrony danych osobowych, to niezależnie od tego, czy administrator (danych osobowych) zgłasza naruszenie organowi nadzorczemu i niezależnie od tego, czy administrator ten informuje o naruszeniu osoby, których dane dotyczą, administrator tworzy i przechowuje dokumenty, dzięki którym realizuje on wymienione poniżej obowiązki dokumentacyjne. Administrator czyni to, mając na uwadze fakt, że stworzona tak dokumentacja musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania art. 33 RODO.

Administrator (danych osobowych) dokumentuje:
– naruszenia ochrony danych osobowych,
– okoliczności naruszenia ochrony danych osobowych,
– skutki naruszenia ochrony danych osobowych,
– działania zaradcze podjęte w związku z naruszeniem ochrony danych osobowych.

Wskazane powyżej dokumenty to nie wszystkie dokumenty, jakie należy przygotować na gruncie RODO, zwłaszcza w kontekście realizacji zasady rozliczalności, jednak są to podstawowe dokumenty, jakie należy przygotować w związku z oceną ryzyka, która modelowo powinna być prowadzona przed przystąpieniem do przetwarzania danych osobowych i w związku z oceną skutków naruszenia, która – co oczywiste – powinna być wykonywana po zaistnieniu naruszenia.

Metodologia

Praca, na poziomie analizy przepisów, pisana jest z wykorzystaniem metody logiczno-językowej. Opierając się na tej metodzie, stworzyłem własną technikę analizy przepisów, czyli etapową analizę semantyczną i tej właśnie techniki używam konsekwentnie do analizy kolejnych przepisów. Metodę opisuję niżej, ale przede wszystkim zwracam uwagę, że jest to swojego rodzaju mikroanaliza. Analizuję przepis przez drobiazgową analizę jego fragmentów. Do instytucji, koncepcji zawartych w przepisach na poziomie ogólniejszym, odnoszę się również na poziomie ogólniejszym w podrozdziałach warstwy „Uwagi".

Etapowa analiza semantyczna przebiega w sposób opisany poniżej.

1. Najpierw wybieram fragment aktu prawnego, który ma być analizowany, przepis. Z wykorzystaniem tej metody można analizować zarówno przepisy krótkie, składające się z kilkunastu wyrazów, jak i przepisy długie.
2. Następnie, używając programu do edycji tekstu (np. MS WORD), kopiuję przepis do pamięci komputera, po czym kilkanaście – powiedzmy dwadzieścia razy – wklejam go w pionie, jeden pod drugim.
3. Następnie w kolejnych kopiach przepisu oznaczam kolejne fragmenty przepisu, które chcę przeanalizować. Staram się, by fragmenty te były możliwie małe, zwykle są to złożenia składające się z kilku słów, wyrażenia frazeologiczne. Czasem są to osobne słowa, zwłaszcza kiedy są to funktory logiczne. Na tym etapie istotne jest, aby w sumie zaznaczone zostały wszystkie słowa przepisu. W analizie pomaga – jeżeli kolejne etapy zaznaczeń się zazębiają – czyli żeby na przykład jedno słowo z jednego zaznaczenia było zaznaczone również w drugim zaznaczeniu.
4. Następnie dokonuję analizy kolejnych zaznaczonych fragmentów. Na tym etapie ważne jest, by nie przeanalizować więcej, niż jest zaznaczone. Pozornie nie ma w tym niczego właściwego, skoro i tak każde słowo przepisu ma być przeanalizowane. Pozornie. Jeśli bowiem zaczniemy analizować większe niż tylko zaznaczone fragmenty przepisu, to tracimy etapowość analizy, a z nią jej dokładność i pewność, że żaden fragment przepisu nie zostanie pominięty w analizie.
5. Następnie kopiuję do pamięci komputera wszystko, co dotychczas napisałem, a to wielokrotnie skopiowany i wklejony tekst przepisu oraz powiązane z nim analizy i wklejam tak, by mieć dwie jednobrzmiące wersje. W ten sposób otrzymuję dwa jednobrzmiące bloki, nazwijmy je blokiem roboczym i blokiem podsumowującym.
6. Z bloku podsumowującego usuwam powtarzający się tekst przepisu (i ewentualnie element wprowadzający i wyprowadzający), tak by pozostały jedynie analizy kolejnych fragmentów przepisu.
7. Blok roboczy pozostawiam jako substrat do dalszych prac, takich jak dyskusja z przedstawicielami doktryny, postulaty nowelizacyjne itd.

Zwracam tu uwagę, że etapowa analiza semantyczna idealnie wpisuję się w warstwową metodę pisania pracy, o której to metodzie piszę niżej. Zastosowanie etapowej analizy semantycznej w opisany

wyżej sposób, daje dwie podstawowe warstwy, czy też kategorie (pod)rozdziałów, do których można następnie nawiązywać w podrozdziałach kolejnych warstw.

Powyżej opisałem podstawowe czynności, które składają się na etapową analizę semantyczną. Niżej czynności dodatkowe i ewentualne uzupełnienia. Przyjąłem taki sposób wywodu, by czytelnik łatwo mógł zrozumieć istotę mojej metody czy techniki.

Odnośnie do 1. Lepiej pracuje mi się nad małymi fragmentami tekstu. Jeżeli artykuł dzielony jest na ustępy i punkty, to najlepiej, a na pewno najwygodniej, przeanalizować część wprowadzającą przepisu, po czym każdy z ustępów osobno.

Odnośnie do 2. Dobrze jest skopiować przepis z pewnym naddatkiem, powiedzmy dwadzieścia razy, wtedy nie trzeba przerywać pracy przy oznaczaniu kolejnych fragmentów przepisu, gdyby zabrakło wklejonych fragmentów. Przerwy takie – przynajmniej piszącemu te słowa – utrudniają płynne myślenie, trzeba niejako wracać do początku z procesem myślowym poświęconym danemu fragmentowi, co nie jest problemem, ale niepotrzebnie czas zabiera.

Stosuję tu również czasem metodę, zgodnie z którą przed tekstem przepisu wpisuję tekst wprowadzający (np. „Ze słów pogrubionych/wytłuszczonych/zaznaczonych itp. w przepisie"), potem następuje tekst przepisu i następnie wpisuję tekst wyprowadzający („wynika, że/wnosimy, że" itp.) i dalej prowadzę odpowiednią analizę. Dla zachowania jednolitości z poprzednimi książkami, w tej i prawdopodobnie w następnej książce stosuję metodę ze wskazanymi dwoma tekstami. Jednocześnie rozważam, dla potrzeb kolejnych projektów, rezygnację z tekstu wprowadzającego i tekstu wyprowadzającego po to, by jeszcze bardziej uprościć metodę.

Odnośnie do 3. Zaznaczenia najwygodniej jest robić czcionką pogrubioną/wytłuszczoną. Podkreślenie jest zbyt mało widoczne. Kursywa może zostać pomylona z kursywą użytą w innym celu. Pozornie wygodne wydaje się użycie kolorowej czcionki lub podświetlenia. Niestety, metody te są niepraktyczne, ponieważ w momencie wydruku tekstu czy to na lokalnej drukarce, czy to w drukarni, zwykle stosujemy druk czarno-biały, z elementami szarości. Jasne czcionki stają się nieczytelne, szarość unifikuje podświetlenia, niektóre kolory podświetleń nałożone na czcionki utrudniają ich odczytanie. Generalnie należy tego unikać.

Odnośnie do 4. Punkty 3 i 4 są jądrem metody. Ważne, by ostrożnie, bez pomijania czegokolwiek, zaznaczyć wszystkie fragmenty przepisu i równie ważne, by następnie omówić przepis w zakresie zaznaczenia. Na tym etapie – właśnie na etapie omawiania zaznaczeń – pojawia się czasem potrzeba korekty zaznaczeń, kiedy okazuje się, że zaznaczono niewłaściwie.

Odnośnie do 5. Blok podsumowujący może zostać umieszczony po bloku roboczym, wtedy blok podsumowujący ma charakter wniosków z analizy prowadzonej w bloku roboczym. Blok podsumowujący może zostać umieszczony przed blokiem roboczym, wtedy blok podsumowujący ma charakter krótkiego analitycznego komentarza do przepisu, a blok roboczy nabiera charakteru uzasadnienia do tego komentarza. W poprzednich dwóch książkach stosuję kolejność: blok podsumowujący – blok roboczy. W niniejszej książce wskutek sugestii jednego z recenzentów stosuję kolejność: blok roboczy – blok podsumowujący. Merytorycznie różnica jest żadna. Wskazane wyżej różnice to raczej kwestia subiektywnego odbioru, rozważania w blokach prowadzone są, jakie są, kolejność ich nie zmienia.

Na poziomie prowadzenia wywodu praca oparta jest na drobiazgowej, opisanej wyżej analizie przepisu. Wszelkie dalsze rozważania mają u początku ustalenia analityczne, dotyczące konkretnych fragmentów konkretnych przepisów. Wywód prowadzony jest w sposób, który nazywam warstwowym. Istotę podziału warstwowego wyjaśniam niżej w pozycji *Konstrukcja pracy*. Tu zwracam jedynie uwagę, że poszczególne warstwy czy też kategorie podrozdziałów różnią się przedmiotem rozważań.

Podział na warstwy zabezpiecza czytelników przed pomyleniem rozważań analitycznych (Analiza, Wnioski z analizy) z rozważaniami o szerszym kontekście (Uwagi). Rozważania z warstw analitycznych są w swoim rodzaju przezroczyste poglądowo. Staram się nie obciążać ich wiedzą o przedmiocie rozważań, podchodzę tam do przepisów, jakimi są. Wiedzę o przedmiocie rozważań staram się wykorzystywać dopiero w warstwie kolejnej (Uwagi).

W kolejnej warstwie czynię lekki skręt w kierunku teorii prawa, zamykam podstawową treść przepisów w ramy zbudowane z praw i obowiązków. Praw osoby, której dane dotyczą i obowiązków ad-

ministratora. Jest to istotne dla wymowy książki, podkreślam bowiem w ten sposób, że w przepisach składających się na RODO są zapisane właśnie prawa i właśnie obowiązki. Dziękuję z tego miejsca Profesorowi Pawłowi Fajgielskiemu, który poświęcił czas na zrecenzowanie niniejszej książki i zgłosił zastrzeżenia do tej koncepcji. Wskutek zastrzeżeń Pana Profesora, zawarłem dodatkowe odniesienia do książki prof. Zygmunta Ziembińskiego. Nie mniej dziękuję drugiemu recenzentowi, Profesorowi Adamowi Sulikowskiemu za zwrócenie mojej uwagi na teorię Wesleya Newcomba Hohfelda.

W kolejnej warstwie zajmuję się zjawiskiem konkretyzacji zasad. Oddzieliłem tę sferę od pozostałych podrozdziałów, by w przeznaczonym temu miejscu skupić się na jednym tylko zjawisku.

Oddzielenie postulatów *de lege ferenda* ma na celu oczywiście nie tylko postawienie tychże, ale też zadbanie o to, by myśli zawarte w postulatach czy do nich wiodące, nie były pomylone z myślami dotyczącymi prawa istniejącego.

Konstrukcja pracy

Konstrukcja niniejszej pracy może być rozpatrywana w dwóch płaszczyznach:
– pierwsza to konstrukcja pracy rozumianej jako całość,
– druga to konstrukcja każdego z rozdziałów pracy.

Konstrukcja pracy rozumianej jako całość

Praca składa się z czterech rozdziałów oraz części dodatkowych, które znajdują się na początku i końcu pracy. Na początku pracy znajduje się *Wstęp*, następna jest część *Konstrukcja pracy*, potem *Cele pracy*. Następnie umieszczone są kolejne rozdziały pracy, kolejno: *Rozdział 1. Ocena ryzyka na gruncie art. 24 RODO*, *Rozdział 2. Ocena ryzyka na gruncie art. 32 RODO*, *Rozdział 3. Naruszenie ochrony danych osobowych i jego zgłaszanie na gruncie art. 33 RODO i art. 34 RODO*. Na końcu pracy znajduje się część: *Tabele pomocnicze. Zestawienia*, dalej znajduje się *Realizacja celów pracy*, wreszcie *Zakończenie*, *Wykaz skrótów*, *Akty prawne. Zestawienie*.

Konstrukcja każdego z rozdziałów pracy

Konstrukcja każdego z rozdziałów pracy oparta jest na pewnym pomyśle. Pomysłem tym jest warstwowa metoda wywodu. Każda warstwa, czyli kategoria podrozdziałów, co niżej jest w szczegółach opisane, poświęcona jest rozważaniom innego rodzaju. Zgadzam się z J. Janowskim, że *Niełatwą jest rzeczą łączenie odległych metodologicznie i mentalnie kompetencji […]*[12], nadawszy jednak pracy metodę warstwową, staram się to czynić i połączenia tego dokonywać.

Rozdziały składają się z podrozdziałów. Podrozdziały te noszą nazwę warstw. Warstw jest siedem.

Niniejsza książka jest czwartym dziełem z cyklu, a trzecim dziełem o budowie, przynajmniej częściowo, warstwowej. Z tego względu – jako ukłon w stronę czytelników – zachowuję w niniejszej książce taki sam układ warstw, jak w książkach poprzedzających.

[12] J. Janowski, *Informatyka prawa*, Lublin 2011, s. 11.

Poniżej wymieniam poszczególne warstwy.

– pierwsza – *Analiza,*
– druga – *Wnioski z analizy,*
– trzecia – *Uwagi,*
– czwarta – *Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa,*
– piąta – *Konkretyzacja zasad,*
– szósta – *Postulaty „de lege ferenda”,*
– siódma – *Rozważania historyczne.*

W warstwie trzeciej, w odniesieniu do analizowanych przepisów wprowadzam dodatkowy stały element, czyli **ocenę realizacji celów pracy w zakresie analizy oceny ryzyka i zjawisk pochodnych**.

Warstwa pierwsza – ***Analiza***

Jak piszę wyżej, prace nad przepisem zaczynam od jego drobiazgowej analizy. Zapis tej analizy znajduje się w podrozdziałach warstwy „Analiza”. Warstwa ta powstaje jako pierwsza. Od jej napisania zaczynam pracę nad każdym rozdziałem. Analizę prowadzę z wykorzystaniem własnej metody wykładni, czyli etapowej analizy semantycznej. Jednym z celów pracy jest – o czym piszę niżej – prezentacja etapowej analizy semantycznej, poprzez prezentację możliwości, jakie ona daje.

Warstwa pierwsza zawiera dłuższą i dokładniejszą wersję rozważań, umieszczonych w warstwie drugiej.

Szczegółowa analiza kolejnych przepisów RODO powinna – tak przynajmniej uważam – pozwolić na ich właściwe stosowanie. Uważam tak, ponieważ mam wrażenie, że trudności w stosowaniu przepisów RODO oraz niewłaściwe ich stosowanie wynikają nie tyle z ich skomplikowania, ile z ich niezrozumienia. Szczegółowa analiza powinna być lekarstwem na tę przypadłość. Na podobny problem – choć nie na gruncie RODO – zwraca uwagę J. Janowski. Zauważa on, że problemem jest niedostateczna współpraca w zakresie prowadzenia badań[13]. Wielowątkowa analiza przepisów RODO, mająca korzenie w solidnej analizie poszczególnych przepisów, czasem do poziomu analizy poszczególnych słów i oparte na tym fundamencie dalsze roz-

[13] Ibidem.

ważania, powinny być lekarstwem na ten problem, przynajmniej w zakresie tematyki niniejszej publikacji i pozostałych publikacji z cyklu.

Analiza prowadzona w warstwie o tym tytule, prowadzona jest z wykorzystaniem etapowej analizy semantycznej.

Warstwa druga – *Wnioski z analizy*

Pracę nad przepisem zaczynam zawsze od drobiazgowej jego analizy, zapis tej analizy znajduje się w warstwie pierwszej. W warstwie drugiej znajdują się wnioski z analizy przepisu. Warstwa druga jest zawsze krótsza od warstwy pierwszej, pozwala zatem czytelnikowi zapoznać się sprawnie z tematyką danego rozdziału. Jeżeli czytelnik szuka jakiejś informacji i nie udało mu się znaleźć jej w spisie treści, to przeczytanie podrozdziałów warstwy drugiej może mu w tym pomóc. Bardziej szczegółowe rozważania znajdzie czytelnik w podrozdziałach warstwy pierwszej, jednak zapoznawszy się z treścią warstwy drugiej – będzie wiedział, gdzie ich szukać.

Podrozdziały warstwy drugiej noszą tytuł „Wnioski z analizy", ich zawartość jest też swojego rodzaju krótkim komentarzem do analizowanego przepisu. Jeżeli czytelnik poszukuje publikacji komentarzowej, to publikacja niniejsza wraz z publikacjami jej towarzyszącymi powinna spełnić jego oczekiwania. Celem moim nie jest stworzenie komentarza do RODO, a przynajmniej nie tylko. Moim celem jest analiza kolejnych grup zagadnień regulowanych na gruncie RODO, prowadzona w ujęciu przedmiotowym, nie zaś w ujęciu wynikającym z kolejności umieszczenia przepisów w akcie prawnym. Cele niniejszej pracy wykraczają poza cele typowego komentarza do aktu prawnego, omawiam je niżej w części *Cele pracy*.

Warstwa trzecia – *Uwagi*

Warstwa trzecia zawiera rozważania, które jakkolwiek związane z tekstem odpowiedniego przepisu, to jednak nie wynikają z niego w sposób bezpośredni. W warstwie tej umieszczam rozważania wychodzące – w moim rozumieniu – poza proste wyniki z interpretacji odpowiednich przepisów. Cechą, która jest mi bliska przy dokonywaniu analizy przepisów, jest prawnicza uważność. Ze względu na tę uważność, staram się oddzielać wnioski z analizy przepisu od skojarzeń, jakie przepis ze sobą niesie.

Jak piszę wyżej, rozważania prawnicze zaczynam zawsze od drobiazgowej analizy przepisu. Po jej zapisaniu, przystępuję do lektury publikacji innych autorów. Pewna część tych lektur prowadzi do sformułowania własnych uwag, które uważam za godne zapisania. Uwagi takie mają czasem charakter nawiązania do poglądów poprzedników, czasem polemiki z tymi poglądami.

W warstwie „Uwagi" umieszczam też (tylko w niniejszym dziele z cyklu) stały element, czyli zestaw pytań zapisanych niżej w *Cele pracy w zakresie analizy oceny ryzyka i zjawisk pochodnych*. Część ta mogłaby tworzyć osobną warstwę, jednak zaburzyłoby to stronę formalną pracy, odróżniając ją od pozostałych prac z cyklu.

Warstwa czwarta – ***Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa***

W tej warstwie znajduje się element wskazany w tytule warstwy. Konceptualizm prawniczy – jako ogólna teoria prawa – jest moją autorską teorią obowiązywania i wykładni prawa. W niniejszej pracy nie zajmuję się obowiązywaniem prawa. Prawo traktuję tu jako coś zastanego i istniejącego w znaczeniu ontologicznym. Prawo „jest", a ja dokonuję jego analizy. Przyjmując, że prawo „jest", to rozważania ontologiczne nie są w pracy prowadzone. Mimo tego korzystam z teorii, wskazując za pomocą jej narzędzi, jakie uprawnienia – prawa i jakie obowiązki wynikają z kolejnych analizowanych przepisów. Zagadnieniem praw i wolności zajmuję się szerzej w pracy poświęconej zasadom w RODO[14]. Na gruncie niniejszej pracy korzystam oczywiście z ustaleń tam poczynionych. Prace stanowią cykl: merytoryczny, badawczy, naukowy, wreszcie – cykl wydawniczy. Ponieważ prace stanowią cykl, za niepotrzebne uważam prowadzenie niektórych rozważań *ab ovo*.

Mam świadomość zagrożenia oskarżeniem o powtarzanie się, wyjaśniam jednak, że intencją moją jest stworzenie cyklu dzieł poświęconych różnym fragmentom RODO i różnym problemom czy też grupom problemów związanych z RODO i szerzej – z ochroną danych osobowych, za racjonalne uważam zatem korzystanie w jednym z dzieł z cyklu, z ustaleń, które poczyniłem w innym z dzieł. Alternatywą byłoby pomijanie pewnych ważnych elementów, ukrywanie związ-

[14] J. Rzymowski, *RODO – GDPR. Zasady...*

ków między pracami lub prowadzenie wywodu równoległego. Prowadzenie wywodu równoległego uważam za niecelowe. Czasem względy wydawnicze, licencyjne itp. zmuszają do takich manewrów, pewna autorska ostrożność, wsparta pewną znajomością prawa autorskiego, pozwoliła mi problemów tych uniknąć. Ukrywanie związków między pracami uważam za nieuczciwe, tym bardziej że nie widzę potrzeby, by przy pisaniu jednej pracy wstydzić się, że napisałem wcześniejszą. Prace stanowią cykl, takie jest założenie, powodów do wstydu nie widzę. Pomijanie elementów w pracy uważam za coś bardzo złego. Człowiek jest człowiekiem tylko, więc czasem bywa, że pisząc, czy wykładając, coś pominiemy. Jest to przejawem niedoskonałości wywodu, jednak niedoskonałość jest ludzką kondycją. Godzę się z tym, jak (chyba) każdy. Gorzej, jeżeli pomijamy coś w wywodzie z niedbalstwa lub intencjonalnie, bo nie chcemy o czymś z jakichś względów pisać. Warstwowa konstrukcja pracy, etapowa analiza semantyczna, oddzielenie poszczególnych sfer wywodu prawniczego, mają na celu zminimalizowanie ryzyka pominięcia w wywodzie czegoś wskutek niedbalstwa. Intencjonalnych pominięć, przynajmniej dlatego, że nie chcę o czymś pisać, staram się nie czynić, przynajmniej świadomie. Nie ukrywam, że przepisy do analizy wybieram, jednak czynię tak z uwagi na fakt konstrukcji cyklu i tematyki kolejnych prac z cyklu. Wybieram przepisy ważne i interesujące naukowo oraz mające znaczenie dla praktyki, jednocześnie tematyka właśnie przesądza o wyborze kolejnych przepisów. Wydaje mi się, że wybieram przepisy istotne z punktu widzenia praktyki administratorów i podmiotów przetwarzających. Staram się też, by praktyka PUODO nie stała się przedmiotem niniejszej pracy.

Warstwa piąta – ***Konkretyzacja zasad*** (zasady)

W warstwie tej zajmuję się związkami danego przepisu z zasadami z art. 5 RODO.

Na marginesie, można się zgodzić z M. Bochenkiem, że *Regulowanie […] w politykach bezpieczeństwa informacji – zasad przetwarzania danych osobowych trzeba dokonywać „ad casum*”[15], z dwoma jednak zastrzeżeniami. A mianowicie, wskazany autor użył zapew-

[15] M. Bochenek, *Ochrona danych osobowych w pomocy społecznej w pytaniach i odpowiedziach*, Lex, Warszawa 2019.

ne słów „zasad przetwarzania danych osobowych" w znaczeniu potocznym, nie zaś w znaczeniu zasad uregulowanych w art. 5 RODO. Ponadto zasad (w znaczeniu zasad z art. 5 RODO) administrator (danych osobowych) nie może regulować gdziekolwiek, ponieważ są one przez prawodawcę uregulowane. Administrator (danych osobowych) możne jedynie i jak najbardziej powinien, uregulować realizację zasad z art. 5 RODO, nie same zasady, a ich realizację.

Warstwa szósta – *Postulaty „de lege ferenda"*

W warstwie tej stawiam postulaty nowelizacyjne. Nie jestem zwolennikiem nowelizowania przepisów tylko po to, by je zmienić. W ogóle nie jestem zwolennikiem zmiany „na inne". Zmiana, jeśli ma mieć sens, powinna być zmianą „na lepsze". Niestety przepisy RODO zawierają wiele niedociągnięć, co wiem choćby z rozważań prowadzonych w wydanych już książkach z cyklu. Ponieważ przepisy są niedoskonałe, to stawiam postulaty nowelizacyjne. Książki, o których mowa to:

– *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*. Kraków 2019.
– *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*. Łódź 2020.
– *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*. Łódź 2020.

Warstwa siódma – *Rozważania historyczne*

W tej warstwie wspominam o zagadnieniach analogicznych do zagadnień rozpatrywanych w niniejszej publikacji, na podstawie prawa obowiązującego. Wskazuję tu historyczne odpowiedniki obowiązujących aktualnie przepisów. Rozważania warstwy siódmej są ograniczone do minimum. Nie jestem historykiem prawa, nie uważam też, by dla analizowanych w niniejszej publikacji zagadnień, ustalenia historyczne miały duże znaczenie.

Praca może sprawiać wrażenie, że jest napisana w duchu pozytywizmu prawniczego, przepisy „są" – „są" w rozumieniu ontologicznym. „Są", czyli istnieją. To, co wynika z przepisów, może z nich wynikać właśnie dzięki temu, że one są. Pobieżna lektura pracy może rzeczywiście wieść do takiego wniosku ale… Zwracam uwagę, że

w wielu miejscach pracy posługuję się konceptualizmem prawniczym oraz narzędziami stworzonymi na bazie tej teorii.

Przypominam tu, że zgodnie z tą teorią na prawo składają się uprawnienia (prawa) osób fizycznych. Uprawnienia te są w istocie cechami osób fizycznych, cechy te podlegają rozumowemu opracowaniu, które można nazwać rozumieniem. Uprawnienia są dwukrotnie konkretyzowane. Pierwsza konkretyzacja ma miejsce podczas tworzenia przepisów. Innymi słowy, przepisy są to uprawnienia skonkretyzowane po raz pierwszy. Druga konkretyzacja ma miejsce podczas interpretacji przepisów, czy to w toku subsumpcji, czy to w toku analizy doktrynalnej. Jak zatem widać, wrażenie, zgodnie z którym praca jest napisana w duchu pozytywizmu prawniczego, byłoby wrażeniem co najmniej nadmiernym. Faktem jest, że pewien pozytywistyczny posmak praca ma, nie wyobrażam sobie jednak pracy dogmatycznej, która posmaku tego byłaby pozbawiona.

Konstrukcja pracy. Uzupełnienie

Na konstrukcję pracy można też spojrzeć inaczej. Praca skonstruowana jest w ten sposób, że patrzymy w niej na RODO przez pryzmat kolejnych czynności administratora. Kolejne czynności rozumiem tu jednak nie jako kolejne czynności wynikające z przepisów, w kolejności takiej, w jakiej ułożył je prawodawca, ale jako kolejne czynności podejmowane przez administratora. Kolejne, jako następujące po sobie.

Stan prawny

Prace nad książką prowadzone były do połowy grudnia 2022 roku, stan prawny, do którego odnoszę się w książce, oceniam więc na 15 grudnia 2022 roku.

Cele pracy

Cele pracy dzielą się na dwie grupy, są to:
– cele pracy dotyczące czynności o charakterze ocen (w zakresie analizy oceny ryzyka i zjawisk pochodnych) oraz
– pozostałe cele pracy.

Z uwagi na odmienność zasygnalizowanych celów pracy, omawiam je poniżej osobno. Poza tym cele należące do drugiej z wymienionych grup – numeruję.

Cele pracy dotyczące czynności o charakterze ocen (w zakresie analizy oceny ryzyka i zjawisk pochodnych)

Wstępna lektura i analiza przepisów RODO oraz ich stosowanie, prowadzą do wniosku, że w związku z każdą, a przynajmniej w związku z podstawowymi czynnościami związanymi z ochroną danych osobowych na gruncie RODO, należy zastanowić się nad pewnymi sprawami. Sprawy te można rozumieć jako punkty, na podstawie których należy uporządkować prowadzony tu namysł prawniczy. Można też je rozumieć jako pytania, które należy zadać i na które należy szukać odpowiedzi w przepisach RODO.

Jeśli chodzi o kwestie ochrony danych osobowych na gruncie RODO, należy najpierw zadać pewne pytania podstawowe, wymieniam je poniżej.
– Jakie czynności należy wykonać w związku z ochroną danych osobowych na gruncie RODO?
– Czy dana czynność jest związana z ochroną danych osobowych na gruncie RODO?
– Jaki jest związek danej czynności z ochroną danych osobowych?

Patrząc najogólniej, jednak już w odniesieniu do czynności związanych z ochroną danych osobowych należy zadać wymienione poniżej pytania.
– Kiedy należy wykonać czynność?
– Co powinno być przedmiotem czynności? (Jak należy wykonać daną czynność?)
– Jakie czynności należy podjąć po wykonaniu czynności, która jest przedmiotem namysłu?

Wśród czynności, które należy wykonać na gruncie RODO, a które mają związek z ochroną danych osobowych, znajdują się trzy czynności, których elementem jest ocena ryzyka. Do nich należą następujące czynności: ocena ryzyka przetwarzania danych osobowych, ocena skutków przetwarzania danych osobowych, ocena skutków naruszenia ochrony danych osobowych. W odniesieniu do każdej z tych czynności trzeba odpowiedzieć na wymienione poniżej pytania.

– Kiedy należy czynność wykonać?
– Co należy poddać ocenie?
– Jakie czynności należy wykonać po wykonaniu danej czynności?

Ocena skutków w znacznej mierze powtarza czynności oceny ryzyka, w związku z tym faktem pomijam analizę tej czynności w niniejszej publikacji.

Dla jasności wywodu wskazuję poniżej, jakie pytania należy zadać wobec każdej czynności, zawierającej w sobie element oceny.

W odniesieniu do oceny ryzyka naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze, należy zadać wymienione poniżej pytania.

– Kiedy należy wykonać ocenę naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze?
– Co należy poddawać ocenie przy dokonywaniu oceny naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze?
– Jakie czynności należy podjąć po wykonaniu oceny ryzyka naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze?

W odniesieniu do oceny skutków naruszenia ochrony danych osobowych należy zadać wymienione poniżej pytania.

– Kiedy należy wykonać ocenę skutków naruszenia ochrony danych osobowych?
– Co należy poddawać ocenie przy dokonywaniu oceny skutków naruszenia ochrony danych osobowych?
– Jakie czynności należy podjąć po wykonaniu oceny skutków naruszenia ochrony danych osobowych?

Konstrukcja pracy jest wynikiem pewnego, przewidzianego przez prawodawcę następstwa czynności, najpierw ocena ryzyka, później ocena skutków naruszenia. Następstwo, o którym tu piszę, jest

specyfiką ochrony danych w obecnym ujęciu. Najpierw administrator danych osobowych ocenia ryzyko, jakie związane jest z kolejnymi czynnościami na danych osobowych, później – jeśli zajdzie naruszenie – to administrator ocenia już nie ryzyko związane z czynnością (bo mało prawdopodobne, by naruszenie pokryło się z czynnością lub czynnościami), ale ze zdarzeniem zakwalifikowanym jako naruszenie. Analiza przepisów związanych z tymi dwoma zjawiskami stanowi oś niniejszej książki.

Pozostałe cele pracy

Paweł Fajgielski pisze, że *Wzmożone zainteresowanie problematyką ochrony danych osobowych*[16], zaowocowało wzmożoną produkcją publikacji dotyczących ochrony danych osobowych, nie zaowocowało niestety wzmożonym zrozumieniem niektórych zjawisk wynikających z RODO. Zjawiskiem takim, które jest omawiane, często jednak bez zrozumienia jego istoty, są wszelkie oceny ryzyka, których trzeba dokonywać na gruncie RODO. Nieinspirowane myślą P. Fajgielskiego, jednak zgodne z jej duchem, jest zarysowanie **pierwszego celu pracy** jako poczynienie ustaleń szczegółowych, dotyczących właśnie ocen ryzyka. Ustalenie, kiedy tych ocen dokonywać należy, co powinno być ich przedmiotem, jest to o tyle istotne, że – jak uważam – praca obok prawdopodobnej wartości naukowej ma również wartość praktyczną. Wszelkie mechanizmy oceny ryzyka, które wprowadzono do RODO, są, z prawnego punktu widzenia, mechanizmami nowymi. Wprowadzono je, jak się wydaje po to, aby – jak to ujął P. Fajgielski – umożliwić skuteczniejszą ochronę *osobom, których dane poddawane są przetwarzaniu*[17]. Poczynienie szczegółowych ustaleń dotyczących dokonywania ocen ryzyka, łącznie ze sformułowaniem i wysunięciem konkretnych propozycji dokonywania tychże ocen powinno – jak się zdaje – mieć walor praktyczny dla praktyków ochrony danych.

[16] P. Fajgielski, *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa 2019, s. 16.

[17] Ibidem.

Drugim celem pracy jest poczynienie ustaleń szczegółowych dotyczących ocen skutków naruszenia. I tu celem jest ustalenie, kiedy tych ocen dokonywać należy i co powinno być ich przedmiotem.

Ocena ryzyka czy też oceny ryzyka – przy ryzyku rozumianym jako ryzyko naruszenia praw (lub wolności) osoby fizycznej – prowadzi do wprowadzania rozwiązań technicznych i organizacyjnych, których celem jest osiągnięcie przez administratora danych stanu, w którym przetwarza on dane osobowe zgodnie z prawem, czyli nie narusza on praw lub wolności osób, których dane dotyczą[18].

Podkreślenia wymaga, że celem technicznej ochrony danych nie jest li tylko techniczna ochrona danych, dane chroni się po coś. Chroni się je po to, aby chronić prawa i wolności osób fizycznych. Z kolei prawa i wolności osób fizycznych chroni się po to, by chronić te osoby[19]. Podobna myśl obecna jest u Ch. Poszwińskiego, który pisze, że: *Z jednej strony mechanizm prawa UE ma na celu ochronę osoby fizycznej, z drugiej – narzuca na administratora (lub odpowiednio procesora) obowiązek poniesienia nakładów na zapewnienie bezpieczeństwa procesu przetwarzania*[20].

Elementem drugiego celu pracy jest ustalenie, jakie prawa i wolności osób fizycznych należy koniecznie na gruncie RODO chronić. Koresponduje to z myślą P. Fajgielskiego, który trafnie zauważa, że *Ochrona danych osobowych nie jest celem samym w sobie; ma rację bytu o tyle, o ile służy ochronie osób, których dane dotyczą*[21].

Trzecim celem pracy jest prezentacja etapowej analizy semantycznej w użyciu. Metodę tę dopracowuję od kilku lat. Z jej wykorzystaniem piszę wszystkie książki z serii, której niniejsza książka jest częścią. Analizy wykonane z wykorzystaniem tej metody znajdują się w książkach wymienionych poniżej:

– J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora,* Kraków 2019.

---

[18] Ibidem.

[19] Podobnie: A. Sobczyk, *RODO. Rozproszona władza publiczna,* Kraków 2019, s. 22–23.

[20] Ch. Poszwiński, op. cit., s. 17.

[21] P. Fajgielski, *Prawo ochrony danych osobowych…*

– J. Rzymowski, *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*, Łódź 2020.
– J. Rzymowski, *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje,* Łódź 2020.
– Również w napisanej wspólnie z D. Spałkiem książce: *RODO – GDPR. Ochrona danych medycznych,* Łódź 2022.

Metodę zaprezentowałem i omówiłem na zjeździe Stowarzyszenia FONTES w 2021 roku.

Czynności, składające się na metodę wymieniam poniżej.

– Pierwszą czynnością jest skopiowanie przepisu do pamięci komputera i następnie wielokrotne zapisanie go na stronie dokumentu. Robię to z wykorzystaniem komputera. Metodę można stosować również z wykorzystaniem papieru, jednak praca z wykorzystaniem komputera jest po prostu szybsza.
– Drugą czynnością jest zaznaczenie, w kolejnych zapisach przepisu, tych jego fragmentów, które nadają się do analizy. Zwykle są to zwroty, złożenia składające się z kilku wyrazów, czasem pojedyncze wyrazy. Ważne, by w każdym z kolejnych zapisów przepisu, czy też w każdej kolejnej kopii zaznaczyć jedynie jeden taki zwrot. Pozwala to zachować jasność wywodu i ogromnie ułatwia analizę. Ważne, by – kiedy patrzymy na całość zaznaczeń, biorąc pod uwagę wszystkie kopie zapisu przepisu – zaznaczone były w sumie wszystkie słowa przepisu. Daje to niejaką pewność, że żaden fragment przepisu nie zostanie pominięty.
– Trzecią czynnością jest dokładna analiza zaznaczonych fragmentów. Należy przy tym baczyć, by analizie poddawać każdorazowo jedynie zaznaczony fragment.
– Czwartą czynnością jest odłączenie uzyskanych analiz i zapisanie ich kolejno, jedna pod drugą. Uzyskujemy w ten sposób skrócony komentarz do przepisu. Na tym etapie kończy się podstawowa część metody. Możliwe są jednak również etapy dalsze.
– Kolejnych czynności nie numeruję, jednak zwracam uwagę, że po odłączeniu uzyskanych krótkich komentarzy, warto zachować skomentowane fragmenty przepisu wraz z odpowiadającymi im komentarzami. Tak uzyskany substrat pozwala, by go wykorzystać do dalszych rozważań. Można go wykorzystać na dwa sposoby. Prze-

de wszystkim, poczynając od zestawów składających się ze skomentowanego fragmentu przepisu i odpowiadającego mu komentarza, można prowadzić dalsze rozważania własne. Rozważania, które u podstaw mają omówienie przepisu. Można również przystąpić do dialogu z innymi autorami. Nieważne, czy dialog ten jest aprobatywny czy polemiczny, do każdego mamy podstawowy substrat, a to skomentowane – omówione, fragmenty przepisu.

Celem pracy jest prezentacja etapowej analizy semantycznej i możliwości, jakie ona daje. Nie omawiam w pracy (poza widniejącymi powyżej uwagami i uwagami umieszczonymi wyżej we *Wstępie*, w części *Metodologia*) tej metody, a po prostu ją stosuję. Analiza w podrozdziałach warstwy „Analiza" jest prowadzona konsekwentnie, z użyciem etapowej analizy semantycznej. Wnioski prezentowane w podrozdziałach warstwy „Wnioski z analizy" są również uzyskiwane z wykorzystaniem tej metody. W podrozdziałach warstwy „Uwagi" i warstwy „Postulaty *de lege ferenda*" również korzystam z etapowej analizy semantycznej, a to poprzez odniesienia do konkretnych fragmentów przepisów i do konkretnych fragmentów ich analizy.

Czwartym celem pracy jest prezentacja konceptualizmu prawniczego – ogólnej teorii prawa. Jest to moja autorska teoria obowiązywania prawa, ułatwiająca też dokonywanie jego wykładni. Teorię tę, podobnie jak wskazaną wyżej metodę wykładni, prezentuję w praktyce w podrozdziałach warstwy „Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa".

Piątym celem pracy jest postawienie postulatów *de lege ferenda*. Cel ten stawiam jako jeden z dalszych, ponieważ nie uważam za celowe, by widzieć stawianie postulatów nowelizacyjnych za cel sam w sobie, przynajmniej w niniejszej pracy. Postulaty należy stawiać tam, gdzie ich postawienie jest konieczne, celowe. Tam, gdzie prawo, czy to wręcz doprasza się o poprawienie, czy też tam, gdzie po prostu prawo można ulepszyć, czy choćby uczynić bardziej zrozumiałym.

Szóstym celem pracy jest dokonanie drobiazgowej analizy tekstu prawnego wybranych przepisów RODO. Cel ten jest, podobnie jak cel piąty, celem swoiście drugorzędnym, uważam jednak, że bez drobiaz-

gowej analizy tekstu prawnego, niemożliwe jest dokonywanie uczciwych ustaleń go dotyczących.

Siódmym celem pracy jest prezentacja warstwowej metody tworzenia prac naukowych. Metoda ta pozwala uzyskać przejrzystą konstrukcję pracy. Stałe elementy, określone przez mnie warstwami, które można nazwać też kategoriami podrozdziałów, są elementami każdego rozdziału pracy. Autorowi daje to łatwość w konstruowaniu poszczególnych rozdziałów. Czytelnikom daje to łatwość w odnalezieniu informacji należących do poszczególnych kategorii. Metoda warstwowa umożliwia też współpracę autorską. W niniejszej pracy tego nie stosuję, ponieważ praca ma charakter ściśle jednoautorski i stanowi jedną z części mojego dzieła habilitacyjnego, tym niemniej możliwość widzę. Metoda warstwowa umożliwia współpracę polegającą na tym, że jeden ze współautorów dokonuje analizy, drugi zajmuje się dyskusją z doktryną, trzeci teorią itd. W ten sposób prawnicy specjalizujący się w różnych dyscyplinach prawniczych mogą zgodnie pracować nad analizą jednego tekstu prawnego i co ważne – każdy w ramach swojej dyscypliny, przez co sprawnie i kompetentnie.

Cele pracy. Uwagi uzupełniające

Pozostając przy celach pracy, należy poczynić kilka jeszcze uwag. Celem pracy jest analiza przepisów RODO, dotyczących bezpieczeństwa danych osobowych, dotyczących ryzyka wiążącego się z przetwarzaniem danych osobowych. Na przepisy te, które omawiam w pracy, składają się art. 24, 32, 33 i 34 RODO. Można oczywiście przedkładać, że z bezpieczeństwem związane są pewne zasady z art. 5 RODO, jak również przepisy poświęcone tworzeniu ogólnego opisu technicznych i organizacyjnych środków bezpieczeństwa oraz nadawaniu upoważnień (i ewentualnie poleceń), jednak przepisami tymi zajmuję się we wcześniejszych książkach i to do poziomu przedstawienia wzorów odpowiednich dokumentów, nie widzę więc sensu, by rozważania te i w tej książce powtarzać.

Celem pracy jest stosowanie rygorów języka prawnego do języka prawniczego. Jest to szczególnie widoczne w warstwach „Uwagi" i „Postulaty *de lege ferenda*". Do dziś brzmi mi w uszach uwaga profesora Macieja Borskiego, który martwił się, czy prezentowana przeze mnie na zjeździe Stowarzyszenia FONTES etapowa analiza seman-

tyczna nie prowadzi do zubożenia języka prawniczego. Rozważania swoje staram się prowadzić poprawnym językiem polskim. Obawę M. Borskiego rozumiem, a Jego głos w dyskusji po wygłoszeniu przeze mnie referatu poświęconego etapowej analizie semantycznej, sprawił mi zaszczyt i przyjemność, jednak tam, gdzie to uważam za konieczne (wskazane wyżej warstwy), tam poświęcam urodę wywodu na rzecz jego dyscypliny i jasności.

Cele pracy mają charakter:
– analityczno-badawczy,
– porządkujący,
– projektujący.

Cel **analityczno-badawczy** realizowany jest w podrozdziałach warstwy „Analiza".

Cel **porządkujący** realizowany jest w podrozdziałach warstw „Wnioski z analizy" i „Uwagi" oraz „Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa".

W podrozdziałach warstwy „Wnioski z analizy" zamieszczone są skrócone wnioski uzyskane w podrozdziałach warstwy „Analiza".

W podrozdziałach warstwy „Uwagi" znajdują się wszelkie istotne asocjacje, jakie dostrzegam oraz opisy sposobów działania administratorów (danych osobowych).

W podrozdziałach warstwy „Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa" znajdują się krótkie opisy obowiązków administratora i uprawnień osób, których dane dotyczą.

Cel **projektujący** realizowany jest w podrozdziałach warstwy „Postulaty *de lege ferenda*", w których znajdują się postulaty nowelizacyjne.

Rozdział 1
Ocena ryzyka
na gruncie art. 24 RODO

Artykuł 24 RODO
Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

1.1. Art. 24 ust. 1 Analiza

Ze słów pogrubionych: ***Uwzględniając*** *[...]* ***administrator wdraża*** *[...]* wynika, że przepis dotyczy sytuacji, w której administrator ma obowiązek coś wdrożyć.

Ze słów pogrubionych: ***Uwzględniając*** *[...]* ***oraz*** *[...]* wynika, że obowiązek wdrożenia ma zostać wykonany z uwzględnieniem dwóch

grup warunków, chociaż łącznie czynników, które administrator musi brać pod uwagę, są trzy grupy. Pierwsza grupa warunków wymieniona jest po słowie: *uwzględniając*, druga grupa warunków wymieniona jest po słowie *oraz*. Z użycia słowa *oraz* wnioskujemy, że między warunkami z pierwszej grupy i między warunkami z drugiej grupy zachodzi koniunkcja, czyli że przepis jest zrealizowany wtedy, kiedy zrealizowane są warunki z jednej i drugiej grupy. Jeśli chodzi o realizację warunków z poszczególnych grup, to omawiam to niżej.

Ze słów pogrubionych: ***Uwzględniając charakter, zakres, kontekst i cele przetwarzania*** *[...]* wynika, że elementy które administrator musi wziąć pod uwagę przy realizacji niniejszego przepisu to: charakter, zakres, kontekst, cele przetwarzania. Między słowem *charakter* a słowem *zakres* oraz między słowem *zakres* a słowem *kontekst* prawodawca użył przecinków. Przecinkiem zwykle zastępowane jest słowo „lub", choć może ono zastępować również słowo „i", dlatego przepis nie jest tu w pełni jasny. Słowo „lub" jest funktorem logicznym o stałym znaczeniu. Kiedy słowo to zostaje użyte w zdaniu i łączy ono dwa elementy, to interpretować należy w ten sposób, że zajść może albo tylko pierwszy element, albo tylko drugi element, albo obydwa elementy jednocześnie, a przynajmniej jest ryzyko takiej interpretacji. Konsekwentne trzymanie się tej zasady prowadziłoby do decyzji interpretacyjnej, zgodnie z którą uwzględniono by:
– **charakter** przetwarzania i **cele** przetwarzania
albo
– **zakres** przetwarzania i **cele** przetwarzania,
albo
– **kontekst** przetwarzania i **cele** przetwarzania,
albo
– **charakter** i **zakres** i cele przetwarzania,
albo
– **charakter** i **kontekst** i cele przetwarzania,
albo
– **zakres** i **kontekst** i **cele** przetwarzania,
albo
– **charakter** i **zakres** i **kontekst** i **cele** przetwarzania.

Wniosek taki wypływa z rozumowania przeprowadzonego poniżej. Zestawiamy: „charakter, zakres, kontekst i cele przetwarzania",

przecinki zastępujemy słowem „lub" i konsekwentnie przeprowadzamy eliminację i łączenie pojęć. Dla jasności rozumowania pozostawiam wyeliminowane pojęcia, ujmując je w nawiasy, dla czytelności zaś, pojęcia, które pozostawiam, zostają wytłuszczone.

Rozumowanie wygląda zatem jak poniżej prezentuję:
charakter i **zakres** i **kontekst i cele przetwarzania**;
charakter i **zakres** (kontekst) **i cele przetwarzania**;
charakter i (zakres) **kontekst i cele przetwarzania**;
(charakter) **zakres** i **kontekst i cele przetwarzania**;
(charakter), **zakres**, (kontekst) **i cele przetwarzania**;
(charakter), (zakres), **kontekst i cele przetwarzania**;
charakter i (zakres), **kontekst i cele przetwarzania**.

W powyższych rozważaniach przyjmuję znaczenie przecinka jako „lub". Wydaje się, że powinien on być przy interpretacji przedmiotowego przepisu interpretowany jako „i" [22]. W tym właśnie duchu interpretuję przepis. Jednocześnie, z uwagi na pewną płynność znaczeniową przecinka, mam pewien niepokój, w związku z którym postuluję zmianę treści komentowanego przepisu, tak by nikt tego niepokoju nie odczuwał. (*6. Art. 24. Postulaty de lege ferenda. 6.1. Art. 24 Postulat 1. Zastąpienie przecinków literami „i"*)

Charakter, zakres, kontekst i cele przetwarzania to pierwsza grupa zjawisk, które administrator musi wziąć pod uwagę przy realizacji omawianego przepisu.

Charakter, zakres, kontekst, cele i ryzyko są wymienione w przepisie w taki sposób, że nie widzę powodu, by je wartościować. Można się zastanawiać, czym jest charakter przetwarzania i kontekst przetwarzania, to jednak sprawa osobna, którą zajmuję się niżej w uwadze (*3.10. Art. 24. Uwaga 10. Charakter, zakres, kontekst i cele przetwarzania*) i (*3.8. Art. 24 Uwaga 8. Zakres) i (3.11. Art. 24. Uwaga 11. Kontekst przetwarzania*).

Nie wydaje się, by intencją prawodawcy było wyłączanie kolejnych ze wskazanych wyżej elementów przepisu z ostatecznego wniosku interpretacyjnego. W związku z tym znowu jedynie wydaje się, że przecinki w odpowiednich miejscach należy zastąpić literami „i". Jeżeli się to uczyni, to okaże się, że administrator ma obowiązek uwzględnić,

[22] A. Malinowski, *Polski tekst prawny. Opracowanie treściowe i redakcyjne,* Warszawa 2012, s. 89.

tak jak wskazano na końcu powyższego wyliczenia charakter i zakres i kontekst i cele przetwarzania. Niżej stawiam odpowiedni postulat *de lege ferenda* w tej sprawie (*6.1. Art. 24 Postulat 1. Zastąpienie przecinków literami i*).

Ze słów pogrubionych: ***Uwzględniając [...] ryzyko naruszenia praw lub wolności osób fizycznych*** *[...]* wynika, że administrator ma obowiązek uwzględnić ryzyko naruszenia praw osób fizycznych oraz ryzyko naruszenia wolności osób fizycznych. Wydaje się, że również w tym miejscu użyto funktora *lub* ze względów przypadkowych. Gdyby rzeczywiście intencją prawodawcy było użycie funktora *lub*, administrator miałby obowiązek uwzględniać:
– ryzyko naruszenia praw osób fizycznych
albo
– ryzyko naruszenia wolności osób fizycznych,
albo
– ryzyko naruszenia praw i wolności osób fizycznych.

Podobnie jak wyżej, w przypadku charakteru, zakresu, kontekstu i celów przetwarzania, tak i tu nie wydaje się, by intencją prawodawcy było wyłączenie praw albo wolności z ostatecznego wniosku interpretacyjnego. Zwracam przy tym uwagę na fakt, że prawa i wolności osób fizycznych zostały zapisane, niejako pod postacią obowiązków administratora w art. 5 RODO. Przepis ten stanowi o zasadach dotyczących przetwarzania danych osobowych. Zagadnienie to rozwijam niżej w uwadze (*3.1. Art. 24 Uwaga 1. Co regulują zasady z art. 5 RODO*), z uwagi zaś na upodobanie do porządku w aktach prawnych, niżej jeszcze stawiam postulat nowelizacyjny (*6.2. Art. 24 Postulat 2. Zastąpienie słowa* lub *słowem* i). Konieczność oceny pod kątem poziomu ryzyka dla praw i wolności osób fizycznych dostrzegają autorzy czescy[23]. Co ciekawe, ślad tej koncepcji obecny jest u A. Cieślika, który pisze, że *Najważniejszymi elementami bezpieczeństwa każdej informacji są poufność, integralność oraz dostępność*[24]. Nie sposób pominąć faktu, że w zjawiskach tych wskazany autor widzi cechy bezpieczeństwa informacji, nie zaś uprawnienia, nie

[23] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, *GDPR / Obecné nařízení o ochraně osobních údajů. Prakticky komentař*, Praha 2017, s. 245.

[24] A. Cieślik, *Ocena (szacowanie) ryzyka*, [w:] *Dokumentacja ochrony danych osobowych ze wzorami*, red. n. Mariusz Jagielski, Warszawa 2022, s. 141.

sposób jednocześnie pominąć faktu, że dwie z trzech wymienionych pokrywają się z zasadami z art. 5 RODO, czyli w istocie są prawami/obowiązkami.

Należy zwrócić uwagę na fakt, że prawodawca nie zdefiniował pojęcia „ryzyko". Pojęciem tym zajmuję się dalej w uwagach (*3.28. Art. 24. Uwaga 28. Ryzyko. Pojęcie na gruncie art. 24*) i (*3.29. Art. 24. Uwaga 29. Ryzyko. Pojęcie na gruncie art. 32*).

Ze słów pogrubionych: *[...] ryzyko naruszenia praw lub wolności osób fizycznych* ***o różnym prawdopodobieństwie i wadze****, [...]* wynika, że administrator powinien brać pod uwagę różne prawdopodobieństwo i wagę ryzyka naruszenia praw i wolności osób fizycznych.

Ze słów pogrubionych: *[...] administrator* ***wdraża odpowiednie środki*** *[...]* wynika, że administrator ma obowiązek wdrażać środki określone w przepisie mianem odpowiednich.

Należy się zastanowić, co oznacza w tym przypadku, że środki są odpowiednie. Odpowiedniość środków należy oceniać przede wszystkim na gruncie omawianego przepisu. Środki odpowiednie to zatem środki odpowiednie do:

– charakteru przetwarzania i
– zakresu przetwarzania, i
– kontekstu przetwarzania, i
– celów przetwarzania, i
– ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

Nad znaczeniem poszczególnych wymienionych powyżej pojęć zastanawiam się niżej, przy omawianiu stosownych fragmentów przepisu. Jestem sobie w stanie wyobrazić, że ktoś przyjmuje, że środki, o których tu mowa, mają być odpowiednie nie do wszystkich wskazanych powyżej czynników, ale że mają one być odpowiednie jedynie do ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, charakter zaś, zakres kontekst i cele przetwarzania stwarzają jedynie środowisko, warunki, czy właśnie kontekst przetwarzania i kontekst ryzyka, nie wydaje się jednak, żeby taka interpretacja była poprawna.

Na ciekawą – choć z pozoru oczywistą sprawę – zwraca uwagę P. Fajgielski. Autor ten wskazuje, że środki, które ma wdrożyć administrator, mają być odpowiednie, a niekoniecznie najlepsze możliwe,

P. Fajgielski pisze[25]: *zabezpieczenia powinny być odpowiednie, nie chodzi tu o zabezpieczenia najlepsze z możliwych (najnowsze, najdroższe, najbardziej zaawansowane technologicznie), a o takie środki techniczne i organizacyjne, które są proporcjonalne*. Zwracam uwagę, że o ile art. 32 ust. 1 RODO stanowi o kosztach, o tyle art. 24 ust. 1 RODO o kosztach nie wspomina. Wynika z tego, że proporcjonalność czy też odpowiedniość środków powinna być uzależniona od okoliczności wskazanych w przepisie, jednak koszt do tych okoliczności nie należy.

Ze słów pogrubionych: *[...] wdraża [...] środki* ***techniczne i organizacyjne****, aby przetwarzanie odbywało się [...]* wynika, że środki, które ma obowiązek wdrożyć administrator, są to środki techniczne i środki organizacyjne. Można sobie wyobrazić próbę rozróżnienia środków technicznych od środków organizacyjnych, uważam jednak taką próbę za niepotrzebną i jałową.

Kiedy patrzymy z lotu ptaka na różne sposoby, za pomocą których zabezpieczane są dane, to możemy uczciwie powiedzieć, że trudno jest (znów) uczciwie zakwalifikować jedne środki do kategorii środków technicznych, a inne środki do kategorii środków organizacyjnych. Należy przy tym zwrócić uwagę na fakt, że stosowanie wspomnianych środków jest sposobem do osiągnięcia celu, którym jest to, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Zwracam uwagę, że nie chodzi tu jedynie o (jakkolwiek rozumiane) bezpieczeństwo danych osobowych.

Ze słów pogrubionych: *[...] wdraża odpowiednie środki techniczne i organizacyjne,* ***aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem*** *[...]* wynika, że celem wdrożenia środków technicznych i organizacyjnych, o których mowa wyżej, jest, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO. Zwracam uwagę, że przepis analizowany stanowi o ocenie ryzyka, której celem nie jest – a przynajmniej nie jest jedynie – ochrona danych osobowych, ale że celem tej oceny jest, by przetwarzanie odbywało się zgodnie z RODO[26].

Analizowany przepis jest niezwykle ciekawy. Są w nim słowa o ryzyku (naruszenia praw i wolności), jednak przepis nakazuje prze-

---

[25] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679...,* Kom. do art. 24.

[26] Podobne stanowisko prezentują autorzy czeskiego komentarza. M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit., s. 245.

prowadzać procedurę, której celem ma być osiągnięcie stanu zgodności przetwarzania danych osobowych z RODO.

Ze słów pogrubionych: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem* ***i aby móc to wykazać****. [...]* wynika, że celem wdrożenia środków technicznych i organizacyjnych, o których mowa wyżej, jest, aby administrator był w stanie wykazać, że przetwarzanie danych osobowych odbywa się w zgodzie z RODO. Obowiązek wykazania faktu przetwarzania danych osobowych zgodnie z RODO jest powtórzeniem zasady rozliczalności i obowiązku rozliczalności, zapisanych w art. 5 ust. 2 RODO[27].

Ze słów pogrubionych: *[...]* ***Środki te są*** *w razie potrzeby* ***poddawane przeglądom i uaktualniane,*** wynika, że administrator (danych osobowych) ma obowiązek poddawać wskazane wyżej środki techniczne i organizacyjne przeglądom i że administrator ma obowiązek wskazane środki uaktualniać.

Ze słów pogrubionych w art. 24 ust. 1 RODO: *[...] Środki te są* ***w razie potrzeby*** *[...]* wynika, że przeglądy i uaktualnianie środków technicznych i organizacyjnych mają zachodzić w razie potrzeby. Potrzeba uaktualnienia środków technicznych i organizacyjnych może być różnie rozumiana.

Przez potrzebę tę można rozumieć potrzebę przeglądu i uaktualnienia środków co jakiś czas, tak aby nie stały się one nieaktualne i aby nie przestały odpowiadać wymienionym w przepisie parametrom, którym odpowiadać powinny.

Przez potrzebę tę można rozumieć potrzebę przeglądu i uaktualnienia środków wynikającą z nagłej zmiany warunków przetwarzania, ze zmiany otoczenia faktycznego, zmiany realiów technicznych czy wręcz zmiany prawa.

Przez potrzebę tę można rozumieć potrzebę przeglądu i uaktualnienia środków wynikającą z przepisów innych niż RODO.

Przez potrzebę tę można rozumieć potrzebę przeglądu i uaktualnienia środków wynikającą z art. 39 ust. 1 lit. b RODO.

---

[27] Podobnie: Ch. Docksey, [w:] *The EU General Data Protection Regulation (GDPR). A Commentary.* Edited by Ch. Kuner, L.A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020, s. 557. Również: M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit.

2.1. Art. 24 ust. 1 Wnioski z analizy

Administrator (danych osobowych) ma obowiązek wdrożyć i uwzględnić okoliczności wskazane w przepisie.

Obowiązek wdrożenia ma zostać wykonany z uwzględnieniem dwóch grup warunków. Między warunkami z pierwszej grupy i między warunkami z drugiej grupy zachodzi koniunkcja, czyli przepis jest zrealizowany wtedy, kiedy zrealizowane są warunki z jednej i drugiej grupy.

Pierwsza grupa warunków, czyli elementów, które administrator musi wziąć pod uwagę przy realizacji niniejszego przepisu to: charakter, zakres, kontekst, cele przetwarzania.

Druga grupa warunków, które administrator ma obowiązek uwzględnić to: ryzyko naruszenia praw osób fizycznych oraz ryzyko naruszenia wolności osób fizycznych.

Administrator (danych osobowych) powinien brać pod uwagę różne prawdopodobieństwa i wagę ryzyka naruszenia praw i wolności osób fizycznych.

Trzecia grupa warunków, które administrator (danych osobowych) ma obowiązek uwzględnić to środki określone w przepisie mianem odpowiednich, które administrator ma obowiązek wdrażać.

Środki odpowiednie to zatem środki odpowiednie do:
– charakteru przetwarzania i
– zakresu przetwarzania, i
– kontekstu przetwarzania, i
– celów przetwarzania, i[28]
– ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

Środki, które ma obowiązek wdrożyć administrator (danych osobowych), są to środki techniczne i organizacyjne. Próbę rozróżnienia środków technicznych od środków organizacyjnych czy też zdefiniowania jednych i drugich uważam za niepotrzebną i jałową. Ślad podobnej myśli dostrzegam u P. Siembidy, który środki te wymienił w dwóch odpowiednich grupach[29].

---

[28] Zasady edytorskie (samotna litera na końcu wersu) poświęcam tu i w kilku innych miejscach książki świadomie na rzecz graficznej jasności.

[29] P. Siembida, [w:] A. Krasuski, P. Siembida, *Analiza ryzyka w ochronie danych osobowych*, Warszawa 2022, s. 247–250.

Celem wdrożenia środków technicznych i organizacyjnych, o których mowa wyżej jest, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO[30].

Celem wdrożenia środków technicznych i organizacyjnych, o których mowa wyżej, jest również, aby administrator (danych osobowych) był w stanie wykazać, że przetwarzanie danych osobowych odbywa się w zgodzie z RODO.

Administrator ma obowiązek poddawać wskazane wyżej środki techniczne i organizacyjne przeglądom i uaktualniać w razie potrzeby. Potrzeba ta może wynikać z różnych czynników.

1.2. Art. 24. ust. 2 Analiza

Ze słów pogrubionych: ***Jeżeli jest to proporcjonalne w stosunku do*** *[...]* wynika, że administrator ma obowiązek zrealizować przepis, jeżeli przedmiot realizacji przepisu jest proporcjonalny do okoliczności wskazanych w przepisie.

Ze słów pogrubionych: *[...]* ***środki, o których mowa w ust. 1****, [...]* wynika, że przedmiotem realizacji przepisu są środki, o których mowa w art. 24 ust. 1 RODO, czyli środki techniczne i organizacyjne podejmowane przez administratora po to, aby przetwarzanie danych osobowych odbywało się w zgodzie z RODO.

Ze słów pogrubionych: *[...]* ***proporcjonalne w stosunku do czynności przetwarzania*** *[...]* wynika, że tym, do czego mają być proporcjonalne środki, są czynności przetwarzania danych osobowych.

Przetwarzanie to czynność na danych osobowych, więc zwrot „czynności przetwarzania" nie ma sensu, oznacza bowiem on „czynność czynność na danych osobowych". Oczywiście taką interpretację łatwo odrzucić, nie zmienia to jednak faktu, że użycie zwrotu „czynność przetwarzania" jest błędem, a co najmniej pewną nadmiernością.

Lektura przepisu wskazuje, że jeżeli jedno ze zjawisk wskazanych w przepisie jest proporcjonalne do drugiego, to skutkuje to jedną decyzją, więc zapewne jeśli nie jest, to skutkuje to drugą decyzją. Na administratorze (danych osobowych) spoczywa więc obowiązek dokonania oceny proporcjonalności, o której tu mowa. Wracam do tego niżej w uwadze *(3.5. Art. 24 Uwaga 5. Proporcjonalność środków w świetle zasady rozliczalności*).

[30] Podobnie: P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679…,* Kom. do art. 24.

Ze słów pogrubionych: *[...]* ***środki*** *[...]* ***obejmują wdrożenie*** *[...]* wynika, że środki o których mowa, obejmują wdrożenie elementu wskazanego dalej w przepisie.

Ze słów pogrubionych: *[...]* ***wdrożenie*** *[...]* ***polityk ochrony danych***. *[...]* wynika, że elementem, który ma podlegać wdrożeniu na warunkach wskazanych w przepisie, są polityki ochrony danych.

Przepis mówi o politykach ochrony danych, czyli jest w nim użyta liczba mnoga wobec słów „polityka ochrony danych". Mogłoby to stworzyć mylne wrażenie, że administrator – jeśli uzna wdrożenie polityki ochrony danych za właściwe – musi wdrożyć co najmniej dwie takie polityki, podczas gdy nie ma powodu, by uważać, że niewłaściwe jest wdrożenie na przykład jednej takiej polityki.

Należy zwrócić uwagę, że obowiązek wynikający z przepisu ma charakter warunkowy. Jeżeli „jest to proporcjonalne", to na administratorze spoczywa obowiązek wdrożenia środków, o których mowa w przepisie, czyli polityk ochrony danych. Zachodzi tu niezwykle ciekawe zjawisko. Na administratorze nie spoczywa obowiązek wdrożenia polityk ochrony danych, chyba że „jest to proporcjonalne w stosunku do czynności przetwarzania", wtedy bowiem na administratorze spoczywa obowiązek wdrożenia polityk ochrony danych.

Ze słów pogrubionych: *[...]* ***odpowiednich polityk*** *ochrony danych [...]* wynika, że polityki ochrony danych czy też polityka ochrony danych, o których mowa w przepisie, czyli które miałyby być wdrożone, jeśli administrator podejmie taką decyzję, powinny mieć przymiot odpowiedniości. Polityki odpowiednie to zapewne polityki dostosowane do konkretnego administratora i do jego konkretnej sytuacji, co jednak nie wyklucza polityki przygotowanej w sposób – powiedzmy – neutralny, bez związku z administratorem i jego sytuacją na etapie przygotowywania a następnie wdrożonej u danego administratora. Niżej w uwadze (*3.6. Art. 24 Uwaga 6. Odpowiedniość polityki ochrony danych*).

Ze słów pogrubionych: *[...]* ***wdrożenie przez administratora*** *[...]* ***polityk*** *[...]* wynika, że polityki ochrony danych, o których mowa w przepisie, muszą zostać przez administratora wdrożone. Musi się odbyć coś, co można określić mianem wdrożenia. Z pogrubionych słów wynikają dwa elementy, a to, że:
– polityki muszą zostać wdrożone,
– wdrożenie polityk musi przeprowadzić administrator.

Jeśli chodzi o to że „polityki muszą zostać wdrożone", oznacza to, że oprócz stworzenia polityk, rozumianej jako ich napisanie, obowiązkiem administratora jest wykonanie innej czynności, czynności wdrożenia. Poza tym, z uwagi na obowiązek rozliczalności wynikający z art. 5 ust. 2 RODO, czynność wdrożenia musi zostać udokumentowana. W sensie funkcjonalnym, przez wdrożenie należy rozumieć świadome i celowe rozpoczęcie stosowania czegoś, w opisywanej sytuacji, świadome i celowe rozpoczęcie stosowania polityki ochrony. Może ono być połączone z rozpoczęciem stosowania przewidzianych w niej procedur, przeszkoleniem pracowników, uruchomieniem rozwiązań technicznych. Wskazane tu przykładowe czynności – związane z wdrożeniem i wszelkie inne analogiczne – można określić wdrożeniem w rozumieniu funkcjonalnym.

Z uwagi na obowiązek rozliczalności, administrator powinien zadbać również o coś, co można by nazwać wdrożeniem w znaczeniu formalnym, czyli po prostu o odpowiedni dokument, z którego będzie wynikało, że wdrożenie miało miejsce. Na etapie tworzenia dokumentu, z dokumentu tego powinno wynikać, że administrator wdraża taką to a taką politykę.

Podejście takie może wydawać się naiwne, można bowiem mieć wątpliwość w kwestii sensowności tworzenia dokumentu wdrożenia polityki ochrony, czyli dokumentu odnoszącego się do innego dokumentu. Prawdą jest, że jest to naiwne, jednak z punktu widzenia obowiązku rozliczalności jest to konieczne. Jednocześnie, kiedy spojrzymy na politykę ochrony i dokument wdrożenia tejże przez pryzmat funkcjonowania polityki, to dokument wdrożenia pewien sens ma. Niedobrze by było, gdyby polityka była tylko papierem, który napisano, kupiono, który jednak nijak nie wpływa na działania administratora. Dzięki wdrożeniu, polityka staje się częścią rzeczywiście funkcjonujących procedur administratora, dokument wdrożenia jest tego jedynie i aż dowodem.

Jeśli chodzi o to, że „wdrożenie polityk musi przeprowadzić administrator", należy rozumieć tak, że istotne, by z dokumentu wdrożenia polityki wynikało, że wdraża ją administrator. Można to uzyskać przez odpowiednie sformułowanie tego dokumentu, umocowanie osób go sporządzających do sporządzania go w imieniu administratora itd.

2.2. Art. 24 ust. 2 Wnioski z analizy

Administrator (danych osobowych) ma obowiązek zrealizować przepis, jeżeli przedmiot realizacji przepisu jest proporcjonalny do okoliczności wskazanych w przepisie.

Przedmiotem realizacji przepisu są środki, o których mowa w art. 24 ust. 1 RODO, czyli środki techniczne i organizacyjne podejmowane przez administratora (danych osobowych) po to, aby przetwarzanie danych osobowych odbywało się w zgodzie z RODO.

Środki te mają być proporcjonalne do czynności przetwarzania danych osobowych.

Środki, o których mowa, obejmują wdrożenie elementu wskazanego dalej w przepisie.

Elementem, który ma podlegać wdrożeniu, na warunkach wskazanych w przepisie RODO, są polityki ochrony danych lub polityka ochrony danych.

Polityki ochrony danych czy też polityka ochrony danych, o których mowa w przepisie, powinny mieć przymiot odpowiedniości, czyli powinny one być dostosowane do konkretnego administratora (danych osobowych) i do konkretnej jego sytuacji.

Polityki ochrony danych, o których mowa w przepisie, muszą zostać przez administratora (danych osobowych) wdrożone. Czynność wdrożenia musi zostać udokumentowana.

Istotne, by z dokumentu wdrożenia polityki wynikało, że wdraża ją administrator (danych osobowych).

1.3. Art. 24. ust. 3 Analiza

Ze słów pogrubionych: ***Stosowanie zatwierdzonych kodeksów postępowania*** *[...]* wynika, że przepis dotyczy stosowania kodeksów postępowania, które zostały zatwierdzone przez krajowy organ ochrony danych. O kodeksach mowa jest w art. 40 RODO.

Ze słów pogrubionych: ***Stosowanie*** *[...]* ***zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42*** *[...]* wynika, że przepis dotyczy stosowania mechanizmu certyfikacji, o którym mowa jest w art. 42 RODO.

Ze słów pogrubionych w art. 24 ust. 3 RODO: ***Stosowanie*** *[...]* ***może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków***, wynika, że sto-

sowanie jednego lub drugiego elementu wskazanego w przepisie może służyć do wykazania, że administrator realizuje obowiązki, które na nim spoczywają. Kryje się tu jednak pewna pułapka, a nawet dwie.

– Po pierwsze ze słów ***może być wykorzystane***, należy wnosić, że na przykład organ ochrony danych nie ma obowiązku z jednego lub z drugiego mechanizmu korzystać.

  Administrator może zatem mieć wprowadzony jeden lub drugi mechanizm, lub nawet obydwa, a mimo tego organ kontrolny może przeprowadzić kontrolę, tak jakby żadnego z tych elementów, czyli ani wdrożonego kodeksu, ani certyfikacji, u danego administratora nie zastosowano.

– Po drugie, ze słów ***jako element dla stwierdzenia przestrzegania***, a zwłaszcza ze słów ***jako element*** należy wnosić, że czy to jeden czy drugi mechanizm, o których mowa w przepisie mogą być traktowane co najwyżej jako element stwierdzenia realizacji przez administratora, spoczywających na nim obowiązków.

Należy przy tym zwrócić uwagę na fakt, że posiadanie certyfikatu nie zwalnia z obowiązku stosowania RODO. Wydaje się to oczywiste, jednak mimo tego prawodawca zdecydował się na umieszczenie wart. 42 ust. 4 RODO, poświęconym certyfikatom, słów: *Certyfikacja przewidziana w niniejszym artykule nie wpływa na spoczywający na administratorze lub podmiocie przetwarzającym obowiązek przestrzegania niniejszego rozporządzenia […]*

Niżej spoglądam na zagadnienie ze strony organu kontrolnego oraz ze strony administratora.

Spojrzenie ze strony organu kontrolnego.

Jeżeli organ kontrolny bierze pod uwagę, przy okazji kontroli, stosowanie przez administratora zatwierdzonego kodeksu postępowania albo stosowanie przez administratora zatwierdzonego mechanizmu certyfikacji, albo stosowanie przez administratora obydwu tych mechanizmów, to organowi kontrolnemu nie wolno na tym poprzestać. Organ kontrolny nie może, na przykład ograniczyć kontroli do stwierdzenia faktu, że administrator stosuje kodeks albo posiada ważny certyfikat, albo posiada obydwa te rozwiązania jednocześnie. Ponadto należy pamiętać, że zadaniem organu, jest (nieco upraszczając) kontrola przestrzegania RODO, nie zaś kontrola przestrzegania kodeksu czy kontrola posiadania certyfikatu.

Spojrzenie ze strony administratora.

Jeżeli administrator stosuje zatwierdzony kodeks postępowania albo zatwierdzony mechanizm certyfikacji, albo stosuje obydwa te mechanizmy, to administratorowi nie wolno na tym poprzestać. Jeżeli na przykład administrator stosuje kodeks i stosowanie tego kodeksu nie gwarantuje realizacji wszystkich obowiązków administratora, to administrator i tak musi te obowiązki realizować. Administrator musi je realizować, wychodząc z działaniem niejako ponad kodeks, ale również czasem naruszając wskazania kodeksu, jeżeli okaże się to konieczne. Należy pamiętać, że stosowanie kodeksu nie zwalnia administratora ze stosowania RODO.

Ze słów pogrubionych w art. 24 ust. 3 RODO: ***Stosowanie*** *zatwierdzonych kodeksów postępowania, o których mowa wart. 40* ***lub*** *zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 […]* wynika, że administrator może stosować albo tylko kodeks, albo tylko posiadać certyfikat, albo stosować kodeks i posiadać certyfikat.

Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO, może być wykorzystane jako element do stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

2.3. Art. 24 ust. 3 Wnioski z analizy

Przepis dotyczy stosowania kodeksów postępowania, które zostały zatwierdzone przez krajowy organ ochrony danych. O kodeksach mowa jest w art. 40 RODO.

Przepis dotyczy stosowania mechanizmu certyfikacji, o którym mowa jest w art. 42 RODO.

Stosowanie jednego lub drugiego elementu wskazanego w przepisie może służyć do wykazania, że administrator (danych osobowych) realizuje obowiązki, które na nim spoczywają. Jeden czy drugi mechanizm, o których mowa w przepisie, mogą być traktowane co najwyżej jako element stwierdzenia realizacji przez administratora spoczywających na nim obowiązków. Organ kontrolny nie może ograniczyć kontroli do stwierdzenia faktu, że administrator (danych osobowych) stosuje kodeks lub posiada ważny certyfikat. W sytuacji, kiedy administrator (danych osobowych) stosuje zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji, na administra-

torze tym lub na organie kontrolnym, lub na sądach spoczywa obowiązek polegający na tym, że jeden lub drugi ze wskazanych elementów lub obydwa jednocześnie mogą być wykorzystane jedynie jako element służący do stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

3. Art. 24 Uwagi

3.1. Art. 24 Uwaga 1

Prawa i wolności

Artykuł 24 ust. 1 RODO nakazuje uwzględniać *[...]* ***ryzyko naruszenia praw lub wolności osób fizycznych*** *[...]*. Sprawy związane z prawami i wolnościami na gruncie RODO szerzej omawiam w monografii *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*[31]. Tu jedynie sygnalizuję najważniejsze elementy koncepcji.

Uważam, że cytowane słowa odnoszące się do praw i wolności osób fizycznych to w istocie klauzula odsyłająca, która odsyła do tych praw i wolności osób fizycznych, które wskazane i uregulowane są w RODO.

W RODO dostrzegam przede wszystkim dwie grupy praw i wolności. Pierwsza grupa to prawa i wolności zapisane w art. 5 RODO, a zwłaszcza w art. 5 ust. 1 RODO. Część wprowadzająca tego przepisu stanowi: *Dane osobowe muszą być*. W związku z tym zasady zapisane w art. 5 ust. 1 RODO to po prostu nic innego jak obowiązki administratora. Skoro zasady to obowiązki administratora, to tym samym zasady to prawa, czyli uprawnienia osób, których dane dotyczą. Z uwagi na fakt, że wspomniane prawa i wolności zapisane są w art. 5 RODO, statuującym jednocześnie zasady, wydaje się, że wobec wspomnianych praw i wolności należy używać nazwy: „prawa i wolności zasadnicze".

System składający się z obowiązków i uprawnień służy ochronie wolności, które tym obowiązkom i uprawnieniom odpowiadają. Z tego względu poprawniej jest mówić o „prawach i wolnościach", nie zaś o „prawach lub wolnościach", ponieważ kiedy chronimy jedne, to chronimy również drugie. W związku z tym stawiam niżej postulat

[31] J. Rzymowski, *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje,* Łódź 2020.

nowelizacyjny (*6.1. Art. 24 Postulat 2. Zastąpienie słowa „lub" słowem „i"*).

Druga grupa praw i wolności to prawa i wolności zapisane w kolejnych przepisach RODO. Z uwagi na fakt, że przepisy te można nazwać – dla odróżnienia od zasad – przepisami szczegółowymi RODO, uprawnienia te można nazywać uprawnieniami szczegółowymi.

Na prawa i wolności, o których mowa w RODO, można też patrzeć szerzej, nie ograniczając się jedynie do RODO[32]. Źródłem uprawnień branych pod uwagę przy okazji dokonywania ocen na gruncie RODO mogą być też inne akty prawne, takie jak KPP UE[33], Konstytucja RP[34]. Prawdopodobnie wszystkie uprawnienia wynikające z KPP UE wypisałem w innej książce[35], będącej częścią cyklu, nie uważam jednak za celowe branie ich pod uwagę przy dokonywaniu oceny ryzyka, niezależnie od tego, czy za jej źródło przyjmiemy art. 24 ust 1 RODO, czy art. 32 ust. 1 RODO. Nie uważam za celowe z bardzo prostego powodu, otóż uprawnienia te, z małym wyjątkiem, nie mają wiele wspólnego z ochroną danych osobowych, z RODO czy z prywatnością, branie zaś pod uwagę kolejnych praw tylko po to, by stwierdzić, że prawdopodobnie nie są zagrożone przy wykonywaniu tej czy innej czynności, uważam właśnie za niecelowe.

Poza tym, traktowanie praw i wolności wynikających z RODO jako najważniejszych w kontekście art. 24 i art. 32 RODO oraz art. 33 RODO i art. 34 RODO, jest uzasadnione z punktu widzenia dyrektywy języka prawnego[36].

Zestawienia praw i wolności zamieszczone są na końcu książki w części zatytułowanej: *Tabele pomocnicze, zestawienia*. Dla zachowania kompletności wywodu, poniżej umieszczam przykładowe prawa i wolności, z podziałem na zasadnicze i szczegółowe. Prawa i wol-

---

[32] Por. K. Wygoda, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie*..., s. 287–288.

[33] *Karta Praw Podstawowych Unii Europejskiej*. Dz.Urz. UE 2016 C 202, s. 1.

[34] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r*. Dz.U. 1997 nr 78, poz. 483 ze zm.

[35] J. Rzymowski, *RODO – GDPR. Przedmiot i cele*...

[36] L. Morawski, *Zasady wykładni prawa*, Toruń 2006, s. 93–95.

ności, które wynikają z KPP UE, zamieszczone są w innej książce[37] z niniejszego cyklu. Prawa i wolności zasadnicze i szczegółowe zostały również zestawione w tej samej książce.

W poświęconej ryzyku publikacji, wydanej przez PUODO znajduje się zdanie, które zawiera wartościową myśl, zdanie to brzmi: *[...] oceniając ryzyko naruszenia praw i wolności osób, których dane dotyczą, osoby odpowiedzialne za przeprowadzenie tego procesu powinny przyjąć perspektywę osób, których dane są przetwarzane i właśnie z tej perspektywy oceniać stopień dotkliwości w przypadku zmaterializowania się zagrożenia*[38].

Współgra to z podejściem, przyjąwszy, że administrator analizuje, czy zostało naruszone prawo do przetwarzania danych osobowych w sposób rzetelny, w sposób zgodny z prawem, w sposób ograniczony co do zakresu itd. Niestety wydaje się, że o ile cytowane zdanie pasuje do przyjętej przeze mnie koncepcji prowadzenia oceny ryzyka, o tyle koncepcja PUODO jest prawdopodobnie inna, ponieważ w zdaniu poprzedzającym zdanie cytowane czytamy: *[...] nieuprawniona modyfikacja danych lub niedostępność danych w wyniku złego ich zabezpieczenia może skutkować utratą zdrowia, a nawet życia*[39].

Dramatyczna wizja PUODO, kiedy ktoś zmienia dane medyczne, a ktoś inny wskutek tego umiera, przemawia do wyobraźni, ale jest niepotrzebna. Jeżeli ktoś zmienia dane w sposób nieuprawniony, to na pewno narusza prawo do przetwarzania danych osobowych w sposób zgodny z prawem, prawo do przetwarzania danych osobowych w sposób ograniczony co do zakresu i prawo do przetwarzania danych osobowych w sposób integralny oraz prawo do przetwarzania danych osobowych w sposób poufny. Wskazane prawa zostają naruszone. Jeżeli zatem z oceny ryzyka wynika wysokie lub średnie (podstawowe) prawdopodobieństwo naruszenia wskazanych praw, to trzeba to prawdopodobieństwo obniżyć. Jeśli dane nie zostaną ujawnione, to nie zostanie naruszone prawo do przetwarzania danych osobowych w sposób zgodny z prawem, prawo do przetwarzania danych osobowych

---

[37] J. Rzymowski, *RODO – GDPR. Przedmiot i cele*...

[38] A. Kaczmarek, M. Młotkiewicz, A. Łapińska, A. Miłocha, M. Mazur, *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1,* Warszawa 2018, s. 7.

[39] Ibidem.

w sposób ograniczony co do zakresu oraz prawo do przetwarzania danych osobowych w sposób poufny. Jeśli nikt nie zmodyfikuje danych w sposób nieuprawniony, ponieważ administrator zabezpieczy dane przed taką modyfikacją, to nie nastąpi naruszenie prawa do przetwarzania danych osobowych w sposób integralny. Kto zapozna się z danymi w sposób nieuprawniony i co z uzyskaną wiedzą zrobi, jest dla naruszenia i dla potencjalnego naruszenia, drugorzędne, ważne, że się ktoś zapoznał lub mógł zapoznać. Można zaryzykować tezę, że prawa zasadnicze stoją niejako „przed" innymi prawami. Jeżeli zostanie naruszone inne prawo niż jedno z praw zasadniczych, to (sic!) któreś z praw zasadniczych zostanie tym samym również naruszone. Prowadzi to do prostego wniosku, że należy szukać naruszeń lub zagrożenia naruszeniami, właśnie praw zasadniczych.

Pewną nadzieję na zrozumienie zagadnienia w PUODO dają przykłady ocen. Co prawda PUODO umieściło przykłady dotyczące oceny skutków naruszenia, czyli pasujące do art. 33 RODO i art. 34 RODO w poradniku poświęconym ocenie ryzyka, czyli art. 24 RODO i art. 32 RODO, ale należy docenić, że zagadnienia są pokrewne, że jednak nieco zrozumieli, choć przykro to napisać, kiedy uświadomimy sobie, że ten urząd nakłada kary na gruncie RODO. „Nieco" jako ocena poziomu rozumienia to w tym wypadku „za mało".

Przykład 1. W wyniku włamania na niewystarczająco zabezpieczony serwer poczty elektronicznej korespondencja prywatna użytkownika X z osobą Y została pozyskana przez osobę Z, która wykorzystała zdobyte informacje do czerpania korzyści finansowych, szantażując adresata i nadawcę wiadomości upublicznieniem informacji – naruszenie prawa do ochrony danych osobowych, prawa do prywatności oraz wolności i prawa do tajemnicy komunikowania się[40].

Prawdą jest, że następują tu naruszenia wskazanych praw, ale w podanym przez PUODO przykładzie następują też naruszenia wymienionych poniżej praw:

– Prawo do przetwarzania danych osobowych w sposób zgodny z prawem, ponieważ przetwarzanie przez naruszyciela nie mieści się w warunkach zgodności z prawem przetwarzania danych osobowych z art. 6 ust. 1 RODO.

[40] Ibidem, s. 10.

– Prawo do przetwarzania danych osobowych w sposób ograniczony co do zakresu, ponieważ przetwarzanie danych osobowych przez naruszyciela na pewno nie jest niezbędne do osiągnięcia celu przetwarzania przez administratora.
– Prawo do przetwarzania danych osobowych w sposób poufny, ponieważ naruszyciel nie był osobą uprawnioną do dostępu do danych osobowych

Przykład 2. W wyniku słabo zabezpieczonej ciągłości działania systemu bankowego, użytkownik X – na skutek niedostępności tego systemu – nie mógł dokonać transakcji finansowej na giełdzie w określonym czasie – naruszenie prawa do ochrony danych osobowych oraz prawa własności[41].

I znów prawdą jest, że naruszone zostaje prawo do ochrony danych osobowych, choć przyznam, że spokojniejszy bym był, gdyby PUODO zdefiniowało treść tego prawa. O ile jasne nie wymaga wyjaśnień, o tyle przyznam, że dla mnie treść tego prawa jasna nie jest, zwłaszcza w kontekście naruszenia. Poza tym naruszone zostają trzy prawa zasadnicze.

– Prawo do przetwarzania danych osobowych w sposób zgodny z prawem, ponieważ przetwarzanie danych osobowych w ten sposób, że administrator nie ma do nich dostępu w wyniku działań osoby trzeciej, na pewno nie mieści się w warunkach zgodności z prawem przetwarzania danych osobowych z art. 6 ust. 1 RODO.
– Prawo do przetwarzania danych osobowych w sposób ograniczony co do zakresu. Tu naruszenie jest ciekawe, bo zwykle dane są lub mogą być przetwarzane ponad zakres, tu przetwarzanie niezbędne do osiągnięcia celu zostało uniemożliwione.
– Prawo do przetwarzania danych osobowych w sposób integralny, bo pewne cechy danych zostały zmodyfikowane – dostępność.

Odchodząc na moment od art. 24 RODO, gdyby opisane zdarzenie miało być kwalifikowane przez pryzmat art. 33 RODO i art. 34 RODO, to byłby z tym problem. Tam kwalifikujemy zdarzenie, które jest naruszeniem na podstawie art. 4 pkt 12 RODO. Opisane zdarzenie raczej takim naruszeniem nie jest, chyba że uznamy, że jest przypadkowym (niezgodnym z prawem) zmodyfikowaniem danych osobowych przechowywanych. Zachodzi tu ciekawe zjawisko, zdarzenie

[41] Ibidem.

jest niekorzystne, należy przed nim zabezpieczać, ale raczej nie jest naruszeniem na gruncie art. 4 pkt 12, co uniemożliwia kwalifikację na gruncie art. 33 RODO i art. 34 RODO.

Nieco niepokoi stwierdzenie, że naruszono prawo własności. O ile przy ocenie skutków naruszenia (a po prawdzie, taką właśnie zaprezentowało PUODO, miast oceny ryzyka) stwierdzenie, że naruszono takie prawo ma sens (powiedzmy), o tyle, przy ocenie ryzyka jest to mocno problematyczne. W sytuacji gospodarki wolnorynkowej, powszechnego zjawiska swobody umów, ogromnej ilości czynności wykonywanych przez organy administracji na życzenie osób fizycznych, takich szczegółowych uprawnień można skonstruować, wydestylować z systemu prawa dosłownie tysiące.

Niepokoi mnie to z dwóch powodów:

– po pierwsze, nie jest jasne, które prawa brać pod uwagę;
– po drugie, niezależnie od tego, które prawa wzięto pod uwagę przy dokonywaniu oceny ryzyka, PUODO może zarzucić, że wzięto pod uwagę te niewłaściwe, bo administrator (nieco przesadzając) oceni ryzyko naruszenia 500 (sic!) praw, a PUODO stwierdzi, że jednak jeszcze jednego, bardzo ważnego nie oceniono.

Koncepcja oparta na prawach zasadniczych z art. 5 RODO zmniejsza ten niepokój, ponieważ jeżeli administrator bierze pod uwagę prawa zasadnicze, to za administratorem stoi autorytet prawodawcy i powaga zasad wykładni prawa. Niestety widać, że PUODO idzie w tym kierunku powoli i bardzo małymi krokami.

PUODO posługuje się pojęciem „prawa i wolności", „prawa lub wolności", jednak jeśli chodzi o konkretne prawa (i konkretne wolności), to brak jest zdecydowanego stanowiska na temat tego, jakie to dokładnie prawa i wolności należy brać pod uwagę przy ocenianiu ryzyka na gruncie art. 24 RODO i art. 25 RODO. Wskazanie praw i wolności w przykładach wziętych z poradnika cieszy tylko trochę, czego powody opisałem, prócz tego autorom poradnika wyraźnie pomyliła się ocena z art. 24 RODO i 25 RODO z oceną (po naruszeniu ochrony danych osobowych) z art. 33 RODO i art. 34 RODO. Przyznam, że ta pomyłka poważnie mnie niepokoi. Gdyby PUODO było studentem piszącym pracę magisterską z prawa, to usłyszałoby zarzut słabego opanowania materiału prawnego, będącego przedmiotem pracy. PUODO studentem nie jest. PUODO m.in. nakłada kary. Dlatego takie szcze-

góły mnie niepokoją, o czym piszę wyżej. Słowa te mogą wydawać się nadmierne, ale uważam, że jako badacz prawa, naukowiec, dydaktyk – nie mogę zamykać oczu, by nie zauważyć, że król może nie jest nagi, ale na pewno jest ubrany bardzo niekompletnie.

3.2. Art. 24 Uwaga 2

Przykładowe prawa i wolności zasadnicze[42]

Przypominam, że prawa i wolności zasadnicze to prawa i wolności wynikające z zasad z art. 5 RODO, czy też zapisane w tych zasadach. Oczywiście między stwierdzeniem, że prawo z zasady wynika, a że prawo jest w zasadzie zapisane, jest poważna różnica. Pierwsze sugeruje pozytywizm prawniczy, drugie jest bliższe koncepcjom prawnonaturalnym. Bliższy jest mi pozytywizm, acz z pewnymi ograniczeniami, jednak nie uważam, by dla potrzeb prowadzonych tu rozważań, czynienie takich zastrzeżeń było kluczowe, wspominam o tym jedynie dla porządku. Niżej wymieniam przykładowe prawa i wolności zasadnicze. Wszystkie wymienione są na końcu książki w części: *Tabele pomocnicze. Zestawienia*.

– Prawo do przetwarzania danych osobowych w sposób zgodny z prawem.
– Wolność od przetwarzania danych osobowych w sposób niezgodny z prawem.

– Prawo do przetwarzania danych osobowych w sposób rzetelny.
– Wolność od przetwarzania danych osobowych w sposób nierzetelny.

– Prawo do przetwarzania danych osobowych w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania.
– Wolność od przetwarzania danych osobowych w sposób nieograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania.

Nieco inne, choć zbliżone, stanowisko prezentują[43] autorzy czeskiego komentarza do RODO. Wskazują oni na zagrożenie jako na mo-

[42] J. Rzymowski, *RODO – GDPR. Przedmiot…*, s. 79–83.

żliwość naruszenia zasad z art. 5 RODO, jednak zestawienie nie zawiera wszystkich zasad, a co więcej, zasady są w nim wymieszane z przepisami szczegółowymi. Czescy autorzy zwracają zatem uwagę na:
– zasadę zgodności z prawem,
– zasadę ograniczenia celu,
– zasadę minimalizacji,
– zasadę ograniczenia przechowywania (w dwóch jej przejawach),
– zasadę integralności.

Nieco niepokoi, że czescy autorzy nie odnoszą się wprost do wskazanych tu przeze mnie zasad, ale odnoszą się do nich opisowo. Jeżeli pamiętamy o nieostrych definicjach zasad w RODO, to podejście takie nie wydaje się niewłaściwe, jednak w wywodzie, w którym mówi się o zasadach, ich nazwy wspomniane być powinny. Dodatkowo czescy autorzy wskazują na niewłaściwe przetwarzanie danych osobowych, przekraczające rozsądne oczekiwania osób, których dane dotyczą i na uniemożliwienie realizacji praw osób, których dane dotyczą. Dlaczego te dwie kategorie zagrożeń są wymieszane z zasadami, tego nie wiem. Być może autorzy kojarzyli pierwsze z zagrożeń z zasadą minimalizacji, a drugie z zasadą rzetelności i zasadą przejrzystości, co czyniłoby ich wywód spójnym. Pomijając precyzję i ewentualną drobną niespójność wywodu czeskich autorów, dostrzegam u nich tę samą myśl, do której i ja doszedłem. Zagrożenie naruszeniem praw i wolności to zagrożenie naruszeniem zasad z art. 5 RODO.

Andrzej Krasuski również – jak widać z jego książki – zgadza się z wyłożoną tu koncepcją wiążącą prawa z art. 5 RODO, czytamy u niego bowiem, że: *Prawa osób fizycznych zostały odzwierciedlone w zasadach przetwarzania danych osobowych, które zostały wyrażone w art. 5 ust. 1 RODO. W zasadach przetwarzania danych osobowych zostały określone obowiązki prawne […] spoczywające na podmiotach przetwarzających dane osobowe, którym odpowiadają prawa osób fizycznych, których dane są przetwarzane. Co do zasady adresatem tych obowiązków jest administrator, przy czym obowiązki dotyczące zapewnienia poufności przetwarzanych danych osobowych[…] odnoszą się również do podmiotu przetwarzającego […] w treści art. 32 RODO[…].*

[43] M. Nuličeк, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit., s. 250–251.

Obowiązkom administratora odpowiadają prawa osób fizycznych, których dane osobowe są przetwarzane[44]. Nie odnoszę się do słów A. Krasuskiego, a jedynie je cytuję, dostrzegam w nich bowiem tezy, które również sam, też w niniejszej książce, stawiam.

Niestety dalej A. Krasuski pisze rzecz niezwykłą.[45] Zrazu wymienia zasady, w czym nie byłoby nic dziwnego, niestety wymienia jedynie cztery spośród nich, czego, przyznam, nie rozumiem. Dalej jednak wskazany autor wywodzi na temat praw wskazanych również w innych niż art. 5 przepisach RODO[46], co jest w znacznej mierze zbieżne z koncepcją praw i wolności szczegółowych, zasygnalizowaną przeze mnie poniżej.

Cieszy mnie, że T. Izydorczyk, podobnie jak ja, uważa, że w zasadach z art. 5 RODO zapisane są prawa i wolności osób, których dane dotyczą. Mój pogląd na temat stanowiska wskazanego autora wyrobiłem sobie po wielokrotnej lekturze tabeli, w której T. Izydorczyk dokonuje niezwykłego zestawienia. Tabela nosi tytuł: *Porównanie podstawowych zasad przetwarzania z punktu widzenia ryzyka praw lub wolności opartego wyłącznie na skutkach dla podmiotów danych*[47]. W opisywanej tabeli wskazany autor w wierszu nagłówkowym wypisał skrócone nazwy zasad, to jest: Zgodność z prawem, Rzetelność, Przejrzystość, Ograniczony cel, Minimalizacja, Prawidłowość, Ograniczenie czasowe, Integralność, Poufność i jednocześnie w kolumnie o charakterze nagłówkowym, w pierwszej kolumnie po lewej stronie autor wypisał dokładnie to samo.

Trudno powiedzieć, czy zasady w tabeli, do której się odnoszę, wypisane są pionowo, a prawa i wolności poziomo, czy zasady wypisane są poziomo, a prawa i wolności pionowo, ponieważ tego autor w tabeli nie wskazał, bądź ja czegoś nie zrozumiałem, jednak dla prowadzonych tu rozważań ważne jest co innego. Otóż ze wskazanej tabeli wynika, że zasady z art. 5 RODO to są właśnie prawa i wolności. Naukowo cieszę się, że T. Izydorczyk tak uważa. Jednocześnie spo-

---

[44] A. Krasuski, [w:] A. Krasuski, P. Siembida. *Analiza ryzyka w ochronie danych osobowych,* Warszawa 2022, s. 94.

[45] Ibidem, s. 94–95.

[46] Ibidem, s. 95–98.

[47] T. Izydorczyk, [w:] *Ochrona danych osobowych. Ocena ryzyka i skutków. Metody i praktyczne przykłady*. red.: M. Gumularz, T. Izydorczyk, Warszawa 2021, s. 144.

sób prezentacji (mimo pewnej niejasności przekazu zawartego w tabeli) powoduje, że tekst T. Izydorczyka niejako potwierdza moje wywody prowadzone w książce wydanej w 2020 roku[48]. Twierdzę tak, ponieważ nie odnajduję w tekście T. Izydorczyka odesłania do mojej książki, mam więc podstawy by domniemywać, że T. Izydorczyk do tych samych wniosków co ja, a przynajmniej do wniosków bardzo analogicznych, doszedł samodzielnie, ewidentnie bez inspiracji moim tekstem, co mnie cieszy.

3.3. Art. 24 Uwaga 3

Przykładowe prawa i wolności szczegółowe[49]

Przypominam, że prawa i wolności szczegółowe to prawa i wolności wynikające z przepisów szczegółowych RODO czy też zapisane w tych przepisach.

Co ciekawe, M. Sakowska-Baryła hołduje, jak się wydaje koncepcji, zgodnie z którą z poszczególnych przepisów RODO wynikają prawa. U autorki tej czytamy bowiem, w kontekście omawiania art. 34 RODO, że: *Z obowiązkiem administratora wynikającym z komentowanego przepisu sprzężone jest prawo osoby, której dane dotyczą, do uzyskania informacji o naruszeniu ochrony danych osobowych*[50]. I gdyby tego nie było dość, dalej czytamy: *Z jednej strony bowiem administrator powinien dokonać zawiadomienia, z drugiej zaś osoba, której dane dotyczą, ma prawo dowiedzieć się, że do takiego naruszenia doszło […]*[51]

– **Prawo** do przetwarzania danych osobowych w sposób zgodny z prawem.
  Wolność od przetwarzania danych osobowych w sposób niezgodny z prawem.

---

[48] J. Rzymowski, *RODO – GDPR. Przedmiot…,* s. 78–118.

[49] Ibidem, s. 95–102.

[50] M. Sakowska-Baryła, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 374.

[51] Ibidem, s. 374, podobnie: s. 376.

– **Prawo** do bycia poinformowanym o celu przetwarzania innym niż cel, w którym dane osobowe zostały zebrane, przysługujące osobie, której dane dotyczą.
Wolność od przetwarzania danych osobowych w warunkach, w których osoba, której dane dotyczą, nie jest poinformowana o celu przetwarzania innym niż cel, w którym dane osobowe zostały zebrane

– **Prawo** do przetwarzania danych osobowych przy uwzględnieniu ochrony danych w ustawieniach domyślnych, przysługujące osobie, której dane dotyczą.
Wolność od przetwarzania danych osobowych bez uwzględnienia ochrony danych w ustawieniach domyślnych.

Analogiczne podejście, zbliżone do „praw i wolności szczegółowych", o których tu piszę, dostrzegam u P. Siembidy, który – co prawda nie wypowiada się w sferze praw i wolności – wymienia[52] jednak 29 obowiązków administratora danych, które wynikają z poszczególnych przepisów RODO. Szkoda, że co A. Krasuski na stronie 94 książki napisanej z P. Siembidą zauważył, tego P. Siembida na stronie 239 tej samej książki nie zauważył.

Jeszcze bliższe mojemu podejściu ujęcie proponują M. Gumularz i T. Izydorczyk[53]. Podejście M. Gumularza i T. Izydorczyka jest niewątpliwie ich podejściem oryginalnym, nieinspirowanym moją koncepcją, choć moja książka pochodzi z roku 2020, a książka wskazanych autorów z roku 2021, to jednak nie znajduję u M. Gumularza i T. Izydorczyka przypisu, który wskazywałby na ewentualną inspirację. Ponadto przedstawiają oni tabelę, w której zestawiają kolejne prawa, przysługujące osobie, której dane dotyczą i choć zestawienie to jest trafne, to jednak autorzy podchodzą do praw osoby, której dane dotyczą, w sposób nieco uproszczony, widzą bowiem prawa tylko w Rozdziale III RODO, pomijając fakt, że tam gdzie w przepisie zapisany jest obowiązek, tam zawarte w nim jest też prawo, co omawiam szerzej w uwagach (*3.25. Art. 24. Uwaga 25, Przepis jako zapis prawa, obowiązku i wolności. Argument z racjonalności prawodawcy*),

[52] P. Siembida, [w:] A. Krasuski, P. Siembida, *Analiza ryzyka…*, s. 239–240.

[53] M. Gumularz, T. Izydorczyk, op. cit., s. 74–77.

(*3.26. Art. 24. Uwaga 26. Przepis jako zapis prawa, obowiązku i wolności. Argument z autorytetu*), (*3.27. Art. 24. Uwaga 27. Przepis jako zapis prawa, obowiązku i wolności. Argument z filozofii*). Mimo niedostatków podejścia M. Gumularza i T. Izydorczyka, wskazuję tu na ich publikację, widzę bowiem, że myśl nasza szła tym samym torem, choć nie jechaliśmy tym samym pociągiem.

Trafną myśl, bliską poruszanych tu zagadnień sformułował A. Mednis, u którego czytamy, że: *[...] ryzyko dla praw i wolności powinno być oceniane niezależnie od wielkości administratora czy podmiotu przetwarzającego*[54]. Wskazany autor myśl tę sformułował w odniesieniu do małych i średnich przedsiębiorstw, uważam jednak, że ma ona wartość uniwersalną.

Koncepcję praw i wolności oraz obowiązków zasadniczych i korespondujących z nimi praw i wolności i obowiązków szczegółowych wyłożyłem w 2020 roku w książce *Przedmiot i cele, zakresy, prawa i wolności, definicje*. Mam poczucie, że koncepcja ta została przyjęta przez polską naukę prawa, przynajmniej w zakresie prawa ochrony danych osobowych. Argumenty przemawiające za tym stanowiskiem wynikają z książki A. Krasuskiego i P. Siembidy[55] (piszę o tym wyżej w *3.2. Art. 24 Uwaga 2. Przykładowe prawa i wolności zasadnicze*) ze wskazanych wyżej rozważań T. Izydorczyka i M. Gumularza, ale też z książki Ch. Poszwińskiego, co niżej ilustruję cytatem. Autor ten całą swoją książkę zbudował, opierając się na schemacie, którego podstawą jest właśnie to, co ja nazywam prawami i wolnościami szczegółowymi. Ograniczę się do zacytowania fragmentów spisu treści książki wskazanego autora, poświęconej ryzyku, w spisie treści znajdujemy więc:

– *Prawo do przejrzystego informowania i przejrzystej komunikacji*.
– *Prawo do bycia poinformowanym w przypadku zbierania danych od osoby, której dane dotyczą*.
– *Prawo do bycia poinformowanym w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą*.

---

[54] A. Mednis, *Pierwsza ocena i przegląd RODO – stanowiska zainteresowanych i główne elementy sprawozdania Komisji Europejskiej*, [w:] *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020* pod red. G. Sibigi. Dodatek specjalny do „Monitora Prawniczego" 2020, nr 23, s. 8.

[55] A. Krasuski, op. cit., s. 95–98.

– *Prawo dostępu przysługujące osobie, której dane dotyczą*[56].

Nie wymieniam kolejnych praw wskazanych przez Ch. Poszwińskiego, nie widzę bowiem sensu w przepisywaniu spisu treści książki, zwracam jednak uwagę, że w samym spisie treści, wskazany autor umieścił 15 praw. Prawa te skorelowane są z konkretnymi przepisami RODO. Podejście to pokrywa się z podejściem, które wyłożyłem we wspomnianej już książce, wydanej w 2020 roku, czyli w: *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*[57]. Wobec braku wskazań na moje publikacje, muszę jednocześnie przyjąć, że wszyscy wskazani autorzy do stanowiska, o którym tu piszę, doszli sami. Cieszy mnie to podwójnie, oznacza bowiem, że sformułowano nie jedno, ale cztery (J. Rzymowski, A. Krasuski i P. Siembida, M. Gumularz i T. Izydorczyk, Ch. Poszwiński) stanowiska, które są tak bliskie sobie, że niemal się pokrywają. Możliwe jest też oczywiście, że wymienieni autorzy inspirowali się wzajemnie, tego nie śledziłem, mogę jednak, z pewnością podkreślić, że stanowisko moje nie było inspirowane stanowiskiem wskazanych autorów, na co wskazują względy temporalne.

3.4. Art. 24 Uwaga 4

Inne prawa i wolności

Piszę wyżej, że praw i wolności pod kątem wykonywania ocen ryzyka, można doszukiwać się też w innych źródłach niż RODO, między innymi w KPP UE. Wyżej (*3.1. Art. 24 Uwaga 1. Prawa i wolności*) wyjaśniam, dlaczego nie uważam za celowe brania pod uwagę wszystkich praw i wolności z KPP UE do ocen ryzyka na gruncie RODO. Pewne jednak prawa i wolności zapisane w KPP UE mają związek z ochroną danych osobowych. Wymieniam je poniżej wraz ze wskazaniem konkretnych przepisów, w których są zapisane.

Wskazane poniżej prawa i wolności można – pod względem redakcyjnym, edytorskim, pod względem ich sformułowania – wyrazić inaczej, należy jednak pamiętać, że inne sformułowanie tego czy innego prawa, to jedynie zmiana o charakterze językowym.

---

[56] Ch. Poszwiński, op. cit., s. 5–9. Spis treści obejmuje strony 5–9, cytowane pozycje znajdują się na stronach 5–6.

[57] J. Rzymowski, *RODO – GDPR. Przedmiot…*, s. 79–104.

– **Prawo** człowieka do poszanowania życia prywatnego i rodzinnego.
Wolność od nieposzanowania prawa do poszanowania życia prywatnego i rodzinnego. (Wolność od naruszeń życia prywatnego i rodzinnego.) (Art. 7 KPP UE)
– **Prawo** człowieka do poszanowania domu.
Wolność od nieposzanowania prawa do poszanowania domu (Wolność od naruszeń domu.) (Art. 7 KPP UE)
– **Prawo** człowieka do poszanowania komunikowania się.
Wolność od naruszeń prawa do komunikowania się. (Art. 7 KPP UE)
– **Prawo** człowieka do ochrony danych osobowych, które go dotyczą.
Wolność od nieposzanowania prawa do ochrony danych osobowych. (Art. 8 ust. 1 KPP UE)
– **Prawo** człowieka do przetwarzania danych osobowych w sposób rzetelny.
Wolność od przetwarzania danych osobowych w sposób nierzetelny. (Art. 8 ust. 2 KPP UE)
– **Prawo** człowieka do przetwarzania danych osobowych w określonych celach.
Wolność od przetwarzania danych osobowych w nieokreślonych celach. (Art. 8 ust. 2 KPP UE)
– **Prawo** człowieka do przetwarzania danych osobowych za zgodą osoby której dane dotyczą.
Wolność od przetwarzania danych osobowych bez zgody osoby, której dane dotyczą. (Art. 8 ust. 2 KPP UE)
– **Prawo** człowieka do przetwarzania danych osobowych na podstawie innej niż zgoda uzasadnionej podstawie prawnej przewidzianej ustawą.
Wolność od przetwarzania danych osobowych z naruszeniem prawa do przetwarzania danych osobowych na podstawie innej niż zgoda uzasadnionej podstawie prawnej przewidzianej ustawą. (Art. 8 ust. 2 KPP UE)
– **Prawo** człowieka do dostępu do zebranych danych osobowych, które go dotyczą.
Wolność od przetwarzania danych osobowych bez dostępu do zebranych danych osobowych, które człowieka dotyczą. (Art. 8 ust. 2 KPP UE)
– **Prawo** człowieka do dokonania sprostowania danych osobowych, które go dotyczą.

Wolność od przetwarzania danych osobowych bez poszanowania prawa do dokonania sprostowania danych osobowych, które człowieka dotyczą. (Art. 8 ust. 2 KPP UE)

Na prawo do ochrony danych osobowych zwracają uwagę D. Lubasz[58], P. Fajgielski[59] oraz autorzy poradnika PUODO[60].

Na fakt, że prawa wynikają również z innych aktów prawnych, nie tylko z RODO, zwraca uwagę A. Krasuski. Autor ten zrazu zwraca uwagę na Traktat o Unii Europejskiej i Traktat o Funkcjonowaniu Unii Europejskiej, dalej na Kartę Praw Podstawowych Unii Europejskiej, na Europejską Konwencję Praw Człowieka i w końcu na Konstytucję RP[61]. Zgadzam się z A. Krasuskim, że wskazane akty prawne zawierają czy też ustanawiają prawa. Absurdem byłoby twierdzenie przeciwne. Zgadzam się do tego stopnia, że we wcześniejszych książkach z cyklu, którego niniejsza jest częścią, sprawy te nawet do pewnego stopnia analizuję, zwracam jednak uwagę na jeden, wcale nie drobny, szczegół. Otóż większość uprawnień ustanowionych we wskazanych aktach prawnych nie ma z ochroną danych osobowych nic wspólnego.

Oczywiście nic nie stoi na przeszkodzie temu, by przy okazji oceniania ryzyka lub przy okazji oceniania skutków naruszenia brać te setki (tak, setki) praw pod uwagę, nie widzę jednak sensu w takim postępowaniu. Jeśli koniecznie brać pod uwagę prawa i wolności zapisane we wskazanych aktach, to uważam, że jedynie te nieliczne, które są związane z ochroną danych osobowych i z prywatnością. Ślad takiego poglądu widzę w wypowiedzi A. Krasuskiego na temat Konstytucji RP[62].

---

[58] Podobnie: D. Lubasz, [w:] *RODO Ogólne rozporządzenie o ochronie danych. Komentarz*, red. nacz. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M. Czerniawski, P. Drobek, U Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka, Warszawa 2018, s. 105.

[59] P. Fajgielski, *Prawo ochrony…*, s. 21.

[60] A. Kaczmarek, M. Młotkiewicz, A. Łapińska, A. Miłocha, M. Mazur, *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1,* Warszawa 2018, s. 4.

[61] A. Krasuski, op. cit., s. 98–112.

[62] Ibidem, s. 112–121.

3.5. Art. 24 Uwaga 5

Proporcjonalność środków w świetle zasady rozliczalności

Z art. 32 ust. 2 RODO wynika, że wdrażane przez administratora danych osobowych i przez podmiot przetwarzający *środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać*, mają być proporcjonalne do przetwarzania. Z art. 5 ust. 2 RODO wynika obowiązek wykazania realizacji zasad z art. 5 ust. 1 RODO. Zasady z art. 5 ust. 1 RODO są realizowane przez przepisy szczegółowe. Do wykazania realizacji zasad nie ma zatem innego narzędzia, jak tylko wykazanie realizacji odpowiednich przepisów szczegółowych. Artykuł 32 RODO konkretyzuje (na poziomie aktu prawnego) i realizuje (na poziomie stosowania aktu prawnego) zasadę poufności i zasadę integralności, aby zatem wykazać realizację tych zasad, administrator musi wykazać realizację art. 32 RODO. Elementem wykazania realizacji tego przepisu jest wykazanie, że środki są proporcjonalne do przetwarzania. Wydaje się, że administrator powinien zatem to ocenić. W gruncie rzeczy jest to proste. Rzecz opisuję w punktach poniżej.

– Najpierw administrator tworzy rejestr czynności przetwarzania danych osobowych.
– Następnie administrator ocenia ryzyko przetwarzania danych osobowych.
– Wskutek oceny ryzyka, administrator dysponuje informacjami o poziomie ryzyka w odniesieniu do konkretnych czynności.
– Tam, gdzie ryzyko jest nieakceptowalne, tam administrator je obniża za pomocą środków technicznych i organizacyjnych. Ryzyko nieakceptowalne to ryzyko wyższe niż niskie.
– Następnie administrator opisuje wprowadzone środki w ogólnym opisie technicznych i organizacyjnych środków bezpieczeństwa.

Należy zwrócić uwagę na jeden jeszcze aspekt odpowiedniości czy też proporcjonalności środków. Otóż proporcjonalność, odpowiedniość jest skalowalna, na co zwraca uwagę Ch. Docksey[63]. Skalowalna w tym sensie, że środki mające zapewnić zgodność z prawem przetwarzania i wykazanie tej zgodności administrator powinien dostosowywać do skali przetwarzania.

[63] Podobnie: Ch. Docksey, op. cit., s. 562.

3.6. Art. 24 Uwaga 6

Odpowiedniość polityki ochrony danych

W art. 24 ust. 2 RODO mowa jest o wdrożeniu przez administratora: *[...]* ***odpowiednich polityk*** *ochrony danych [...]* Należy się chwilę zatrzymać przy tym, co oznacza występujący w przepisie przymiot odpowiedniości polityki ochrony danych.

Polityka ochrony danych jest środkiem bezpieczeństwa, a dokładniej jednym ze środków technicznych i organizacyjnych, które może wdrożyć administrator, jeżeli uzna to za stosowne. Administrator wdraża ten środek – jak zresztą jakikolwiek inny – po to, aby obniżyć poziom ryzyka naruszenia praw i wolności osób fizycznych do poziomu akceptowalnego, czyli do poziomu niskiego. Odpowiednia polityka ochrony danych jest to zatem taka polityka, którą administrator uznaje za środek techniczny, który umożliwi obniżenie poziomu ryzyka naruszenia praw i wolności osób fizycznych do poziomu akceptowalnego. Innymi słowy, odpowiednia polityka to polityka, którą administrator (danych osobowych) wdraża po dokonaniu oceny ryzyka naruszenia praw i wolności osób fizycznych, o której to ocenie mowa jest w art. 24 ust. 1 RODO.

3.7. Art. 24 Uwaga 7

Charakter, zakres, kontekst i cele przetwarzania

W art. 24 ust. 1 RODO czytamy m. in.: *Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych [...]* Niestety fragment cytowanej części przepisu jest niezrozumiały.

Zrozumiałe są słowa o zakresie przetwarzania, celach przetwarzania oraz o ryzyku naruszenia praw i (sic!) wolności osób fizycznych. Słowa o charakterze i kontekście przetwarzania są, przynajmniej dla mnie, na gruncie informacji, jakie wynikają z RODO, zwłaszcza w wersji polskojęzycznej RODO, niezrozumiałe. Tym niemniej staram się poniżej ustalić znaczenie tych słów, dla jasności wywodu, w kolejnych uwagach. Najpierw odnoszę się do słów bardziej zrozumiałych, potem do mniej zrozumiałych.

3.8. Art. 24 Uwaga 8

Zakres przetwarzania

Odnosząc się do zakresu przetwarzania, można stwierdzić, że zapewne dotyczy on tego, jak szeroko dane są przetwarzane, czyli jakie dane i w jakim „zakresie", czyli jak wiele czynności na tych danych jest wykonywanych.

Jakie dane – zarówno w rozumieniu jakościowym – czyli jakie konkretnie dane, czy też kategorie danych, jak i w znaczeniu ilościowym – jaka ilość danych.

Przez zakres przetwarzania można też, jak się wydaje, rozumieć, czy administrator przetwarza tak zwane dane zwykłe, czy przetwarza dane szczególnych kategorii.

Niestety polskie tłumaczenie RODO zawiera w odniesieniu do słowa „zakres" niekonsekwencję translatorską. W wersji angielskiej w art. 24 ust. 1 RODO czytamy: *Taking into account the nature, scope, context and purposes of processing*, w wersji polskiej zaś czytamy *Uwzględniając charakter, zakres, kontekst i cele przetwarzania*. Znaczenia są tu na tyle zbliżone, że nie warto prowadzić dywagacji.

Niestety dalej, w art. 25 ust. 2 RODO w wersji angielskiej czytamy: *That obligation applies to the amount of personal data collected, the extent of their processing*, w wersji polskiej zaś czytamy *Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania*. W wersji polskiej mamy zatem w sąsiadujących przepisach „zakres" i „zakres", jednak w art. 25 ust. 2 RODO, „zakres przetwarzania" występuje obok „ilości zbieranych danych osobowych", co mogłoby prowadzić do wniosku, że „zakres […] przetwarzania" nie zawiera w sobie „ilości zbieranych danych osobowych", ponieważ pojęcia te występują obok siebie w tym samym przepisie. Do wniosku takiego prowadzi jednak lektura wersji polskiej RODO. Lektura wersji angielskiej do wniosku takiego nie prowadzi. W art. 24 ust. 1 RODO, co wskazałem wyżej, widnieje „scope", w art. 25 ust. 2 RODO widnieje „extent of their processing", czyli w wersji angielskiej „the amount of personal data collected" widnieje obok „the extent of their processing", jednak nie stoi to na przeszkodzie, by uznać, że zarówno „the amount of personal data collected", jak i „the extent of their processing" mieszczą się zakresem w „scope".

Niestety lektura wersji czeskiej również nie nastraja optymistycznie. W art. 24 ust. 1 RODO czytamy: *S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování*, w art. 25 ust. 2 RODO zaś czytamy: *Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování*. Jak widać, w jednym przepisie widnieje „rozsahu", a w drugim „množství shromážděných osobních údajů" i „rozsahu jejich zpracování" widnieją obok siebie, co prowadziłoby do wniosków analogicznych do tych, które można uzyskać z analizy wersji polskojęzycznej.

Ciekawa propozycja rozumienia pojęcia „zakres" i pozostałych pojęć zawartych w przepisie znajduje się w wydanym w 2020 roku dokumencie *Szablon raportu z procesu oceny skutków dla ochrony danych w Unii Europejskiej: propozycja. d.pia.lab Policy Brief*[64]. Dla jasności wywodu posługuję się wersją polskojęzyczną. Otóż pojęcie „Zakres" jest we wskazanym dokumencie rozszyfrowane na dwie kategorie pojęć „Skala (jak wiele? O jakim zasięgu?)" i „Czas (kiedy? Jak długo?)"[65] .

Kiedy analizuję zestawienie: charakter, zakres, kontekst i cele przetwarzania, to mam nieodparte wrażenie, że zakres przetwarzania to pojęcie, które można rozszyfrować jako: jakie konkretnie kategorie danych są przetwarzane, jak wiele tych danych jest i czy są to dane szczególnych kategorii lub dane dotyczące naruszeń prawa, czy tzw. dane zwykłe. Wrażenie to wynika z pewnej eliminacji, skoro cel to cel przetwarzania, skoro charakter to czynność, skoro kontekst to przetwarzanie jedynie przez administratora lub przez inne podmioty, np. przy zbieraniu danych, to dlaczego przy ocenie ryzyka nie ma miejsca na wzięcie pod uwagę kategorii danych. Dlaczego administrator, który ocenia ryzyko, nie ma brać pod uwagę tego, jakie dane przetwarza. Chyba powinien. Skoro zaś powinien, to zapewne kategorie przetwarzanych danych to właśnie zakres przetwarzania.

Można też wyprowadzić pogląd tyleż kompromisowy co salomonowy, że zakres przetwarzania to inne określenie kategorii prze-

[64] D. Kloza, A. Calvi, S. Casiraghi, S. Vazquez Maymir, N. Ioannidis, A. Tanas, N. Van Dijk, P. Uściński, M. Otmianowski (TRANS. 2021), *Szablon raportu z procesu oceny skutków dla ochrony danych w Unii Europejskiej: propozycja. d.pia.lab Policy Brief*. 2020 (1), s. 1–56.

[65] Ibidem, s. 8. Zachowuję w cytacie oryginalną ortografię i interpunkcję.

twarzanych danych, ilości przetwarzanych danych i czasu, przez jaki dane są przetwarzane.

Wydaje się, że takie salomonowe podejście bliskie jest K. Wygodzie. Autor ten wskazuje, że oceniając zakres czynności, nie należy ograniczać się *do zakresu przetwarzanych danych – ich kategorii*, ale że należy również uwzględniać czynności na danych[66], co niestety zbliża takie rozumienie znaczenia zakresu czynności do rozumienia charakteru czynności przyjętego przez tego samego autora. Możliwe jest, że K. Wygoda ma rację, ponieważ w przepisie mowa jest – co należy przyznać – o „zakresie przetwarzania", czyli o „zakresie czynności na danych", nie zaś o „zakresie danych osobowych".

3.9. Art. 24 Uwaga 9

Cele przetwarzania

Odnosząc się do celów przetwarzania, można stwierdzić, że jest to chyba najczytelniejszy fragment przepisu. Cele przetwarzania należy – jak się wydaje – rozumieć jako cele, w których administrator przetwarza dane osobowe.

Warto przy tym zwrócić uwagę na fakt, że cele przetwarzania, o których mowa w art. 24 ust. 1 RODO, powinny się pokrywać z celami przetwarzania, o których mowa w art. 13 ust. 1 lit. c RODO i w art. 14 ust. 1 lit. c RODO, i w art. 15 ust. 1 lit a RODO, i w art. 30 ust. 1 lit. b RODO. Cele przetwarzania, które widnieją w analizowanym przepisie to również te same cele, które widnieją w kontekście zasad: ograniczenia celu, prawidłowości, minimalizacji i przechowywania z art. 5 ust. 1 RODO. Cele przetwarzania widnieją również w art. 6 RODO, w art. 9, 11, 17, 18, 19, 23 RODO, w niektórych ze wskazanych przepisów po kilka razy. Cele przetwarzania napotykamy również w art. 25 ust. 1 RODO i to w złożeniu: *Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania*, w art. 27 ust. 2 lit. a RODO, analogicznie, w złożeniu: *przewarzania, które […] ze względu na swój charakter, kontekst, zakres i cele*. Szczególnie istotne jest, że cele przetwarzania widnieją w art. 32 ust. 1 RODO i to – na co zwracam uwagę – w złożeniu: *Uwzględnia-*

[66] K. Wygoda, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie…*, s. 286.

jąc stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, czyli w złożeniu pokrywającym się ze złożeniem w art. analizowanym, czym zajmuję się niżej w uwadze (*3.12. Art. 24. Uwaga 12. Ocena ryzyka naruszenia praw i wolności z art. 24 RODO, a ocena ryzyka naruszenia praw i wolności z art. 32 RODO*).

Nie wymieniam tu wszystkich wystąpień słowa „cele" w RODO, z uwagi na doniosłość tegoż wystąpienia zwracam jednak jeszcze uwagę, że „cele" widnieją w art. 35 RODO i to w złożeniu *[...] ze względu na swój charakter, zakres, kontekst i cele [...]* treściowa bliskość przepisów wskazuje tu, jak uważam na to, że znaczna cześć oceny skutków powinna pokrywać się z oceną ryzyka – ocena skutków jest szersza i ma inny cel niż ocena ryzyka.

3.10. Art. 24 Uwaga 10

Charakter przetwarzania

Charakter przetwarzania jest jedną z cech przetwarzania, które występują w omawianym przepisie i w innych przepisach, jednak jest to cecha niezrozumiała. W wersji anglojęzycznej widnieje *nature*, co jest, w zakresie nie pierwszych znaczeń, odpowiednikiem słownikowym słowa *charakter*. „Charakter przetwarzania" widnieje w kilku miejscach RODO, co istotne, widnieje w art. 32 ust. 1 RODO, który podobnie jak art. 24 RODO wspomina o ocenie ryzyka i to również w złożeniu: *charakter, zakres, kontekst i cele przetwarzania*. Niestety, prawodawca posługuje się tu wyrażeniem niejasnym. Wydaje się jednak, że z samego miejsca w przepisie można wywnioskować znaczenie słowa, otóż w wyliczeniu *charakter, zakres, kontekst i cele przetwarzania*, słowo „charakter" znajduje się na pierwszym miejscu. Być może odpowiedź na pytanie o to, czym jest charakter przetwarzania jest bardzo prosta, ponieważ być może mowa tu po prostu o „czynności przetwarzania". Jakieś założenie interpretacyjne trzeba przyjąć i trzymać się go w dalszych pracach. Założenie, zgodnie z którym charakter przetwarzania to po prostu czynność (nazwa czynności), jest funkcjonalnie do zaakceptowania. Czynność pochodząca z rejestru czynności przetwarzania danych osobowych (art. 32 RODO), będącego u konkretnego administratora podstawą wykonywanej oceny ryzyka. Mam świadomość, że w toku dochodzenia do tego wniosku słowo „może" wystąpiło dwa razy, nie ukrywam jednak, że wywód

jest tu możliwy do podważenia. Jest on taki, ponieważ przepis jest niejasny. Trudno jest w niebudzący wątpliwości sposób analizować niejasne przepisy.

Przez „charakter przetwarzania" można też rozumieć czynność i to rozumieć tak, jak czynności są wskazane w art. 32 ust. 2 RODO, czyli przesyłanie, przechowywanie i przetwarzanie w inny sposób niż przesyłanie lub przechowywanie.

Uwzględnienie czynności z rejestru czynności przetwarzania danych osobowych i uwzględnienie czynności z art. 32 ust. 2 RODO daje pewność realizacji obowiązku, niezależnie od tego, które z dwóch przyjętych znaczeń jest właściwe. Istnieje oczywiście ryzyko, że właściwe jest jakieś inne, nieodkryte jeszcze rozumienie znaczenia słów „charakter przetwarzania danych osobowych", jednak domniemanie racjonalności prawodawcy[67] skłania właśnie do wskazanych rozumień.

Pewną koncepcję interpretacyjną można znaleźć w dokumencie powstałym na Vrije Universiteit Brussel; w dokumencie tym widnieje *Nature (what types of processing operations?)*[68], w jego zaś polskiej wersji językowej widnieje *Charakter (jaki rodzaj operacji przetwarzania?)*[69]. Przechodząc mimo koszmarnego zwrotu „operacji przetwarzania", można uznać, że autorom dokumentu chodzi o rodzaj czynności, czyli najprawdopodobniej po prostu o czynność. Interpretacja ta jest mi bliska, ponieważ jest ona analogiczna do interpretacji, którą wskazuję wyżej i do której doszedłem na drodze wykładni przepisu.

Mam pełną świadomość słabości tego wywodu, jednak nie jestem chyba odosobniony w moich zmaganiach, przykładem może być tu niezwykle ciekawa i wartościowa książka pod redakcją M. Gawrońskiego[70], w której redaktor i współautorzy posługują się zwrotem „charakter prze-

---

[67] L. Morawski, op. cit., s. 159–162.

[68] D. Kloza, A. Calvi, S. Casiraghi, S. Vazquez Maymir, N. Ioannidis, A. Tanas, N. Van Dijk *(2020), Data protection impact assessment in the European Union: developing a template for a report from the assessment process. d.pia.lab Policy Brief, 2020(1), s.* 7.

[69] Ibidem, s. 8.

[70] Red. M. Gawroński, A.P. Czarnowski, M. Dominiak, A. Gawron, M. Gawroński, M. Kibil, K. Kloc, K. Kunda, P. Naklicka, Z. Piotrowska, P. Punda, M. Sztąberek, M. Wojtas, *RODO przewodnik ze wzorami*, Warszawa 2018, s. 123, 125, 136, 167, 263, 285, 292. Dalsze poszukiwania zarzuciłem.

twarzania", też w złożeniu: „charakter, zakres, kontekst i cele przetwarzania", jednak tego, czym jest ten charakter – nie rozszyfrowują.

Ciekawą uwagę znajdujemy u K. Wygody, który twierdzi, że charakter przetwarzania wiąże się *[...] raczej z przetwarzaniem jako takim, a nie z rodzajami czy kategoriami przetwarzanych danych*[71] osobowych. Dalej z wypowiedzi K. Wygody[72] wynika, że dzięki uwzględnieniu *charakteru przetwarzania* możliwa jest ocena *czynności/operacji przetwarzania pod kątem ich częstotliwości/cykliczności/długości okresu* wykonywania czynności, *skali* czynności, *narzędzi i technologii przetwarzania*, *podmiotów* wykonujących czynności.

Jak zatem widać, K. Wygoda uważa (chyba), że charakter przetwarzania to nic innego jak czynność.

3.11. Art. 24 Uwaga 11

Kontekst przetwarzania

Kontekst przetwarzania jest jedną z cech przetwarzania, które występują w omawianym przepisie i w innych przepisach, jednak jest to cecha podobnie niezrozumiała jak charakter przetwarzania. Problemy interpretacyjne z kontekstem przetwarzania są analogiczne wobec problemów interpretacyjnych z charakterem przetwarzania. Innymi słowy, niezależnie od wersji językowej, nie za bardzo wiadomo, jak słowo „kontekst" tu zinterpretować. Dla ukonkretnienia wywodu prezentuję poniżej wizję interpretacji przedstawioną na Vrije Universiteit Brussel. Otóż autorzy dokumentu, o którym tu piszę, wskazali[73] następująco: Kontekst (w jakich okolicznościach?). Pozycję tę podzielili następnie na dwie, a to:

– wewnętrzny (dotyczący administratora),
– zewnętrzny (dotyczący poszczególnych osób, grup, społeczeństwa itp.).

Nie wiadomo, czym jest wskazany w przepisie kontekst przetwarzania, w związku z tym przyjęcie założenia, że dzieli się on tak, jak wskazali badacze z Vrije Universiteit Brussel, jest racjonalne, aczkolwiek nieco niepokoi mnie druga część wyjaśnienia, przyjęta przez

[71] K. Wygoda, op. cit.

[72] Ibidem.

[73] D. Kloza, A. Calvi, S. Casiraghi, S. Vazquez Maymir, N. Ioannidis, A. Tanas, N. Van Dijk, P. Uściński, M. Otmianowski (TRANS. 2021), op. cit.

ekspertów z Brukseli. Gdyby pozostać przy tym podejściu, to widziałbym je nieco inaczej.

– Kontekst wewnętrzny – dane osobowe przetwarza jedynie administrator.
– Kontekst zewnętrzny – czynność przetwarzania zawiera w sobie element obcy wobec administratora, na przykład osoby, od których dane są zbierane, odbiorców, podmioty przetwarzające.

Zupełnie inne rozumienie pojęcia „kontekst przetwarzania" znajdujemy u K. Wygody, który przedkłada, że kontekst przetwarzania *wskazuje na konieczność odniesienia się do wszelkich okoliczności prawnych i faktycznych przetwarzania*[74].

Ciekawe podejście do kontekstu przetwarzania danych osobowych prezentuje A. Cieślik. Czynność, którą nazywa „ustanowieniem kontekstu", widzi jako pierwszą czynność w procesie zarządzania ryzykiem. Co dla mnie najciekawsze, wskazany autor prezentuje rysunek, zatytułowany: *Schemat kontekstu przetwarzania danych osobowych*. Rysunek ten składa się z czterech klocków czy też pól tekstowych, ułożonych w następującej, od góry patrząc, kolejności: *Przetwarzanie danych osobowych*, *Proces*, *Czynność*, *Operacja*[75]. Następnie wskazany autor na kilku stronach przygląda się przetwarzaniu danych osobowych, w tym prezentuje pokaźnych rozmiarów tabelę zatytułowaną: *Przykładowy opis procesu przetwarzania*[76], która to tabela jest w gruncie rzeczy przykładową pozycją z rejestru czynności przetwarzania danych osobowych, prowadzonego na podstawie art. 30 ust. 1 RODO, wzbogaconą o elementy nieobligatoryjne. Nie chcę tu prowadzić dyskursu z wywodami A. Cieślika, nie jest to moim celem, zwracam jednak uwagę, że na koniec wywodów o kontekście przetwarzania wskazany autor uzyskuje dwa punkty:

1) wykaz aktywów wspomagających,
2) wykaz czynności przetwarzania z przypisanymi poziomami klasyfikacji przetwarzanych danych osobowych[77].

---

[74] K. Wygoda, op. cit.

[75] A. Cieślik, *Ocena (szacowanie) ryzyka*, [w:] *Dokumentacja ochrony danych osobowych ze wzorami*. Red. n. Mariusz Jagielski, Warszawa 2022, s. 146.

[76] Ibidem, 151–154.

[77] Ibidem, 154 i 158.

Aktywa wspomagające to w ujęciu A. Cieślika techniczne i organizacyjne szczegóły przetwarzania danych osobowych, o czym wspominam jedynie dla porządku. Dla mojego wywodu istotne jest, że drugi z cytowanych elementów to wykaz czynności, który kilka stron wcześniej A. Cieślik nazywa „opisem procesów przetwarzania danych osobowych przez rejestr przetwarzania”[78]. Językowy koszmarek, który tu cytuję, ma swój szczególny urok, ale zostawiając to na boku, dostrzec należy, że elementem – jak uważam – dominującym kontekstu przetwarzania w ujęciu A. Cieślika jest przetwarzanie danych osobowych, czyli czynność na danych. Pomijając pojęciowo-definicyjne szamotanie wskazanego autora, widać, że przetwarzanie jest u A. Cieślika kluczem do kontekstu przetwarzania.

3.12. Art. 24 Uwaga 12

Ocena ryzyka naruszenia praw i wolności z art. 24 RODO, a ocena ryzyka naruszenia praw i wolności z art. 32 RODO

Na kolejnych stronach zestawiam art. 24 ust. 1 RODO z art. 32 ust. 1 RODO. Wnioski z zestawiania opisuję, najpierw jednak przepisy zestawiam w tabelach, uważam bowiem, że takie wręcz geometryczne zestawienie daje pogląd na zbieżności i różnice.

[78] Ibidem, s. 154.

Art. 24 ust. 1 RODO	Art. 32 ust. 1 RODO
Uwzględniając	Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz
charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze,	charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze,
administrator	administrator i podmiot przetwarzający
wdraża odpowiednie środki techniczne i organizacyjne,	wdrażają odpowiednie środki techniczne i organizacyjne,
aby	aby
przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać.	
Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.	
	zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku: a) pseudonimizację i szyfrowanie danych osobowych; b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

(Tabela z anglojęzycznymi wersjami przepisów znajduje się na kolejnej stronie.)

Art. 24 ust. 1 RODO	Art. 32 ust. 1 RODO
Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: a) the pseudonymisation and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Analiza porównawcza treści art. 24 ust. 1 RODO i treści art. 32 ust. 1 RODO prowadzi do bardzo ciekawych wniosków. Przepisy te wyglądają podobnie i nieuważna ich lektura może prowadzić do wniosku, że obydwa statuują ten sam obowiązek, a mianowicie obowiązek przeprowadzenia oceny ryzyka. Do wniosku takiego prowadzi jednak jedynie lektura nieuważna, lektura uważna prowadzi do wniosku całkiem innego.

Przede wszystkim należy się zastanowić, co łączy obydwa przepisy, a co różni.

Pierwszym elementem łączącym jest to, że w obydwu przepisach zapisany jest obowiązek uwzględnienia. Uwzględnienia okoliczności zapisanych w przepisie, tyle tylko, że okoliczności te jedynie do pewnego stopnia się pokrywają, jednak nie w całości.

Zarówno art. 24 ust. 1 RODO jak i art. 32 ust. 1 RODO nakazują uwzględnić: *charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze*[79]. To łączy przepisy. Nad tym, czym są *charakter zakres, kontekst i cele przetwarzania,* zastanawiam się wyżej w odpowiednich uwagach (*3.7. Art. 24. Uwaga 7. Charakter, zakres, kontekst i cele przetwarzania*), (*3.10. Art. 24. Uwaga 10. Charakter przetwarzania*) i (*3.8. Art. 24 Uwaga 8. Zakres*), (*3.11. Art. 24. Uwaga 11. Kontekst przetwarzania*) (*3.9. Art. 24. Uwaga 9. Cele przetwarzania*), tu zwracam szczególnie uwagę na fakt, że oba przepisy nakazują uwzględnić *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze*.

Kolejny fragment, który łączy przepisy, to fragment, w którym przepis nakazuje, by podmioty, które go stosują, wdrażały *odpowiednie środki techniczne i organizacyjne*. Również to łączy przepisy.

Pozostałe fragmenty obydwu przepisów jednak je dzielą, czy też odróżniają.

Artykuł 24 ust. 1 RODO nakłada obowiązki na administratora[80], art. 32 ust. 1 RODO nakłada obowiązki na administratora i na pod-

[79] W art. 24 ust. 1 RODO mowa jest o „różnym prawdopodobieństwie wystąpienia", a w art. 32 ust. 1 RODO mowa jest o różnym prawdopodobieństwie. Różnicę tę świadomie pomijam w wywodzie głównym, bo jest ona wyłącznie przejawem niekompetencji tłumacza i niedbalstwa ewentualnych redaktorów.

[80] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679…,* Kom. do art. 24.

miot przetwarzający[81]. Jest to różnica istotna, o której zwłaszcza podmioty przetwarzające pamiętać powinny, jest to jednak różnica istotna organizacyjnie. Merytorycznie istotniejsze są dalsze różnice.

Artykuł 32 ust. 1 RODO nakazuje administratorowi, by ten uwzględnił stan wiedzy technicznej i koszt wdrażania. Fragmentu tego nie ma w art. 24 ust. 1 RODO. Jak zatem widać, art. 32 skłania się nieco ku kwestiom technicznym.

Tym, co szczególnie różni obydwa przepisy, jest cel przeprowadzenia wskazanej w przepisie czynności, czyli „oceny ryzyka". Niżej wskazuję, jaki cel, z którego przepisu wynika.

– Z art. 24 ust. 1 RODO wynika, że celem jest, *aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać*.
– Z art. 32 ust. 1 RODO wynika, że celem jest, *aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku*, *w tym między innymi w stosownym przypadku:*
  a) pseudonimizację i szyfrowanie danych osobowych,
  b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
  c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
  d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Po zestawieniu przepisów w tabeli i omówieniu powyżej – pod tabelą, nie widzę sensu, by dalej zagadnienie, w zasadzie proste, w kształt słów ubierać. Jednocześnie chcę zwrócić uwagę na pewien wniosek, który nasuwa się po porównaniu przepisów. Artykuł 24 ust. 1 RODO nakazuje przeprowadzić ocenę po to, by przetwarzanie było zgodne z RODO. Artykuł 32 ust. 1 RODO nakazuje przeprowadzić ocenę po to, by dane osobowe były bezpieczne.

Z art. 24. ust. 1 RODO wynika zatem więc raczej nakaz przeprowadzenia audytu zgodności z RODO lub przeprowadzenia oceny działania administratora i obowiązek dbałości, *aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wyka-*

[81] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit., s. 291.

zać[82]. Z art. 32 ust. 1 RODO wynika raczej nakaz przeprowadzenia oceny ryzyka.

Przy stosunkowo dużym stopniu przylegania treści obydwu przepisów do siebie, nie ma raczej sensu przeprowadzania dwóch osobnych ocen ryzyka – odpowiednio po jednej do każdego przepisu. Nie ma sensu, chyba że administrator jest zwolennikiem przeprowadzania audytu przestrzegania RODO, co wydaje się podejściem jak najbardziej zalecanym. Wtedy jako podstawę do przeprowadzenia audytu (sprawdzenia) traktować należy art. 24 ust. 1 RODO.

Należy zwrócić tu uwagę na pewien jeszcze szczegół, otóż P. Litwiński, P. Barta i M. Kawecki piszą, że *[...] RODO nie zawiera [...] minimalnych wymagań w zakresie zastosowania środków zabezpieczenia danych, których spełnienie automatycznie powodowałoby uznanie, że działania administratora są zgodne z obowiązującymi przepisami w tym zakresie*[83]. Jest to w znacznym stopniu prawdą, ale:

– należy pamiętać, że RODO wymienia zagrożenia, ryzyka parametry oceny, czy jakkolwiek to nazwiemy, które należy brać pod uwagę przy wykonywaniu oceny ryzyka na podstawie art. 32 RODO, zawarte są one w art. 32 ust. 2 RODO;
– należy pamiętać, że ocena ryzyka z art. 32 RODO jest (nieco upraszczając) składową oceny ryzyka z art. 24 RODO (o ile na gruncie art. 24 RODO administrator przeprowadza ocenę ryzyka);
– należy pamiętać, że administrator, dokonując oceny ryzyka na gruncie art. 32 RODO, ma obowiązek wziąć pod uwagę parametry z art. 32 ust. 2 RODO, jeżeli tego nie uczyni, może liczyć się z odpowiedzialnością (co najmniej administracyjną).

Mając na uwadze powyższe, należy stwierdzić za wskazanymi autorami, że *[...] RODO nie zawiera [...] minimalnych wymagań w zakresie zastosowania środków zabezpieczenia danych, których spełnienie automatycznie powodowałoby uznanie, że działania administratora są zgodne z obowiązującymi przepisami w tym zakresie*[84]*,* ale za

[82] Podobnie: M. Gumularz, T. Izydorczyk, op. cit., s. 14.

[83] P. Litwiński, P. Barta, M. Kawecki, [w:] P. Litwiński (red.) P. Barta, M. Kawecki. *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 285.

[84] Ibidem.

to są elementy, których pominięcie przy ocenie ryzyka skutkuje automatycznie niezgodnością tej oceny z przepisami.

Na zbieżność treści art. 24 RODO i art. 32 RODO zwraca uwagę P. Fajgielski, który twierdzi[85] – z czym należy się zgodzić – że art. 32 RODO zawiera bardziej szczegółową regulację, w której doprecyzowano wymogi dotyczące bezpieczeństwa, z czym oczywiście również nie sposób się nie zgodzić.

Paweł Fajgielski nie prezentuje tak szczegółowej analizy jak powyższa, prezentuje jednak wniosek, który sprawia wrażenie, że analogiczną przeprowadził, twierdzi on bowiem, że *przewidziane w art. 24 wymogi nie ograniczają się jedynie do zabezpieczenia danych, ale obejmują także inne działania zmierzające do zapewnienia zgodności przetwarzania danych z przepisami RODO*[86]. Z tym poglądem również nie sposób się nie zgodzić.

Edyta Bielak-Jomaa i D. Lubasz trafnie zwracają uwagę, że dobrze przeprowadzona analiza ryzyka może przyczynić się do ograniczenia naruszeń w procesach przetwarzania danych osobowych[87]. Myśl ta tylko pozornie jest mało odkrywcza, ale kiedy uświadomimy sobie, że zagrożenia z art. 32 ust. 2 RODO (ocena ryzyka) to te same zjawiska, które konstytuują naruszenie ochrony danych osobowych na gruncie art. 4 pkt 12 RODO, kiedy przypomnimy sobie, że zarówno art. 32 ust. 1 RODO jak i art. 24 ust. 1 RODO, jak i art. 33 ust. 1 RODO, jak i art. 34 ust. 1 RODO odwołują się do tych samych praw i wolności (zapewne) zapisanych w art. 5 RODO, to dostrzeżemy przenikliwość i nieledwie geniusz tej myśli.

3.13. Art. 24 Uwaga 13

Artykuł 24 RODO a artykuł 32 RODO

Wyżej zastanawiam się nad relacją między art. 24 RODO a art. 32 RODO. Rzecz można ująć jeszcze inaczej, otóż można przyjąć, że obydwa przepisy dotyczą przeprowadzania oceny ryzyka, różni je cel przeprowadzania tej oceny.

---

[85] P. Fajgielski, op. cit.

[86] Ibidem.

[87] E. Bielak-Jomaa, D. Lubasz, op. cit., s. 57.

– Celem art. 24 RODO jest zgodność z RODO i możliwość wykazania tej zgodności[88].
– Celem art. 32 RODO jest zapewnienie stopnia bezpieczeństwa odpowiadającego ryzyku[89].

Zapewnienie odpowiedniego stopnia bezpieczeństwa (odpowiadającego ryzyku) jest elementem zgodności z RODO. W takim razie administrator, który wykonuje ocenę ryzyka z art. 32 ust. 1 i 2 RODO, wykonuje tym samym cześć oceny ryzyka z art. 24 ust. 1 RODO. Pozostaje mu zatem do wykonania ta część oceny ryzyka i wdrożenia środków, która nie dotyczy bezpieczeństwa przetwarzania danych osobowych.

3.14. Art. 24 Uwaga 14

Poziomy ryzyka

Prawodawca tylko pozornie nie wskazuje, jakie należy przyjmować poziomy ryzyka. Dokładnie wczytanie się w RODO pozwala te poziomy w RODO odnaleźć. Motyw 76 Preambuły RODO, na który wskazuje K. Wygoda[90], stanowi m.in., że *Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko*.

Jak zatem widać, napotykamy tu 2 poziomy ryzyka naruszenia praw i wolności, a to:
– ryzyko i
– wysokie ryzyko[91].

Skala dwustopniowa może się wydawać wystarczająca, ale warto zwrócić uwagę na fakt, że skoro zastanawiamy się tu nad ryzykiem naruszenia praw i wolności, to zapewne możliwe jest, że owe prawa i wolności zostają naruszone, a nie tylko zachodzi ryzyko ich naruszenia. W związku z tym należy wyróżnić jeszcze jeden poziom ryzyka, a mianowicie **ryzyko zrealizowane**. Zachodzi ono w sytuacji, kie-

---

[88] P. Barta, M. Kawecki, P. Litwiński, [w:] P. Barta, D. Dörre-Kolasa, M. Kawecki, A. Krzyżak, P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021, s. 283.

[89] Podobnie, choć nie było inspiracją: Ibidem.

[90] K. Wygoda, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie*..., s. 287.

[91] Podobnie: Ch. Poszwiński, op. cit., s. 35.

dy zdarzenie miało miejsce. Jeżeli patrzy się przez pryzmat art. 32 RODO, to ten poziom ryzyka wydaje się dziwny, jak bowiem można mówić o naruszeniu praw i wolności, kiedy nie ma jeszcze mowy o przetwarzaniu. Oczywiście przy okazji wykonywania oceny ryzyka na gruncie art. 32 RODO ten poziom ryzyka powinien być werbalizowany na przykład następująco:

– „**ryzyko, które zrealizuje się na pewno, jeżeli administrator rozpocznie przetwarzanie danych osobowych w dany sposób**".

Sytuacja upraszcza się, o czym piszę niżej, kiedy patrzymy przez pryzmat art. 33 i art. 34 RODO. Tam jest to po prostu „naruszenie praw i wolności", które zaszło w wyniku naruszenia ochrony danych osobowych.

Ocena ryzyka na gruncie art. 24 RODO i na gruncie art. 32 ust. 1 RODO ma charakter prewencyjny[92]. Administrator ocenia możliwe ryzyko, które wystąpi, czy też prawdopodobnie wystąpi, kiedy już administrator będzie przetwarzał dane osobowe. Ryzyko oceniane jest też na gruncie art. 33 RODO, art. 34 RODO. Administrator ocenia tam jednak ryzyko, które się zrealizowało wskutek naruszenia ochrony danych. Z art. 33 i 34 RODO wynikają poniżej poziomy ryzyka.

– **Ryzyko o małym prawdopodobieństwie naruszenia praw i wolności osób fizycznych**. Wnioskujemy o nim ze słów art. 33 ust. 1 RODO: *[...] chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych*.
– **Wysokie ryzyko naruszenia praw i wolności osób fizycznych**. Wnioskujemy o nim ze słów art. 34 ust. 1 RODO: *[...]wysokie ryzyko naruszenia praw lub wolności osób fizycznych*.

Nie sposób nie odnieść się tu do słów P. Litwińskiego, P. Barty i M. Kaweckiego, którzy twierdzą, że są tylko trzy poziomy ryzyka: *brak ryzyka – ryzyko – wysokie ryzyko*. Autorzy ci wywodzą, że *[...] małe* zagrożenie *naruszeniem praw i wolności osoby, której dane dotyczą [...] jest równoznaczne z brakiem ryzyka [...]*[93]. Nie znajduję w (nieprzytoczonych tu) wywodach wskazanych autorów, podstaw do takiego utożsamienia. Niskie ryzyko i brak ryzyka to dwa zupełnie od-

[92] K. Wygoda, op. cit., *s*. 284.

[93] P. Litwiński, P. Barta, M. Kawecki, [w:] P. Litwiński (red.) P. Barta, M. Kawecki, op. cit., s. 286.

mienne zjawiska. Jeżeli na przykład administrator przechowuje dane osobowe i nie czyni z nimi nic innego poza przechowywaniem i dane są doskonale zabezpieczone, to ryzyko ich zniszczenia jest niskie, ale ryzyko ich ujawnienia przy przesyłaniu nie zachodzi, nie ma go, nie istnieje – zachodzi w tym zakresie brak ryzyka. Zgadzam się jednak z poglądem wskazanych autorów w pewnym zakresie, otóż uważam, że możliwy jest poziom ryzyka wskazany poniżej.

– **Brak ryzyka naruszenia praw i wolności osób fizycznych**.

Zwracam przy tym uwagę, że „Brak ryzyka naruszenia praw i wolności osób fizycznych" jest różny zarówno od ryzyka o małym prawdopodobieństwie (art. 33 ust. 1 RODO), jak i od ryzyka o średnim poziomie (art. 33 RODO i motyw 76 Preambuły RODO). Należy zwrócić uwagę, że na drabinie ryzyka naruszenia praw i wolności „Brak ryzyka naruszenia praw i wolności osób fizycznych" znajduje się na najniższym z jej szczebli. Istnienie poziomu, który określamy nazwą „brak ryzyka", wynika – jak się wydaje – z faktu, że istnieje ryzyko o różnym poziomie.

Kiedy wyobrazimy sobie ryzyko jako pewien ciąg następstw, to ryzyka o coraz wyższym poziomie dążą do zrealizowania się ryzyka, a ryzyka o coraz niższym poziomie dążą do braku ryzyka. Istnienie zdarzenia i istnienie braku ryzyka zdarzenia wydają się być warunkami istnienie różnych poziomów ryzyka.

Z art. 33 RODO wynika jeszcze jeden poziom ryzyka naruszenia praw i wolności osób fizycznych. Jest to poziom ryzyka, który skutkuje obowiązkiem zgłoszenia naruszenia do PUODO, nie jest to bowiem poziom niski, a dokładniej, nie zachodzi małe prawdopodobieństwie naruszenia praw i wolności osób fizycznych. RODO nie wskazuje jak ten poziom ryzyka powinien być nazwany. Jest to poziom wyższy od niskiego i niższy od wysokiego. Wydaje się, że można tu mówić o średnim poziomie ryzyka. Można zatem wyróżnić:

– **Ryzyko o średnim poziomie**.

Wydaje się, że ryzyko o tym poziomie można utożsamić z ryzykiem, określonym wyżej jako „ryzyko", o poziomie uzyskanym z Preambuły RODO.

Rozważam tu poziomy ryzyka naruszenia praw i wolności osób fizycznych, ale skoro możliwe jest ryzyko naruszenia praw i wolności osób fizycznych, to zapewne możliwe jest też naruszenie praw i wolności osób fizycznych. Zachodzi ono w sytuacji, kiedy zdarzenie jest

tak poważne, że nie sposób już mówić o ryzyku naruszenia tych czy innych praw, ale że prawa te zostają naruszone. Wydaje się, że należy w związku z tym wyróżnić poziom ryzyka naruszenia praw i wolności wskazany poniżej.

– **Naruszenie praw i wolności osób fizycznych**.

Poziom ten znajduje się niejako ponad wysokim poziomem ryzyka naruszenia praw i wolności osób fizycznych. Wyżej poziom ten został określony jako „ryzyko zrealizowane".

Prowadzone powyżej rozważania ilustruję na następnej stronie tabelą. Miejsce w tabeli oddaje poziom ryzyka naruszenia praw i wolności osób fizycznych (niski – nisko, wysoki – wyżej).

Poziomy ryzyka naruszenia praw i wolności osób fizycznych		
Nazwa skrócona	Odpowiedni fragment przepisu (podstawa prawna)	Nazwa poprawna
Ryzyko zrealizowane	Art. 34 ust. 1 RODO + zasada *a fortiori*	Naruszenie praw i wolności osób fizycznych
Poziom ryzyka wysoki	Art. 34 ust. 1 RODO *Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.*	Wysokie ryzyko naruszenia praw i wolności osób fizycznych.
Poziom ryzyka wysoki z zastrzeżeniami	Art. 34 ust. 3 RODO *Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach: […]*	
Poziom ryzyka średni (podstawowy, niższy od wysokiego, wyższy od niskiego)	Art. 33 ust. 1 RODO *W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, […]*	
Poziom ryzyka niski	Art. 33 ust. 1 RODO *[…] chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.*	Ryzyko o małym prawdopodobieństwie naruszenia praw i wolności osób fizycznych.
Brak ryzyka naruszenia praw i wolności osób fizycznych		

3.15. Art. 24 Uwaga 15

Zestawienie poziomów ryzyka naruszenia praw i wolności osób fizycznych

Mając na uwadze czynione powyżej uwagi, można zestawić poziomy ryzyka naruszenia praw i wolności osób fizycznych na kształt swoistej drabiny ryzyka. Wygląda ona jak poniżej.

– Naruszenie praw i wolności osób fizycznych. – ono znajduje się najwyżej.
– Wysokie ryzyko naruszenia praw i wolności osób fizycznych. Wnioskujemy o nim ze słów art. 34 ust. 1 RODO: *[...] wysokie ryzyko naruszenia praw lub wolności osób fizycznych*.
– Ryzyko o średnim poziomie (ryzyko). Wnioskujemy o nim z art. 33 RODO i z motywu 76 Preambuły RODO.
– Ryzyko o małym prawdopodobieństwie naruszenia praw i wolności osób fizycznych. Wnioskujemy o nim ze słów art. 33 ust. 1 RODO: *[...] chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych*.
– Brak ryzyka naruszenia praw i wolności osób fizycznych.

Na związek poziomów ryzyka w różnych przepisach zwraca autor piszący o tym w komentarzu oxfordzkim[94].

Również autorzy jednego z czeskich komentarzy do RODO zwracają uwagę na występowanie różnych poziomów ryzyka w różnych przepisach RODO. Ciekawostkę stanowi fakt, że o ile komentarz oxfordzki został wydany w roku 2019, o tyle czeski komentarz, w którym jest o tym mowa, został wydany w roku 2017. Autorzy czescy wskazują, że występuje „ryzyko, wysokie ryzyko i niskie ryzyko”[95]. Nie sądzę, by autorzy komentarza oxfordzkiego inspirowali się treścią komentarza czeskiego, znajomość języka czeskiego nie jest niestety powszechna, jednak zbieżność toku myśli wskazuje – jak uważam – na poprawność tegoż, a przynajmniej wskazywać może.

---

[94] C. Burton, op. cit., s. 641.

[95] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek. op. cit., s. 249. Tłumaczenie cytatu, jak i pozostałych cytatów z języka czeskiego jest autorstwa J. Rzymowskiego. Z uwagi na fakt, że jest to jednak nie cytat a jego tłumaczenie, zaznaczam go cudzysłowami, nie zaś kursywą.

Jeśli chodzi o ryzyko, które nie ma dookreślenia, żadnej dodatkowej nazwy, ryzyko, rzekłbym – bezprzymiotnikowe, czyli „ryzyko" jako takie, ryzyko jako zjawisko, to wskazani czescy autorzy przedkładają, że jest ono *[...] ogólną miarą wdrożenia środków technicznych i organizacyjnych* zastosowanych *w celu wypełnienia obowiązków wynikających z [...]* [96] RODO.

Zwracam uwagę na pozorny truizm zawarty w powyższym tłumaczeniu cytatu. Autorzy czescy wskazują, że ryzyko to miara wdrożenia. Wydaje się, że jest to aktualne zarówno dla ryzyka ocenianego na gruncie art. 24 RODO i art. 32 RODO, jak i dla ryzyka ocenianego na gruncie art. 33 RODO i art. 34 RODO. Zastanowienie się nad tym poglądem pozwala dostrzec jego wartość. Administrator (danych osobowych) ocenia ryzyko i zależnie od wyniku tej oceny, dowiaduje się, jaki poziom wdrożenia środków technicznych i organizacyjnych występuje w jego strukturze. Następnie administrator podejmuje działania w celu jak największego obniżenia ryzyka.

Kolejny poziom ryzyka, który wskazali czescy autorzy to **wysokie ryzyko**. Wyżej w uwadze (*3.14. Art. 24. Uwaga 14. Poziomy ryzyka*) wskazuję na ten sam poziom ryzyka, tu jednak, dla porządku wskazuję, na jego wystąpienie u autorów czeskich. Podobnie jak ja, wskazują oni na związek tego poziomu ryzyka z art. 34 RODO, który uzależnia obowiązek informowania osób, których dane dotyczą, o naruszeniu ochrony danych osobowych od wysokiego poziomu ryzyka.

Czescy autorzy zwracają[97] słusznie uwagę na fakt, że wysokie ryzyko występuje i jest istotne dla art. 34 RODO i art. 35 RODO i art. 36 RODO.

Kolejny poziom ryzyka, o jakim piszą czescy autorzy, to niskie ryzyko. Oczywiście się z nimi zgadzam, że ryzyko takie występuje.

Dalej piszą oni, że *Niskie ryzyko aktywuje niektóre wyjątki spod obowiązków zapisanych w [98] RODO*. W pierwszej chwili podejście to mnie zaskoczyło, po chwili uznałem jednak i opinię tę podtrzymuję, że podejście takie jest trafne. Naruszenie skutkuje obowiązkiem zgłoszenia do organu. Naruszenie o ryzyku (naruszenia praw i wolności) na poziomie niższym niż wysoki i wyższym niż niski. Naruszenie na

---

[96] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit.

[97] Ibidem.

[98] Ibidem.

poziomie bezprzymiotnikowym. Naruszenie na poziomie wysokim skutkuje dodatkowo obowiązkiem poinformowania osób, których dane dotyczą. Informowanie (organu lub osób) jest więc zasadą. Naruszenie na poziomie niskim ustanawia wyjątek od obowiązku informowania. Ma to doniosłe następstwa, wynikające z faktu, że wyjątków nie należy interpretować rozszerzająco.

Podkreślam zatem raz jeszcze, ryzyko naruszenia praw i wolności, o którym mowa w art. 24 RODO, 32 RODO, 33 RODO i 34 RODO, to za każdym razem niejako to samo (rodzajowo) ryzyko oraz (już bez zastrzeżeń ostrożnościowych) to za każdym razem ryzyko naruszenia tych samych praw i wolności.

Przywołuję tu powyższe ustalenia, są one bowiem w znacznej mierze zgodne z moimi. Tym, co szczególnie cenię w ustaleniach czeskich autorów, jest, że mam poczucie, że kiedy piszą o ryzyku, to jest to za każdym razem to samo ryzyko, a jedynie przyjmuje ono różne poziomy, w różnych sytuacjach, do których odnoszą się różne przepisy.

Warto w tym miejscu przywołać doniosły pogląd T. Izydorczyka i M. Gumularza, którzy zwracają uwagę, że ryzyko, o jakim mowa jest w RODO, to za każdym razem ryzyko naruszenia praw i wolności osób fizycznych[99], nie zaś np. ryzyko dla administratora. Tytułem uzupełnienia można dodać jedynie, że chodzi o osoby, których dane dotyczą. Uzupełnienie to jest istotne, ponieważ administrator danych osobowych może być osobą fizyczną, a jednak nawet w tej sytuacji raczej nie chodzi o jego prawa i wolności, ale o prawa i wolności innych niż administrator osób fizycznych, których dane osobowe administrator przetwarza.

Na temat poziomów ryzyka w bardzo wyważony sposób wypowiadają się M. Ciemiński i M. Magdziak. Zwracają oni uwagę, że *zazwyczaj wyróżnia się ryzyko niskie, średnie, wysokie i bardzo wysokie. Niekiedy też przyjmuje się inne skale, wskazując, że dane ryzyko jest „wyższe niż średnie" lub „niższe niż wysokie"*[100]. W użytych w drugim z wyliczeń nazwach dostrzegam ślady zmagań, które ja też prowadziłem, zmagań z nazwaniem poziomu ryzyka, który wynika z przepisów, jednak nie został w tych przepisach nazwany – „Poziom ryzyka

[99] M. Gumularz, T. Izydorczyk, op. cit., s. 41.

[100] M. Ciemiński, M. Magdziak, [w:] D. Lubasz red. n. *Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych*, Warszawa 2022, s. 291.

średni (podstawowy, niższy od wysokiego, wyższy od niskiego)" z zamieszczonej wyżej w podrozdziale tabeli „Poziomy ryzyka naruszenia praw i wolności osób fizycznych". Dalej, również trafnie, wskazani autorzy piszą, że: *Opracowanie skali ryzyka jest punktem wyjścia do podjęcia odpowiedniej reakcji na ryzyko oraz stworzenia mapy ryzyka, na której powinny zostać uwzględnione wszystkie jego kategorie oraz ich poziom* [101].

Przytaczam powyższą wypowiedź z uwagi na jej wyważoną trafność, należy jednak uzupełnić, że o ile zajmujemy się ryzykiem na gruncie RODO, to skalę tegoż opracował prawodawca. Piszę o tym w uwadze (*3.14. Art. 24. Uwaga 14. Poziomy ryzyka*). Faktem jest, że prawodawca zrobił to w tak obecny na gruncie RODO niedbały sposób, ale takim samym faktem jest, że poziomy ryzyka, które wskazane są w przepisach RODO i które z przepisów tych wynikają, układają się w skalę, na dole której jest „Brak ryzyka naruszenia praw i wolności osób fizycznych", a na górze, której jest „Ryzyko zrealizowane".

Jeśli zaś chodzi o kategorie ryzyka, to kategorie te są w RODO zawarte dwukrotnie, raz w odniesieniu do oceny ryzyka w art. 32 ust. 2 RODO i drugi raz w odniesieniu do naruszenia ochrony danych osobowych w art. 4 pkt 12 RODO.

3.16. Art. 24 Uwaga 16

Definicja ryzyka

Wspomniani autorzy czeskiego komentarza poczynili ciekawe uwagi w sprawie ryzyka oraz – na co zwracam uwagę – ryzyko to zdefiniowali. Otóż piszą oni, że **ryzyko** jest *[...]* ***ogólną miarą wdrożenia środków technicznych i organizacyjnych zastosowanych w celu wypełnienia obowiązków wynikających z [...]*** [102] ***RODO***.

Wyżej odnoszę się do pojęcia ryzyka u czeskich autorów, jednak pojęcia „ryzyko" rozumianego jako jeden z trzech odnotowanych przez nich poziomów, jakie ryzyko przyjmuje. Zwracam uwagę, że wska-

---

[101] M. Ciemiński, M. Magdziak, [w:] D. Lubasz red. n., *Analiza ryzyka…,* s. 291. Autorzy ci powołują się na publikację, której autorem jest P. Welenc, jest to: P. Welenc, [w:] *Systemy zarządzania zgodnością. Compliance w praktyce.red.* B. Makowicz, B. Jagura, Warszawa 2020, s. 93.

[102] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit.

zani autorzy w istocie ryzyko zdefiniowali. Definicję tę, lekko ją uzupełniwszy redakcyjnie, zaznaczyłem wyżej czcionką wytłuszczoną.

Samym pojęciem ryzyka zajął się, choć nieco mimochodem, A. Cieślik, u którego czytamy, że *ryzyko możemy rozumieć jako zdarzenia, w wyniku których może zostać obniżony wymagany poziom poufności, integralności lub dostępności informacji* [103]. Wydaje się, że ogólna myśl jest dobra. Coś się dzieje, to coś może, czy też mogło się stać (prawdopodobieństwo), to coś jest poważne lub nie (waga), ale prawdopodobieństwo i waga to jednak składowe zdarzenia, a właśnie o zdarzeniu pisze A. Cieślik.

Wskazany autor pisze o ryzyku ciekawe rzeczy, z którymi się zgadzam. Otóż czytamy u niego, że ***Ryzyko jest kombinacją prawdopodobieństwa wystąpienia zagrożenia oraz potencjalnego skutku w przypadku pojawienia się tego zagrożenia***. *Materializacja ryzyka może prowadzić do straty finansowej, utraty dobrego imienia, lub wizerunku, braku możliwości realizacji procesów biznesowych, wydatku środków związanych z wystąpieniem incydentu*[104]. Zgadzam się i tu z A. Cieślikiem, z jednym jednak zastrzeżeniem, otóż wszystkie czarne scenariusze, o których A. Cieślik pisze, są zapewne realne i oczywiście można brać je pod uwagę, ale przede wszystkim należy brać pod uwagę możliwość naruszenia praw i wolności.

3.17. Art. 24 Uwaga 17

Podmiot zobowiązany

Należy podkreślić, że obowiązki wynikające z art. 24 RODO spoczywają na administratorze. Uwagę na to zwrócili K. Wygoda[105] oraz P. Barta, M. Kawecki i P. Litwiński[106]. Wskazani autorzy zwrócili uwagę na fakt, że obowiązki wynikające z przepisu spoczywają na administratorze, również w sytuacji, kiedy jest on administratorem we współadministrowaniu. Wydaje się, że myśl ta wymaga pewnego uzupełnienia.

---

[103] A. Cieślik, *Ocena (szacowanie) ryzyka*, [w:] *Dokumentacja ochrony danych osobowych ze wzorami*, Red. n. Mariusz Jagielski, Warszawa 2022, s. 144.

[104] Ibidem, s. 160. Pogrubienia A. Cieślik.

[105] K. Wygoda, op. cit., s. 285.

[106] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 283.

Otóż zgadzam się z tym, że obowiązki, które wynikają z art. 24 RODO, spoczywają na administratorze, wynika to bowiem z przepisu w sposób oczywisty, dokładnie ze słów: *Uwzględniając […] administrator wdraża […]* ze wskazaniem na słowo „administrator". Zgadzam się też, że obowiązki te spoczywają na współadministratorach, jednak należy pamiętać, że z uwagi na treść art. 26 RODO, współadministratorzy mogą ustalić, który z nich, które obowiązki realizować będzie. Może się to okazać szczególnie istotne przy porównywaniu obowiązków wynikających z art. 24 RODO z obowiązkami wynikającymi z art. 32 RODO. Obowiązki wynikające z art. 32 RODO spoczywają na administratorze i na podmiocie przetwarzającym. Nie od rzeczy jest wspomnieć, że pogląd, iż obowiązki z art. 24 RODO spoczywają na administratorze podziela również P. Fajgielski[107].

3.18. Art. 24 Uwaga 18

Subiektywne podejście

Krzysztof Wygoda zauważa, że podejście *oparte na ryzyku […] jest niewątpliwie w pewnym stopniu zawsze subiektywne*[108]. Myśl ta warta jest rozwinięcia.

Kiedy oceniamy ryzyko zaistnienia jakiegoś zdarzenia, to zawsze pojawia się element subiektywny, ocenny. Przewidujemy zdarzenie przyszłe, niepewne i przewidujemy skutki jego zaistnienia. W realiach ubezpieczeniowych miejsce to wypełniane jest wiedzą aktuariuszy, którzy z kolei znają prawdopodobieństwa zaistnienia zdarzeń; znają, bo wiedza ta wynika z niezliczonych zdarzeń, które miały miejsce w praktyce ubezpieczeniowej. W dziedzinie ochrony danych takich danych brak, a przynajmniej brak danych obiektywnych, sprawdzonych, danych, co do których można by orzec, że są one obiektywne. Z uwagi na brak takich danych, prawdopodobieństwo, ryzyko, podlega zawsze ocenie. Jeżeli zdarzenie zajdzie, to stan niepewności przemienia się w stan pewności. Zdarzenie zaszło, ryzyko się zrealizowało (piszę o tym również niżej w rozważaniach na temat art. 33 RODO i art. 34 RODO).

---

[107] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679…*

[108] K. Wygoda, op. cit., s. 284.

Jeżeli zdarzenie się zrealizowało, to zwykle zaistniała przynajmniej część zdarzeń, których zaistnienie przewidywano, można zatem ocenić ich skutki. Już tylko skutki, bo przy zdarzeniu, które zaistniało, nie ma sensu oceniać prawdopodobieństwa jego zaistnienia. Podejście oparte na ryzyku to ocenianie prawdopodobieństwa zaistnienia zdarzenia (i skutków tegoż), ale przed zaistnieniem zdarzenia. Ze względu na – mówiąc otwarcie – wypowiadanie się na temat zdarzeń przyszłych i niepewnych, należy się liczyć z tym, że wypowiedzi te mogą mieć dwie cechy, wskazuję je poniżej.

– Oceny dokonywane przez różne osoby na podstawie tych samych kryteriów mogą, z uwagi na nieostrość tych kryteriów, różnić się od siebie.
– Oceny mogą nie oddawać istoty zagadnień, innymi słowy – prawdopodobieństwo, że skutki zdarzenia zostaną ocenione nietrafnie. Zdarzenie będzie miało miejsce, mimo że nie powinno albo nie będzie miało miejsca, mimo ocenionego wysokiego prawdopodobieństwa zaistnienia. Skutki będą poważne, mimo że miały być błahe lub skutki będą błahe, mimo że miały być poważne.

Oceniając ryzyko, wypowiadamy się na temat przyszłości. Jest to ubierane w rozmaite metodyki, rysunki, wykresy; jest to okraszane wzorami, współczynnikami i ogólnie zdobione mnóstwem elementów, ale cokolwiek uczynimy, za czymkolwiek skryjemy ocenę, to i tak jej istotą jest wypowiedź na temat przyszłości, na temat zdarzenia przyszłego, niepewnego i na temat skutków tego zdarzenia.

Zakładam, że u podstaw myśli K. Wygody mogły leżeć rozważania analogiczne do powyżej zaprezentowanych. Pewien tego nie jestem, acz subiektywizm wynikający z podejścia opartego na ryzyku, mnie się kojarzy właśnie tak, jak zaprezentowałem powyżej.

Czy subiektywizm jest tu zjawiskiem niewłaściwym – trudno orzec. Wydaje się jednak, że obiektywizm jest zjawiskiem pożądanym. Nie da się go osiągnąć, można i – jak uważam – należy do niego dążyć. Do obiektywizmu oceny dążymy dzięki stosowaniu parametrów wskazanych w RODO i ocenianiu zdarzeń przyszłych przez ich pryzmat i przez pryzmat praw i wolności wskazanych w RODO.

O podejściu opartym na ryzyku piszą też P. Barta, M. Kawecki, P. Litwiński. Autorzy ci posuwają się nawet do stwierdzenia, że *Artykuł 24 ust. 1 RODO stanowi również jeden z wielu przypadków ema-*

nacji w przepisach RODO zasady tzw. „risk based approach", tj. podejścia opartego na ryzyku […][109].

Niestety muszę się do tego poglądu ustosunkować. Niestety, ponieważ pogląd jest poniekąd trafny, ryzyko, podejście oparte na ryzyku są w istocie myślą przewodnią ochrony danych osobowych na gruncie RODO, ale… Ale należy się zastanowić, czy nazwanie podejścia opartego na ryzyku mianem zasady nie jest aby nieco pochopne.

Na pewno nie jest to zasada taka, jak zasady z art. 5 RODO (czy z art. 6 RODO, czy w ogóle z Rozdziału II RODO)[110] , czyli nie jest to zasada w znaczeniu dyrektywalnym, czyli nie jest to zasada/przepis. Jeżeli jest to zasada, to jest to raczej zasada w znaczeniu postulatywnym, inaczej zasada/postulat. Posługuję się tu terminologią używaną przez J. Wróblewskiego i K. Opałka[111]. Przechodząc na terminologię R. Dworkina[112] i H.L.A. Harta[113], należy stwierdzić, że jest to raczej zasada/*principle* niż zasada/reguła/*rule*, czyli, że jest to zasada, którą realizuje się do pewnego stopnia. Sam obowiązek stosowania podejścia opartego na ryzyku można zakwalifikować jako zasadę/regułę/*rule*, ale dalej, już w ramach realizacji tego obowiązku jesteśmy raczej w domenie zasady/*principle*.

Poczyniwszy powyższe uwagi, mogę – jak się zdaje – zakwalifikować podejście oparte na ryzyku jako zasadę, jednak właśnie przy poczynieniu wskazanych uwag.

Podobne stanowisko prezentują autorzy poradnika wydanego przez PUODO, czytamy w nim: *Zasada podejścia opartego na ryzyku (*risk based approach*) jest ważną, perspektywiczną koncepcją, stanowiącą trzon ogólnego rozporządzenia o ochronie danych*[114]. Nie chcę śledzić drogi pomysłu, czy szedł on od PUODO czy do PUODO, tak czy inaczej, wszelkie umieszczone powyżej uwagi dotyczące podejścia opartego na ryzyku jako zasady, są aktualne i w odniesieniu do wypowiedzi PUODO.

---

[109] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 284.

[110] J. Rzymowski, *RODO – GDPR. Zasady*…, s. 65–128.

[111] K. Opałek, J. Wróblewski. *Zagadnienia teorii prawa*, Warszawa 1969, s. 92.

[112] R. Dworkin, *Biorąc prawa poważnie,* Warszawa 1998.

[113] H.L.A. Hart, *Pojęcie prawa,* Warszawa 1998.

[114] A. Kaczmarek, M. Młotkiewicz, A. Łapińska, A. Miłocha, M. Mazur, *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1,* Warszawa 2018, s. 4.

3.19. Art. 24 Uwaga 19

Nieostrość przepisu. Skutki

Jeszcze jedna myśl K. Wygody zasługuje na odnotowanie, tym razem nieco polemiczne. Otóż autor ten pisze najpierw, że użycie w przepisie zwrotów niedookreślonych wynika z faktu zmieniających się *warunków przetwarzania*. Dalej autor ten pisze, że *nałożenie na administratorów obowiązku wdrożenia odpowiednich środków technicznych*, które mają zapewnić *zgodność z RODO* i umożliwić *wykazanie owej zgodności […] bez wskazania jednoznacznych standardów, wytycznych, nawet w ujęciu wariantowym […] wydaje się działaniem wysoce niebezpiecznym dla ochrony praw osób, których dane dotyczą*[115].

Faktem jest, że nie wskazano w RODO, jak środki wdrażać; faktem jest, że nieumiejętne wdrożenie godzi w prawa (i wolności) osób, których dane dotyczą, ale należy koniecznie pamiętać o jednym jeszcze elemencie.

Otóż niejasny przepis jest zagrożeniem dla administratorów. Swojego rodzaju ciekawostkę stanowi fakt, że RODO nie przewiduje kary administracyjnej za naruszenie art. 24 RODO. Trafnie zwraca na to uwagę wspomniany wyżej K. Wygoda, który wskazuje, że o ile naruszenie przepisu nie skutkuje karą za samo naruszenie tego właśnie przepisu, to kara może mieć miejsce za naruszenie zasad z art. 5 RODO[116]. Nie sposób się z tym nie zgodzić, ale należy pamiętać o pewnym szczególe. Artykuł 24 ust. 1 RODO pokrywa się do pewnego stopnia z art. 32 ust. 1 RODO. Nie chcę tu wskazywać zbiegów treści i różnic w niej, ponieważ czynię to wyżej w uwadze (*3.12. Art. 24. Uwaga 12. Ocena ryzyka naruszenia praw i wolności z art. 24 RODO a ocena ryzyka naruszenia praw i wolności z art. 32 RODO*). Tu jednak pragnę wskazać, że mało prawdopodobne jest, by administrator wykonywał jednocześnie dwie oceny ryzyka, jedną na gruncie art. 24 RODO i jedną na gruncie art. 32 RODO. Powiem więcej, wiem, że zwykle wykonywana jest jedna taka ocena. Nie posiadam tu wyników badań ilościowych, takowych bowiem nie prowadzę, ale z mojego doświadczenia wynika, że nie do pomyślenia jest, by admi-

[115] K. Wygoda, op. cit.

[116] Ibidem, s. 285.

nistrator wykonywał jednocześnie dwie oceny ryzyka, jedną na podstawie art. 24 RODO i jedną na podstawie art. 32 RODO.

Administratorzy wykonują jedną ocenę ryzyka, o ile w ogóle wykonują jakąkolwiek. Ocena ryzyka bywa uważana za czynność trudną, skomplikowaną, nieledwie wymagającą wiedzy fachowej, przekraczającej możliwości przeciętnego inspektora ochrony danych lub prawnika. Nie jest to prawdą, co – jak mam nadzieję – wyjaśniam w niniejszej książce, a na poparcie tezy o łatwości wykonania oceny, na końcu książki załączam gotowe do wykorzystania uniwersalne tabele oceny ryzyka, zgodne z RODO. Z opisanych tu powodów, administratorzy często niewłaściwie wykonują oceny ryzyka, o ile – jak piszę wyżej – w ogóle je wykonują. Niewykonana lub źle wykonana ocena ryzyka może być powodem nałożenia kary administracyjnej, nie za naruszenie art. 24 ust. 1 RODO, ale za naruszenie art. 32 ust. 1 i ust. 2 RODO. Karę administracyjną za naruszenie art. 32 RODO przewiduje art. 83 ust. 4 RODO.

Trzeba zatem napisać to otwarcie, niejasność art. 24 ust. 1 RODO – część wprowadzająca i pokrewnego mu art. 32 ust. 1 RODO są zagrożeniem dla administratora. Artykuł 24 RODO jest zagrożeniem pozornie tylko w takim zakresie, o jakim pisze K. Wygoda. Zważywszy jednak na fakt, że w znacznej mierze treść art. 24 ust. 1 RODO pokrywa się z treścią art. 32 ust. 1 RODO i z uwagi na fakt, że administratorzy realizują obowiązki wynikające z obydwu przepisów poprzez przeprowadzanie jednej oceny ryzyka, bełkotliwość przepisów, a łagodniej pisząc – niejasność, może skutkować poniesieniem odpowiedzialności przez administratora, a z uwagi na zakres art. 32 RODO, również przez podmiot przetwarzający.

3.20. Art. 24 Uwaga 20

Jak i kiedy oceniać ryzyko

Należy się zastanowić, kiedy oceniać ryzyko naruszenia praw i wolności osób fizycznych. Odpowiedź na to pytanie zawarta jest w art. 24 ust. 1 RODO. Dla przypomnienia cytuję przepis, pozbawiony elementów niekoniecznych dla rozumowania: *Uwzględniając […] ryzyko […] administrator wdraża […] środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. […]*

Jak zatem widać, administrator ma wdrożyć środki. To stanowi podstawę rozumowania. Środki te administrator ma wdrożyć, „uwzględniając ryzyko". Wynika z tego, że ocena ryzyka musi poprzedzać wdrożenie środków. Jest tak, ponieważ niemożliwe jest uwzględnienie ryzyka bez uprzedniego wykonania oceny poziomów, jakie owo ryzyko przyjmuje Przypominam jednocześnie o celu art. 24 ust. 1 RODO. Cel ten najlepiej oddany jest przez następujący cytat, otóż celem jest, *aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać*.

Prześledźmy zatem. Do przeprowadzenia oceny ryzyka konieczna jest wiedza o tym, jakie czynności będą wykonywane. Ocena ryzyka poprzedza wdrożenie środków. Celem środków jest zgodność przetwarzania z RODO. Żeby przetwarzanie było zgodne z RODO, należy najpierw wdrożyć środki. Kolejność jest zatem następująca:
– ustalenie, jakie czynności będą wykonywane,
– udokumentowanie ustalenia wykonywanych czynności poprzez stworzenie rejestru czynności przetwarzania danych osobowych, za które odpowiada administrator,
– przeprowadzenie oceny ryzyka,
– udokumentowanie (stworzenie dokumentacji) przeprowadzenia oceny ryzyka,
– wdrożenie środków,
– udokumentowanie (stworzenie dokumentacji) wdrożenia środków.

3.21. Art. 24 Uwaga 21

Powtarzanie ocen ryzyka

Należy się zastanowić nad tym, czy ocenę, o której mowa w art. 24 ust. 1 RODO, należy powtarzać. Podkreślam, że nie piszę tu o ocenie pod kątem bezpieczeństwa przetwarzania, o której stanowi art. 32 RODO. Tu piszę o ocenie pod kątem zgodności z RODO. Wydaje się, że tę ocenę należy powtarzać kiedy:
– administrator przewiduje pojawienie się nowej czynności,
– dotychczas wykonywana czynność ulegnie zmianie w zakresie ocenianych jej elementów.

Otwarte pozostaje pytanie o wykonywanie oceny ryzyka w sposób powtarzalny, co jakiś czas, może w sposób ciągły. Paweł Fajgielski pisze nawet, że *Wdrożenie przez administratora środków tech-*

nicznych i organizacyjnych nie jest działaniem jednorazowym, ale powinno przybrać postać procesu, w ramach którego administrator dokonuje przeglądu i w razie potrzeby uaktualnia przyjęte wcześniej zabezpieczenia[117], jednak autor ten nie wskazuje, jak, czy też z jakim nasileniem ten proces wyglądać powinien.

O ile nie wyobrażam sobie, by ocena ryzyka techniczno-organizacyjnego nie była powtarzana, o tyle wyobrażam sobie, że ocena pod kątem zgodności z RODO nie jest często, może latami powtarzana. Jest to ryzykowne, ponieważ jeżeli administrator nie powtarza oceny ryzyka, to traci jej funkcję kontrolną. Zakładam jednak, że jeśli tę funkcję traci, to jest tego świadom.

Na pytanie o to, kiedy należy powtarzać czynność oceny ryzyka, można odpowiedzieć też niejako od innej strony. Czynność oceny ryzyka, o której mowa w art. 24 ust. 1 RODO, jest to czynność ukierunkowana na cel. Celem tym jest, *aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać*. Można uznać, że w momencie, w którym ocena ryzyka przestaje realizować wskazany cel, właśnie wtedy należy ocenę tę powtórzyć. Po czym powtórzyć po raz kolejny i kolejny. Za każdym razem, kiedy ostatnio wykonana ocena ryzyka nie realizuje już celu wskazanego w przepisie.

3.22. Art. 24 Uwaga 22

Wykazanie realizacji obowiązków

Na osobną uwagę zasługuje obowiązek wykazania realizacji obowiązków z art. 24 ust. 1 RODO. Sam obowiązek wykazania realizacji obowiązków też jest zapisany w art. 24 ust. 1 RODO, może zatem przez to być przypadkiem pominięty lub zbagatelizowany, tym bardziej że naruszenie art. 24 RODO nie jest zagrożone karą administracyjną. Należy jednak pamiętać, że wykazanie realizacji obowiązków wynikających z RODO jest konkretyzacją art. 5 ust. 2 RODO w zakresie rozliczalności, a ten przepis jest zabezpieczony karą administracyjną. Wspominam o tym w (*Art. 24 ust. 1. Wnioski z analizy*) oraz w (*2.1 Art. 24.ust. 1 Analiza*).

Należy zwrócić uwagę na swojego rodzaju metaobowiązek zawarty w art. 24 ust. 1 RODO. Czytamy tam, że *[...] administrator*

[117] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679...*

wdraża odpowiednie środki […] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Jak widać, w przepisie zapisane są (nieco upraszczając wywód) dwa obowiązki, wymieniam je poniżej.

– Obowiązek pierwszy – administrator ma obowiązek wdrożyć środki, dzięki którym przetwarzanie danych osobowych będzie odbywało się zgodnie z RODO.
– Obowiązek drugi – administrator ma obowiązek wykazać, że wdrożył środki i że przetwarzanie odbywa się zgodnie z RODO.

Na obowiązek wykazania realizacji obowiązków zwraca uwagę P. Fajgielski, który pisze wprost, że *Służyć temu może dokumentowanie przeprowadzonej analizy ryzyka i innych działań podjętych w celu zapewnienia zgodności z przepisami komentowanego rozporządzenia*[118]. Zgadzam się ze stanowiskiem cytowanego autora, dodatkowo zaś wzory dokumentacji mogącej służyć wskazanemu tu celowi zamieszczam na końcu niniejszej książki.

Również E. Bielak-Jomaa i D. Lubasz zwracają uwagę na konieczność dokumentowania analizy ryzyka i – co uważam za szczególnie cenną wskazówkę – podkreślają, że dokumentacja oceny ryzyka pozwala na skontrolowanie, czy ocenę tę przeprowadzono właściwie i czy właściwie dalej z ryzykiem postępowano[119].

Wracając do konkretyzacji zasad, zwracam uwagę, że analogiczne do mojego zdania o konkretyzacji zasad przez przepisy szczegółowe RODO prezentuje T. Izydorczyk. Autor ten pisze: *Można powiedzieć, w uproszczeniu, że inne (szczegółowe) wymogi RODO albo wprost wynikają z tych zasad, albo są z nimi ściśle powiązane*[120].

Podobne, choć nieco inaczej wyrażone stanowisko znajdziemy u Ch. Poszwińskiego, który przy okazji omawiania prawa do *przejrzystego informowania i przejrzystej komunikacji pisze,* że *Punktem wyjścia będzie omówienie zasady przejrzystości, która zdaje się odgrywać kluczową rolę w wyjaśnieniu założeń prawodawcy unijnego*

---

[118] Ibidem.

[119] E. Bielak-Jomaa, D. Lubasz, op. cit., s. 38.

[120] T. Izydorczyk, op. cit., s. 132. Cieszę się naukowo, że T. Izydorczyk nie umieścił w rozdziale, do którego fragment tu odsyłam, przypisu do żadnej z moich książek, oznacza to bowiem zapewne, że poglądami moimi się nie inspirował, a przypadkowy fakt zbieżności naszych poglądów może – jak mam nadzieję – świadczyć o ich trafności, chyba, że obaj się mylimy.

przyjętych w art. 12 RODO[121]. W ogóle u Ch. Poszwińskiego dostrzegam głębokie zrozumienie zjawiska konkretyzacji zasad przez przepisy. Mam poczucie, że piszemy to samo, tylko nieco innymi językami. Chrystian Poszwiński pisze, że: *Celem prawodawcy unijnego jest osiągnięcie takiego stanu, w którym przepisy będą wskazywały ogólne zasady, jakimi powinny kierować się podmioty w trakcie przetwarzania danych osobowych – przy jednoczesnym założeniu, że szczegółowy sposób postępowania będzie tworzony osobno przez każdego administratora odpowiednio do okoliczności i na jego własne ryzyko*[122]. Jak widać, wskazany autor dostrzega związek między zasadami a przepisami, co prawda Ch. Poszwiński wskazuje raczej na kierunek od przepisu do zasady, ja ten kierunek widzę dopiero na poziomie wykazania realizacji zasady, ponieważ na poziomie realizacji zasady widzę raczej kierunek od zasady do przepisu, tym niemniej podróżujemy chyba w tym samym kierunku intelektualnym.

3.23. Art. 24 Uwaga 23

Przepis jako zapis prawa, obowiązku i wolności

Powracając do rozważań prowadzonych wyżej w uwagach, zatrzymam się nad problemem wynikania praw i wolności z przepisu.

Można sobie wyobrazić, że koncepcja, zgodnie z którą w każdym przepisie zapisane jest prawo i obowiązek, i wolność jest dla kogoś nieprzekonująca. Można wyobrazić sobie podejście, w którym ktoś uważa, że jeżeli konkretne słowa przepisu mówią o obowiązku, to przepis ten ustanawia tylko obowiązek. Odpowiednio, w takim podejściu, jeżeli konkretne słowa przepisu mówią o uprawnieniu, to przepis ten ustanawia tylko uprawnienie i oczywiście jeżeli konkretne słowa przepisu mówią o wolności, to przepis ten ustanawia tylko wolność. Oczywiście ja tak nie uważam, jednak z uwagi na doniosłość zagadnień związanych z prawami, obowiązkami i wolnościami dla tematyki niniejszej książki, pogląd taki w książce umieszczam, choć głównie po to, by wskazać, że jest to pogląd błędny. Uważam, że podejście takie jest niewłaściwe. Uważam, że niezależnie od tego, czy w warstwie językowej przepis wyraża prawo czy obowiązek, to i tak

[121] Ch. Poszwiński, op. cit., s. 70–71.

[122] Ibidem, s. 17.

zawsze przepis ten ustanawia trzy zjawiska, czyli ustanawia prawo, ustanawia obowiązek i ustanawia wolność. Konkretną wolność związaną z danym prawem i z danym obowiązkiem.

Zastanówmy się zatem, z czego wynika pogląd, że przepis, niezależnie od tego, czy w warstwie językowej jest nim mowa o prawie, obowiązku czy o wolności, za każdy razem ustanawia zarówno prawo, jak i obowiązek, jak i wolność.

Uważam, że za stanowiskiem takim przemawiają różne argumenty, zarówno argumenty natury teoretycznej, jak i argumenty natury dogmatycznej, jak i argumenty z autorytetu, omawiam je poniżej, w kolejnych uwagach.

3.24. Art. 24 Uwaga 24

Przepis jako zapis prawa, obowiązku i wolności

Argument z treści przepisów

Za koncepcją, zgodnie z którą w przepisie zapisany jest zawsze obowiązek i prawo przemawia moim zdaniem argument, który można chyba nazwać dogmatycznym, bo jest to argument z treści przepisu. Weźmy na przykład artykuł 5 ust. 1 lit c RODO, czyli przepis ustanawiający zasadę minimalizacji (przetwarzania danych osobowych). Każda z zasad nadaje się jako przykład, ale opierając się na tej, wyjaśnienie będzie proste. Zasady z art. 5 ust. 1 RODO mają charakter obowiązków. To, jak sądzę, nie podlega dyskusji. O tym, że zasady z art. 5 ust. 1 RODO moją charakter obowiązków, wnosimy z treści elementu wprowadzającego, który znajduje się na początku art. 5 ust. 1 RODO. Czytamy tam: *Dane osobowe muszą być*. W związku z tym cały przepis ustanawiający zasadę należy czytać: Dane osobowe muszą być: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").

Dla uproszczenia wywodu przyjmijmy, że zasada minimalizacji oznacza obowiązek przetwarzania danych osobowych w zakresie adekwatnym, stosownym i ograniczonym do niezbędnego do realizacji celów administratora. Obowiązek ten można by próbować realizować wprost, gdyby nie było innych przepisów RODO, które go konkretyzują, ale takie przepisy są. Zasada konkretyzowana jest przez przepisy, z których wynika, jakie dane zbierać, jak je zbierać oraz przez przepisy, które przyczyniają się do kontroli zakresu przetwarzanych danych.

(Pomijam w wywodzie, że minimalizacja dotyczy nie tylko tego, jakie dane administrator zbiera, ale i tego, co z nimi czyni.) Zasada minimalizacji konkretyzowana jest dzięki zgodności zakresu przetwarzania z art. 6, 9 i 10 RODO. Oczywiście wskazane przepisy związane są głównie z zasadą zgodności z prawem z art. 5 ust. 1 RODO, ale z przepisów tych wynika również zakres przetwarzania danych osobowych. Obowiązkowy zakres. Czy jednak art. 6, 9 i 10 RODO statuują obowiązki, przynajmniej w warstwie językowej, to nad tym należałoby się poważnie zastanowić. W przepisach tych czytamy: *Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy […] Zabrania się przetwarzania danych osobowych ujawniających* (i uzupełniająco: *Ust. 1 nie ma zastosowania, jeżeli spełniony jest […]*), *Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie […]* Jak widać, prawodawca użył w przepisach form bezosobowych.

Można więc już tu się zastanowić, czy realizacja art. 6, 9 i 10 RODO to obowiązek administratora, czy prawo osoby, której dane dotyczą, czy wolność, która tę osobę chroni. Kiedy spoglądamy na art. 6, 9 i 10 RODO przez pryzmat art. 5 RODO, który ustanawia obowiązki, to mamy poczucie, że art. 6, 9 i 10 RODO ustanawiają obowiązki po stronie administratora. Kiedy jednak spoglądamy na te przepisy bez tła wynikającego z art. 5 RODO, to fakt, że z art. 6, 9 i 10 RODO wynikają obowiązki, nie jest już taki oczywisty. Okazuje się, że przepisy te powinny być zrealizowane, ale czy mają one być zrealizowane, ponieważ jest to obowiązkiem administratora, czy ponieważ jest to prawem osoby, której dane dotyczą – nie jest to takie oczywiste. Zasada minimalizacji jest też konkretyzowana przez art. 14 ust. 1 lit. d RODO. Przepis ten nakłada na administratora obowiązek podawania osobie, której dane dotyczą, informacji o kategoriach danych osobowych, które są przez administratora zbierane. Jak zatem widać, zasadę konkretyzuje przepis, który statuuje obowiązek, ale już z art. 15 ust. 1 lit. b RODO wynika, że osoba, której dane dotyczą, jest uprawniona do uzyskania informacji o kategoriach odnośnych do danych osobowych. Widać więc, że zasadę minimalizacji konkretyzują trzy przepisy, co do których nie wiadomo tak do końca, czy ustanawiają (w warstwie językowej, bo poza nią uważam, że wiadomo) obowiązki czy upraw-

nienia (art. 6, 9, 10 RODO), przepis ustanawiający obowiązek (art. 14 RODO) i przepis ustanawiający uprawnienie (art. 15 RODO).

Nie jest to koniec wywodu dotyczącego konkretyzacji zasady. Artykuł 17 RODO – prawo do bycia zapomnianym, cytuję część wprowadzającą: *Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe […]* Jak zatem widać, przepis w warstwie językowej ustanawia i prawo osoby, i obowiązek administratora. Do przepisów konkretyzujących dochodzi więc kolejny, który – co stanowi tu nowość w warstwie językowej – ustanawia i prawo i obowiązek. W tym miejscu kończę podawanie przykładów, celem moim nie jest bowiem wskazanie wszystkich przepisów które konkretyzują daną zasadę. Celem moim jest wskazanie, że zasadę zapisaną w art. 5 RODO konkretyzują przepisy, spośród których niektóre w warstwie językowej ustanawiają obowiązki, inne zaś w warstwie językowej ustanawiają uprawnienia, jak również przepisy, które w warstwie językowej ustanawiają zarówno obowiązki, jak i uprawnienia, oraz przepisy, które w odniesieniu do obowiązków i uprawnień w warstwie językowej zachowują neutralność. Jeżeli chcemy uporządkować zaprezentowany materiał, to najprościej jest sprowadzić treść przepisów konkretyzujących zasady do wspólnego mianownika i dalej, sprowadzić do tego samego mianownika samą zasadę, ale o tym niżej. Tym wspólnym mianownikiem może być prawo (uprawnienie), może być nim obowiązek, może być nim wolność (konkretna wolność, która znaczeniowo odpowiada danemu przepisowi, danemu prawu, danemu obowiązkowi).

Ustanowione w art. 6, 9 i 10 RODO warunki zgodności przetwarzania danych osobowych z prawem łatwo jest zakwalifikować jako obowiązki administratora. Artykuł 14 RODO ustanawia obowiązek po stronie administratora. Artykuł 15 RODO ustanawia uprawnienie po stronie osoby, której dane dotyczą, jeżeli jednak z uprawnieniem tym nie korelowałby, czy też inaczej: nie byłby sprzężony obowiązek po stronie administratora, to uprawnienie to miałoby jedynie charakter obrzędowy czy wręcz symboliczny. Osoba, której dane dotyczą, składałaby żądanie dotyczące uzyskania pewnych informacji, nieobciążony zaś obowiązkiem administrator, żądania tego by nie realizował, a przecież jeżeli administrator nie zrealizuje tego żądania, to grozi mu odpowiedzialność administracyjna na gruncie art. 83 ust.

5 lit. b RODO. Nie ma zatem na poziomie rozumienia treści przepisu niczego, co uniemożliwiałoby dostrzegać w art. 15 RODO obowiązek administratora. I wreszcie jeśli chodzi o art. 17 RODO, to prawodawca rzecz tu nieco ułatwił, ponieważ zapisał w warstwie językowej przepisu tak prawo, jak i obowiązek.

Przeprowadzone wyżej rozważania doprowadziły do sprowadzenia zaprezentowanych przepisów do wspólnego mianownika, którym jest obowiązek administratora. Nic nie stoi na przeszkodzie, by przeprowadzić rozumowanie analogiczne, w którym sprowadzamy zaprezentowane przepisy do innego wspólnego mianownika, którym jest uprawnienie osoby, której dane dotyczą. Jeśli zatem chodzi o art. 6, 9 i 10 RODO, prawem (uprawnieniem) osoby, której dane dotyczą, jest, by jej dane osobowe były przetwarzane wyłącznie na warunkach wskazanych przez prawodawcę w tych przepisach (odpowiednio do sytuacji, pomijam szczegóły), podobnie prawem osoby, której dane dotyczą, jest, by otrzymała od administratora informacje wskazane w art. 14 RODO. Jeśli zaś chodzi o art. 17 RODO, to z uwagi na komfortową dla interpretatora warstwę językową tego przepisu nie trzeba nawet szczególnie wywodzić, że z przepisu tego wynika prawo osoby, której dane osobowe dotyczą.

Jak zatem widać, zasada minimalizacji jest konkretyzowana przez pewne przepisy (nie wskazałem wszystkich, część jedynie, która do sformułowania wywodu jest wystarczająca). Przepisy te można zinterpretować jako obowiązki administratora czy też – wyrażając się precyzyjniej – interpretator może przyjąć, że z przepisów tych wynikają obowiązki administratora, ale również ten sam interpretator może bez najmniejszego problemu wskazać, że z tych samych przepisów wynikają prawa, czyli uprawnienia osoby, której dane dotyczą. Drobnym tylko uzupełnieniem jest wskazanie, że system złożony z praw i obowiązków ma na celu ochronę wolności. To oczywiście jeden tylko z celów tego systemu, analogicznym celem jest bowiem realizacja obowiązków administratora oraz – jak uważam – przede wszystkim realizacja uprawnień osób, których dane dotyczą. Przepisy szczegółowe RODO można – jak mam nadzieję wskazuję to wyżej – zinterpretować zarówno jako przepisy ustanawiające obowiązki, jak i jako przepisy ustanawiające uprawnienia, jak i jako przepisy chroniące wolności.

Jednocześnie należy się zastanowić, czy nie ma czegoś dziwnego w konkretyzacji zasady, która jak wiemy ustanawia obowiązek

po stronie administratora, przez uprawnienia, które przysługują osobie, której dane dotyczą.

Oczywiście w warstwie językowej zasada ustanawia obowiązek po stronie administratora, więc, by oszczędzić sobie zdziwienia, którego możliwość tutaj sygnalizuję, interpretator może sprowadzić interpretację przepisów szczegółowych RODO, które konkretyzują zasadę do obowiązków, wtedy realizacja zasady jawi się bardzo prosto. Zasada statuująca obowiązek jest konkretyzowana przez przepisy statuujące obowiązki. Administrator, by zrealizować zasadę, musi zrealizować przepisy, które tę zasadę konkretyzują. Administrator ma również obowiązek, który wynika z art. 5 ust. 2 RODO, a mianowicie obowiązek wykazania realizacji zasady. Obowiązek ten nosi nazwę zasady rozliczalności, czy też dokładniej jest to obowiązek rozliczalności zapisany w zasadzie rozliczalności. Administrator, by zrealizować zasadę rozliczalności, musi wykazać, że zrealizował konkretne zasady z art 5 ust. 1 RODO. Pamiętając jednak o tym, że zasady konkrety zachowane są przez przepisy szczegółowe, administrator, by zrealizować zasadę rozliczalności w odniesieniu na przykład do zasady minimalizacji, musi zrealizować obowiązki wynikające z przepisów konkretyzujących zasadę minimalizacji.

Rozumowanie oparte na obowiązku może być równie dobrze oparte na prawie, czyli uprawnieniu. Administrator, który chce zrealizować zasadę minimalizacji, czyli prawo osoby, której dane dotyczą, do tego, by jej dane osobowe były przetwarzane przez administratora w sposób ograniczony co do zakresu, musi zrealizować uprawnienia osób, których dane dotyczą, które to uprawnienia konkretyzują prawo do przetwarzania danych osobowych w sposób ograniczony co do zakresu. Administrator realizuje te uprawnienia oczywiście poprzez realizację swoich obowiązków, ale tak naprawdę administrator realizuje te uprawnienia poprzez wykonywanie pewnych czynności faktycznych. Obowiązek czy uprawnienie są to zjawiska prawnicze, z których wynika konieczność wykonania pewnych czynności faktycznych przez osobę zobowiązaną, które to czynności są zarówno realizacją obowiązków, jak i uprawnień, oraz – o czym przypominam na marginesie – służą ochronie odpowiednich wolności.

Jak widać z powyższych wywodów, przepisy szczegółowe RODO mogą być interpretowane jako przepisy ustanawiające obowiązki, ale te same przepisy mogą być interpretowane jako przepisy ustanawia-

jące uprawnienia, tak samo jest z zasadami z art. 5 RODO. Jedynie do interpretatora przepisów należy decyzja, czy w zasadach z art. 5 RODO dopatrzy się on obowiązków, czy w zasadach tych interpretator dopatrzy się uprawnień.

W podobnym duchu idzie myśl Ch. Poszwińskiego. Pisze on, że: *Obowiązki administratora wynikają z poszczególnych praw osób, których dane dotyczą, dlatego też ryzyko nie będzie powiązane z możliwością dochodzenia prawa przez podmiot danych, lecz z niedopełnieniem obowiązków przez administratora. Samo postępowanie będzie jedynie pochodną nieprzestrzegania konkretnych przepisów*[123]. Myśl Ch. Poszwińskiego jest mi ogromnie bliska, jest bowiem zgodna z opracowanym przeze mnie konceptualizmem prawniczym jako ogólną teorią prawa.

3.25. Art. 24 Uwaga 25

Przepis jako zapis prawa, obowiązku i wolności

Argument z racjonalności prawodawcy

Uzupełniając powyższy wywód, użyć można jednego jeszcze argumentu, tym razem z pogranicza dogmatyki i teorii. W RODO wielokrotnie znajdujemy odesłania do praw i wolności, jednocześnie w warstwie językowej RODO owe prawa i wolności, do których przepisy odsyłają, nie występują. Prawa i wolności występują w RODO w przepisach odsyłających. Pamiętajmy jednak, że prawodawca jest racjonalny, jeżeli zatem prawodawca umieszcza w RODO fragment, który łatwo może być zinterpretowany jako fragment ustanawiający prawa i wolności, to obowiązkiem interpretatora jest, by iść za myślą czy też intencją prawodawcy i tak właśnie fragment ten zinterpretować. Jeśli interpretator tego nie czyni, to lekceważy racjonalność prawodawcy. Odsyłając ogólnie do rozważań prowadzonych w innych miejscach niniejszej książki, mogę uczciwie stwierdzić że jeżeli w art. 5 RODO dostrzeżemy prawa i wolności to ogromnie ułatwia to dokonywanie oceny ryzyka oraz dokonywanie oceny skutków naruszenia, co również jest – jak uważam – spójne z koncepcją racjonalnego prawodawcy.

[123] Ibidem, s. 21.

3.26. Art. 24 Uwaga 26

Przepis jako zapis prawa, obowiązku i wolności

Argument z autorytetu

Kolejnym argumentem jest argument z autorytetu. Otóż koncepcja, która utożsamia prawo, obowiązek i wolność nie jest koncepcją nową. Co więcej, koncepcja ta jest częścią większej koncepcji, twórcą której jest Wesley Newcomb Hohfeld. Koncepcja ta funkcjonuje od ponad stu lat, jest nadal żywa, choć mam poczucie, że może być nielubiana, ponieważ kwestie, które są w niej poruszane, są objaśniane z jej użyciem w sposób niezwykle prosty i łatwy do zrozumienia. W każdym razie W.N. Hohfeld w 1913 roku przedstawił zestawienie pojęć[124], i w 1917 roku zestawienie to powtórzył[125]. Prezentuję je poniżej w tabeli. Pojęcia zestawione są w ten sam sposób zarówno w artykule z 1913 roku, jak i w artykule z 1917 roku. Co ciekawe, w artykule, przed przejściem do właściwego wywodu W.N. Hohfeld twierdzi, że podejście oparte wyłącznie na prawie i wolności jest nadużywane i że niepotrzebnie odnosi się je do wszystkich stosunków prawnych. Tym samym wskazany autor uważa podejście oparte na prawach i wolności za coś zwykłego i tradycyjnie stosowanego.

{	Jural Opposites	rights no-rights	privilege duty	power disability	immunity liability
{	Jural Correlatives	right duty	privilege duty	power liability	immunity disability

Wesley N. Hohfeld pisze, że *[…] most promising line of procedure seems to consist in exhibiting of the various relations in a scheme of 'opposites' and 'correlatives, ' and then proceeding to exemplify their individual and application in concrete cases*[126].

---

[124] W.N. Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*. "The Yale Law Journal", Nov., 1913, Vol. 23, No. 1 (Nov., 1913), s. 16–59. Stable URL: https://www.jstor.org/stable/785533

[125] W.N. Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, "The Yale Law Journal", Jun., 1917, Vol. 26, No. 8 (Jun., 1917), pp. 710–770. Stable URL: https://www.jstor.org/stable/786270

[126] W.N. Hohfeld, *Some Fundamental…*

W języku polskim oznacza to, że „najbardziej obiecująca linia postępowania wydaje się polegać na ukazaniu różnych relacji w schemacie „przeciwieństw" i „korelacji", a następnie przystąpieniu do egzemplifikacji ich indywidualności i zastosowania w konkretnych przypadkach". Dalej, wyjaśniając relacje między obowiązkiem i prawem W.N. Hohfeld pisze, że *'Duty' and 'right' are correlative terms. correlative terms. When a right is invaded, a duty is violated*[127], co tłumaczymy na: „'Obowiązek' i 'prawo' to pojęcia korelatywne. Kiedy narusza się prawo, narusza się obowiązek". Jeżeli zatem osoba, której dane dotyczą, skorzysta z prawa z art. 15 RODO i zażąda informacji, to obowiązkiem administratora jest tej informacji udzielić. Jeżeli administrator nie udzieli informacji, to narusza uprawnienie i narusza obowiązek. Myślę, że dla potrzeb namysłu nad tym, czy zasady na pewno statuują prawa, obowiązki i wolności, w tym miejscu można by wywód przerwać. Tym niemniej podkreślić należy, że W.N. Hohfeld uważa prawo za niezmienny korelatyw obowiązku[128]. Cytowany autor uważa obowiązek za coś, co powinno się robić lub coś, czego powinno się nie robić (*one ought or ought not to do*)[129]. Z kolei uprawnienie W.N. Hohfeld uważa za coś, co może być żądane zgodnie z prawem (*whatever may be lawfully claimed*)[130].

Patrząc na zestawienie W.N. Hohfelda, można jedynie zastanawiać się, które ze wskazanych przezeń pojęć, na które polskie pojęcia tłumaczyć należy. „Duty" to obowiązek, korelatywem obowiązku jest prawo, czyli „right". Wolność, na przykład „wolność od przetwarzania danych osobowych w sposób nieograniczony co do zakresu", czyli wolność zapisana w zasadzie minimalizacji to w ujęciu cytowanego autora „immunity", czyli wolność od cudzej władzy lub kontroli[131].

Ciekawą rzeczą, na którą zwrócono uwagę już w czasach W.N. Hohfelda, jest, że używał on terminów znanych[132].

---

[127] Ibidem, s. 32.

[128] Ibidem, s. 31.

[129] Ibidem, s. 32.

[130] Ibidem, s. 31.

[131] Ibidem, s. 55.

[132] Walter Wheeler Cook. *Hohfeld's Contributions to the Science of Law*, "The Yale Law Journal", 1919, Jun., Vol. 28, No. 8 (Jun., 1919), pp. 723. Stable URL: https://www.jstor.org/stable/787275

Podkreślić należy, że teoria W.N. Hohfelda, mimo że ma już ponad sto lat, jest teorią nadal żywą. Nie podaję tu kolejnych odniesień w literaturze do teorii W.N. Hohfelda, zwrócę jednak uwagę na wypowiedź C. Nyquista z 2002 roku. Autor ten pisze: *Hohfeld provides a vocabulary that captures the four different uses of the word right: right (in a Hohfeldian sense), privilege, power and immunity. He argues that a legal relation is always between two persons and that a right, privilege, power or immunity is always linked to a correlative (duty, no-right, liability and dusability). In other words, if someone has a Hohfeldian right, another person has a duty*[133]. Tłumaczymy to na: „Hohfeld podaje słownictwo, które obejmuje cztery różne użycia słowa prawo: prawo (w hohfeldiańskim rozumieniu), przywilej, władza i immunitet. Obstaje on że stosunek prawny jest zawsze między dwiema osobami i że prawo, przywilej, władza lub immunitet jest zawsze połączony z korelatem (obowiązek, brak prawa, odpowiedzialność i niemożność). Innymi słowy, ma hohfeldiańskie prawo, inna osoba ma obowiązek".

Wolność, o której W.N. Hohfeld również pisze, jest z mojego punktu widzenia uzupełnieniem relacji uprawnienia i obowiązku. Wynika to z wydanego w 2002 roku artykułu C. Nyquista. Autor ten pisze o koncepcji W.N. Hohfelda między innymi, że: *A person with an immunity cannot have a particular legal relations changed by another [...]*[134], czyli: „Osoba z immunitetem nie może mieć konkretnych stosunków prawnych zmienionych przez kogoś innego". Tu widzę wolności, o których piszę w innych miejscach niniejszej publikacji.

Współcześnie w Polsce myślą W. Hohfelda zajmuje się M. Błahut, który w swoim artykule zwraca uwagę na zbieżność między teoriami W.N. Hohfelda, H.L.A. Harta i R. Dworkina[135]. Autor ten szczególnie drobiazgowo wyjaśnia różnicę między „privilege", którą określa mianem wolności relacyjnej, a „immunity", które określa mianem immunitetu. Rozważania M. Błahuta potwierdzają moje prze-

---

[133] C. Nyquist, *Teaching Wesley Hohfeld's Theory of Legal Relations*, "Journal of Legal Education",2002, March/June, Vol. 52, No. 1/2 (March/June 2002), pp. 239–240. Stable URL: https://www.jstor.org/stable/42893752

[134] Ibidem, s. 240.

[135] M. Błahut, *Pojęcie prawa podmiotowego we współczesnej liberalnej filozofii prawa.* „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2002, Rok LXIV, z. 1.

konanie, że wolności, o których piszę na gruncie RODO to raczej „immunitety" w ujęciu Hohfelda.

Drugi argument z autorytetu to argument oparty na wywodach profesora Zygmunta Ziembińskiego. Autor ten pisze, że: *[...] stosunek „bycia uprawnionym wobec..." jest odwrotnością stosunku „bycia zobowiązanym wobec..." [...]*[136]. Zacytowane zdanie oddaje istotę zagadnienia, całość rozumowania znajduje się w znanym i lubianym podręczniku do logiki prawniczej.

W poglądy W.N. Hohfelda i A. Ziembińskiego wpisuje się pogląd Ch. Poszwińskiego, który w swojej książce pisze, że *Pojęcie praw, a także ich rola i funkcje w procesie przetwarzania świadczą o wysokim stopniu zintegrowania tych praw z obowiązkami administratora i procesora*[137]. Wskazany autor dostrzega związek między prawami i obowiązkami, podobnie jak Z. Ziembiński, a pomija wolności, czego nie czyni W.N. Hohfeld.

3.27. Art. 24 Uwaga 27

Przepis jako zapis prawa, obowiązku i wolności

Argument z filozofii

Argumentem, który pozostawiłem na koniec wywodu poświęconego prawom, obowiązkom i wolnościom, jest argument oparty na mojej własnej teorii obowiązywania i wykładni prawa, noszącej nazwę „konceptualizm prawniczy jako ogólna teoria prawa".

Podstawą, na której oparta została ta teoria, jest pojęcie uprawnienia. Uprawnienie jest analogiczne do powszechników w ujęciu Arystotelesa. Arystoteles twierdził, że pojęcia ogólne istnieją o tyle, o ile przejawiają się w rzeczach (prof. Kazimierz Twardowski pisał w odniesieniu do Arystotelesa o uobecnianiu się pojęć w rzeczach[138]). Ja twierdzę – idąc tą sama drogą – że prawa na przykład takie, jak prawo własności czy prawa, które zapisane są w RODO, istnieją o tyle, o ile przejawiają się w konkretnych uprawnieniach konkretnych osób.

---

[136] Z. Ziembiński, *Logika praktyczna*, Warszawa 1995, s. 234.

[137] Ch. Poszwiński, op. cit., s. 58.

[138] K. Twardowski, *O filozofii średniowiecznej wykładów sześć*, Warszawa 1910, s. 6.

Uprawnienie jest cechą osoby fizycznej, której przysługuje. Dopiero z uprawnienia wynika obowiązek.

Wyobraźmy sobie na przykład prawo do przetwarzania danych osobowych w sposób ograniczony co do zakresu, zapisane w zasadzie minimalizacji. Pozornie w zasadzie tej przede wszystkim zapisany jest obowiązek, co wnosić można z językowej warstwy zasady. Wystarczy jednak wyobrazić sobie administratora, który nie przetwarza danych osobowych konkretnej osoby fizycznej, w takiej sytuacji wobec tej osoby fizycznej ten administrator nie ma żadnego obowiązku i dopiero, jeśli dane osobowe tej osoby znajdą się (powiedzmy) w organizacji administratora, to wtedy po stronie administratora pojawia się stosowny obowiązek. Widać więc, że obowiązek niejako przynosi osoba fizyczna razem ze swoimi danymi i ze swoim uprawnieniem. Oczywiście dane nie muszą zostać przyniesione przez osobę, której dotyczą, mogą trafić do administratora inną drogą, tym niemniej prawo tej osoby jest z nimi ściśle związane i dopiero z tego prawa wynika obowiązek administratora. Jednocześnie stosunek prawny nie zachodzi między administratorem a danymi, ani między osobą, której dane dotyczą, a danymi. Stosunek prawny zachodzi między administratorem a osobą, której dane dotyczą. Zachodzi, tyle że pojawia się on dopiero wtedy, kiedy dane osobowe – o czym piszę wyżej – znajdą się „w organizacji" administratora, czyli, inaczej ujmując, stosunek prawny między administratorem a osobą, której dane dotyczą, pojawia się dopiero, kiedy podmiot staje się administratorem w odniesieniu do danych tej konkretnej osoby.

Fakt, że w przepisie (odnoszę się tu do zasady minimalizacji) zapisany jest obowiązek przetwarzania danych w sposób ograniczony co do zakresu (nie zaś uprawnienie lub wolność), ma jedynie znaczenie językowe. Z punktu widzenia całości relacji, która zachodzi między administratorem (danych osobowych) a osobą, której dane dotyczą, nie ma znaczenia, czy w przepisie zapisany jest obowiązek, prawo, czy (raczej tego się nie stosuje) wolność. Przepis, na co należy zwrócić uwagę, jest jedynie fizykalnym (fizycznym, faktycznym, graficznym, zapisanym) śladem uprawnienia, przepis jest zjawiskiem językowym zapisanym graficznie, a zapisanym dlatego, że współcześnie żyjemy w kulturze słowa pisanego i nie uczymy się przepisów na pamięć.

Uprawnienie jest konkretyzowane dwa razy. Pierwszy raz uprawnienie jest konkretyzowane przez prawodawcę na etapie formułowania przepisu. Przechodząc na chwilę na siatkę pojęciową, która funkcjonuje w Republice Czeskiej, możemy stwierdzić, że na etapie formułowania przepisu prawodawca formułuje prawo w znaczeniu obiektywnym. Drugi raz uprawnienie jest konkretyzowane na etapie interpretacji przepisów w konkretnym stanie faktycznym. Przechodząc i tu na czeską siatkę pojęciową, możemy stwierdzić, że na tym etapie interpretator formułuje prawo w znaczeniu subiektywnym[139].

Podkreślenia wymaga, że między przepisem a prawem, obowiązkiem i wolnością, które zapisane są w przepisie, nie ma żadnych dodatkowych łączników, które występują na przykład w normatywizmie i noszą tam nazwę norm.

Jest zatem przepis. Przepis składa się ze słów. Słowa mają znaczenie. Dzięki znaczeniu słów, interpretator ustala, komu jakie uprawnienie przysługuje, na kim jaki obowiązek spoczywa, i kogo jaka wolność chroni. Uprawnienie jest – jak wskazuję wyżej – cechą osoby fizycznej. Cecha ta jest rozumiana na etapie interpretacji przepisu przez interpretatora, a na etapie tworzenia przepisu, w sensie potencjalnym czy też obiektywnym, przez twórcę przepisu (piszę wyżej o dwuetapowej konkretyzacji uprawnień).

Należy zwrócić uwagę, że prawo w proponowanym ujęciu nie potrzebuje żadnych dodatkowych źródeł. Prawo istnieje, ponieważ istnieje świat czy też byt. Świat, byt – co wiemy od Parmenidesa – jest ciągły, nie zaczyna się, nie kończy, nie ma przerw ani stopni. W związku z tym, uprawnienie, które istnieje w sensie rozumowym, istnieje nie mniej niż osoba, która rozumie to uprawnienie, czyli w której rozumie, czy też umyśle się ono pojawia i nie mniej niż osoba, której to uprawnienie przysługuje i oczywiście nie mniej niż osoba, na której spoczywa obowiązek z uprawnienia wynikający. Uprawnienie nie może istnieć w sensie niższym, słabszym czy innym niż osoby, którym przysługuje, ponieważ byt nie ma stopni, coś nie może być bardziej lub mniej od czegoś innego. Jeśli coś jest, to po prostu jest. Pozornie są to truizmy, stają się takimi dopiero, kiedy je wypowiemy, a zwłaszcza kiedy zrozumiemy ich doniosłe znaczenie.

[139] A. Gerloch, *Teorie práva*, 8 vyd. Plzeň 2021, s. 23.

Wskazane tu pozorne truizmy pozwalają wskazać, że nie ma żadnego problemu w wykazaniu związku między przepisem a rzeczywistością, do której przepis się odnosi. Odnoszę się tu do normatywistycznego pseudoproblemu, z wykazaniem związku między sferą powinności a sferą istnienia. Różnica między *sein* a *sollen* jest niczym więcej jak normatywistycznym, niepotrzebnym wymysłem.

Dowodem na istnienie uprawnienia – co wynika z ustaleń czeskiego ontologa profesora Zbynka Fischera, znanego jako Egon Bondy – jest istnienie odpowiadającego mu obowiązku. Uważam tak, ponieważ Egon Bondy przedkłada, że dowodem na istnienie czegokolwiek, w tym (a może nawet zwłaszcza) na istnienie świata i oczywiście jego składowych jest to, że w świecie obserwowalne są zmiany czy też fazy[140]. Różnica między prawem i obowiązkiem jest taką właśnie zmianą. Podobną zmianą jest różnica między prawem jednej osoby a prawem drugiej osoby.

Pozostając przy ustaleniach E. Bondego, należy zwrócić uwagę, że wbrew temu, co moglibyśmy na pierwszy rzut oka przyjąć, prawo i obowiązek nie są swoimi przeciwieństwami, a jedynie się uzupełniają, E. Bondy mówi o tożsamości przeciwieństw[141]. Wynika z tego, że w sensie ontologicznym, czyli w sensie istnienia, prawo i obowiązek są tym samym, czyli cechami osoby, której prawo przysługuje.

Jest to myśl na tyle istotna, że należy ją sformułować raz jeszcze: zarówno prawo, jak i obowiązek są cechami osoby, której prawo przysługuje. Jest to istotne też na gruncie RODO, gdzie znaczna część przepisów sformułowana jest w postaci obowiązków, są to jednak obowiązki, w których zapisane są przede wszystkim uprawnienia, czyli prawa osób, których dane dotyczą.

Na temat prawa i obowiązku, a zwłaszcza ich ścisłego związku, należy poczynić pewną jeszcze uwagę. Otóż immanentną cechą obowiązku jest jego obowiązywanie. Brzmi to pozornie banalnie, jeżeli jednak obowiązek by nie obowiązywał, nie wywoływałby specyficznych dla siebie skutków po stronie osoby zobowiązanej i po stronie

---

[140] E. Bondy, *Když jsem všecko napsal, zůstala mi kategorie procesu; ale co to je, ne–li prázdné slovo?,* [w:] E. Bondy, *Příběh o příběhu*. Praha 2009, s. 37.

[141] E. Bondy, *Potíže z identitou protikladů: cesty k poznání však bývají nejen křivolaké, ale leckdy i pro smích; kdybych chtěl být učencem, byl bych toto líčeni raději přeskočil a předložil elegantni výsledek; zatím se jen ukázalo, že s dialektikou to było nějak vágní,* [w:] E. Bondy. *Příběh o příběhu,* Praha 2009, s. 32.

osoby uprawnionej, to nie byłby obowiązkiem. W takim razie, jak widać, immanentną cechą obowiązku jest jego stałe powiązanie z odpowiadającym mu uprawnieniem. Jednocześnie system zbudowany z obowiązku i uprawnienia służy ochronie wolności.

Na marginesie prowadzonych rozważań zwracam uwagę, że zarówno myśl E. Bondego, jak i konceptualizm prawniczy są zbieżne z teorią W.N. Hohfelda, tyle że W.N. Hohfeld, w duchu jurysprudencji analitycznej, zajmuje się analizą znaczenia pojęć, E. Bondy zajmuje się ich istnieniem, ja zaś, korzystając z ustaleń E. Bondego i Arystotelesa, zajmuję się istnieniem praw, obowiązków i wolności.

3.28. Art. 24 Uwaga 28

Ryzyko. Pojęcie na gruncie art. 24

Niezwykle ciekawą obserwację poczynił A. Krasuski, otóż zauważył on, że prawodawca unijny *Nie zdefiniował […] pojęcia „ryzyko" […]*[142]. Podobną konstatację znajdujemy u D. Lubasza i E. Bielak-Jomaa[143]. Brak definicji tego pojęcia w akcie prawnym wydaje się być w swoim rodzaju niezwykły. Prawodawca na gruncie RODO posługuje się tym pojęciem wiele razy. Dla potrzeb tej książki dość powiedzieć, że ryzyko musi być brane pod uwagę na gruncie art. 24, 32, 33 i 34 RODO. Za każdym razem jest to ryzyko naruszenia praw i (sic!) wolności osób fizycznych. Co ciekawe, samo pojęcie „ryzyko" jest do znalezienia w jednej z norm. Czytamy, że: *Ryzyko jest kombinacją następstw, które mogą być wynikiem zajścia niepożądanego zdarzenia oraz prawdopodobieństwa zaistnienia tego zdarzenia*[144].
Podobną konstatację wyczytać można u T. Izydorczyka i M. Gumularza, którzy piszą, że: *żaden z przepisów RODO nie definiuje, czym jest ryzyko naruszenia praw lub wolności osób fizycznych*[145]. Konstatacja ta jest trafna, z tym jednak uzupełnieniem, że o ile samej

[142] A. Krasuski, [w:] A. Krasuski, P. Siembida, *Analiza ryzyka w ochronie danych osobowych,* Warszawa 2022, s. 21.

[143] E. Bielak-Jomaa, D. Lubasz, op. cit., s. 29.

[144] PN–ISO/IEC 27005:2014–01. *Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji*, s. 20.

[145] M. Gumularz, T. Izydorczyk, op. cit., s. 41.

definicji ryzyka w RODO nie znajdziemy, o tyle składowe oceny tegoż ryzyka – owszem, znajdziemy w RODO.

W art. 24 ust. 1 RODO czytamy: *Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać.* Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

Dla zrozumienia ryzyka na gruncie art. 24 RODO mamy zatem dwie składowe, wymieniam je poniżej:

1) ryzyko jest kombinacją następstw, które mogą być wynikiem zajścia niepożądanego zdarzenia, oraz prawdopodobieństwa zaistnienia tego zdarzenia,
2) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

Kiedy następnie dokonamy podstawienia, to prawdopodobnie dowiadujemy się, że:

– „ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze jest kombinacją następstw naruszenia praw i wolności osób fizycznych i prawdopodobieństwa zaistnienia naruszenia praw i wolności osób fizycznych".

Dalsza lektura art. 24 RODO prowadzi jednak do kolejnych wniosków. Otóż z przepisu wynika, że celem oceny ryzyka i następnie wdrożenia środków organizacyjnych i technicznych jest: *aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać*. Wiemy więc, o jakie następstwo naruszenia praw i wolności osób fizycznych chodzi. Następstwem, do którego odnosi się prawodawca w przepisie, jest przetwarzanie **nie**zgodnie z RODO.

Kiedy dokonamy kolejnego podstawienia to widzimy, że :

– „ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze jest kombinacją przetwarzania niezgodnie z RODO i prawdopodobieństwa zaistnienia naruszenia praw i wolności osób fizycznych".

Głębsze zastanowienie prowadzi jednak do wniosku, że interpretator przepisu musi uczynić tu pewną intelektualną pętlę. Należy bowiem zadać sobie pytanie o to, czym jest „przetwarzanie niezgodnie z RODO". Odpowiedzi może paść chyba wiele, wydaje się jednak, że

najlepsza i najkrótsza odpowiedź brzmi, że przetwarzanie niezgodnie z RODO to przetwarzanie niezgodnie z art. 5 RODO. Uważam tak, ponieważ art. 5 RODO niejako spina, łączy prawa, obowiązki i wolności, które wynikają z poszczególnych przepisów RODO. Artykuł 5 RODO ustanawia zasady dotyczące przetwarzania danych osobowych, czyli nic innego, jak prawa i wolności dotyczące przetwarzania danych osobowych. Wykonawszy zatem tę pętlę i kolejne podstawienie otrzymujemy definicję ryzyka zaprezentowaną poniżej.

– „Ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze jest kombinacją naruszenia praw i wolności osób fizycznych, które są zdefiniowane w art. 5 RODO i prawdopodobieństwa zaistnienia naruszenia (tych) praw i wolności osób fizycznych".

O ile można zgodzić się z przytoczoną na początku uwagi tezą A. Krasuskiego, zgodnie z którą prawodawca w RODO nie definiuje ryzyka w RODO, o tyle teza, zgodnie z którą, w odniesieniu do ryzyka, prawodawca *[...] nie określa kryteriów jego ustalenia*[146], jest wątpliwa. Faktem jest, że może kryteriów ustalenia prawodawca nie określa, ale ten sam prawodawca w art. 32 ust. 2 RODO wskazuje, jakie zdarzenia o charakterze zagrożeń należy brać pod uwagę przy ocenianiu ryzyk.

3.29. Art. 24 Uwaga 29

Ryzyko. Pojęcie na gruncie art. 32

Analogiczne jak w poprzedniej uwadze rozumowanie można przeprowadzić wobec ryzyka na gruncie art. 32 RODO. W art. 32 ust. 1 RODO czytamy m.in., że: *Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku [...]*.

W art. 32 ust. 2 RODO czytamy, że: *Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wią-*

[146] A. Krasuski, op. cit., s. 35.

żące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Tu również możemy użyć definicji ryzyka znajdującej się w normie. Czytamy więc, że: *Ryzyko jest kombinacją następstw, które mogą być wynikiem zajścia niepożądanego zdarzenia, oraz prawdopodobieństwa zaistnienia tego zdarzenia*[147].

Z uwagi na obecność art. 32 ust. 2 RODO, rozumowanie przeprowadzone na gruncie art. 32 RODO jest nieco inne niż przeprowadzone na gruncie art. 24 RODO.

Składowe definicji, z którymi mamy tu do czynienia, wymieniam poniżej, dwie pierwsze pokrywają się ze składowymi z rozumowania prowadzonego na gruncie art. 24 RODO, ale trzecia zmienia rozumowanie.

1. *Ryzyko jest kombinacją następstw, które mogą być wynikiem zajścia niepożądanego zdarzenia, oraz prawdopodobieństwa zaistnienia tego zdarzenia.*
2. *Ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze*.

Trzecia składowa rozumowania, którą trzeba wziąć pod uwagę, wynika z art. 32 ust. 2 RODO. Jest to:

3. *Ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.*

Z definicji z normy widać, że ryzyko ma dwie składowe, następstwa zdarzenia i prawdopodobieństwo zdarzenia. Lektura art. 32 RODO każe sądzić, że następstwa, o których mowa, to naruszenie praw i wolności osób fizycznych.

Najpierw łączymy pierwszą i drugą składową definicji. Otrzymujemy wtedy: ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze *jest kombinacją naruszenia*

[147] PN–ISO/IEC 27005:2014–01. *Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji*, s. 20.

praw lub wolności osób fizycznych i prawdopodobieństwa zaistnienia naruszenia praw lub wolności osób fizycznych.

Należy zwrócić uwagę na fakt, że o ile „naruszenie praw i wolności osób fizycznych" ma przypisane w przepisie prawdopodobieństwo i wagę, o tyle w art. 32 ust. 2, w którym mowa jest o zagrożeniach technicznych, nie ma mowy o prawdopodobieństwie i wadze zaistnienia tych zagrożeń, a jedynie o ryzyku, które wynika z ich zaistnienia. Jednocześnie lektura art. 32 ust. 1 RODO i art. 32 ust. 2 RODO każe sądzić, że ocena ryzyka przeprowadzana na gruncie art. 32 ust. 2 RODO poprzedza ocenę ryzyka przeprowadzoną na gruncie art. 32 ust. 1 RODO.

Po podstawieniu pozostają zatem dwie składowe, wymieniam je poniżej.

1. Ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze jest kombinacją naruszenia praw lub wolności osób fizycznych i prawdopodobieństwa zaistnienia naruszenia praw lub wolności osób fizycznych.
2. Ryzyko wiążące się z przetwarzaniem danych osobowych, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Mamy zatem dwa ryzyka: ryzyko naruszenia praw i wolności osób fizycznych i ryzyko wiążące się z przetwarzaniem. Wydaje się, że można poczynić tu pewien dalszy i radykalny krok, najpierw jednak trzeba uświadomić sobie pewne zjawiska.

Ryzyko wiążące się z przetwarzaniem danych osobowych to właśnie ryzyko naruszenia praw i wolności osób fizycznych. Dane nie mają praw, ludzie mają prawa. Kiedy zachodzi jakieś zagrożenie techniczne lub organizacyjne dla danych, to tym samym zachodzi zagrożenie dla praw i wolności osób fizycznych.

Konkretne zagrożenia techniczno-organizacyjne skutkują zagrożeniem dla konkretnych praw i wolności. Patrząc na to od strony praw i wolności, konkretne prawa i wolności są zagrożone przy zagrożeniu konkretnymi zagrożeniami techniczno-organizacyjnymi. I idąc dalej… Zajście konkretnych zdarzeń o charakterze techniczno-organizacyjnym skutkuje naruszeniem konkretnych praw i wolności, zawsze tych samych przy takiej samej kategorii zdarzenia.

Po poczynieniu powyższych ustaleń okazuje się, że dwa ryzyka, o których piszę wyżej, a to ryzyko naruszenia praw i wolności osób fizycznych i ryzyko wiążące się z przetwarzaniem to w istocie jedno czy też to samo ryzyko. Podział artykułu 32 RODO na ust 1 i ust. 2 (pomijam resztę przepisu) narzuca myśl o tym, że w art. 32 ust. 1 RODO mowa jest o innym ryzyku niż w art. 32 ust. 2 RODO; że pierwsze to ryzyko naruszenia praw i wolności i że drugie to ryzyko wiążące się z przetwarzaniem. Kiedy jednak zrozumiemy, że z przetwarzaniem danych osobowych wiąże się właśnie ryzyko naruszenia praw i wolności, to okazuje się, że ryzyko o którym mowa w art. 32 ust. 1 RODO i ryzyko, o którym mowa w art. 32 ust. 2 RODO to w istocie to samo ryzyko, a jedynie inaczej nazwane. Inaczej, ponieważ każda z nazw odnosi się do innej części tego ryzyka. „Ryzyko wiążące się z przetwarzaniem danych osobowych" to nazwa dotycząca zdarzenia; „ryzyko naruszenia praw i wolności osób fizycznych" to nazwa osadzona w pojęciach prawnych i prawniczych. Zwracam uwagę, że mamy tu do czynienia z niejako dwoma etapami ustalania tego, jakie ryzyko zaszło. Zachodzi zdarzenie. Zdarzenie wiążące się z przetwarzaniem danych osobowych. To zdarzenie skutkuje naruszeniem praw i wolności. Zawsze tych samych. Jeśli więc chodzi o prawdopodobieństwo, to sensowne są rozważania dotyczące prawdopodobieństwa zajścia zdarzenia wiążącego się z przetwarzaniem danych osobowych.

I dalej, jeśli chodzi o wagę, to zdarzenie dlatego ma jakąkolwiek wagę w sferze danych osobowych, że skutkuje naruszeniem konkretnych praw i wolności. Powtórzmy, prawdopodobieństwo jest związane ze zdarzeniem, waga z prawami i wolnościami.

Przypomnijmy, mamy pozornie dwa wymienione poniżej ryzyka:

1. Ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze jest kombinacją naruszenia praw lub wolności osób fizycznych i prawdopodobieństwa zaistnienia naruszenia praw lub wolności osób fizycznych.
2. Ryzyko wiążące się z przetwarzaniem danych osobowych, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Wiemy już, że ryzyka te są w istocie tym samym ryzykiem, które w wyniku podziału przepisu na dwa ustępy sprawia wrażenie,

jakby było dwoma różniącymi się od siebie ryzykami. Kiedy dokonamy podstawień, to uzyskujemy ryzyko wskazane poniżej. (Zapisuję je w punktach, tak by łatwiej było zrozumieć co jest czym.)

– **Ryzyko** naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze
– wiążące się z przetwarzaniem danych osobowych
– **jest** kombinacją naruszenia praw lub wolności osób fizycznych
– i prawdopodobieństwa zaistnienia naruszenia praw lub wolności osób fizycznych,
– czyli prawdopodobieństwa przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Jak widać, prawdopodobieństwo zaistnienia naruszenia praw i wolności osób fizycznych i prawdopodobieństwo przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych są tym samym, można więc jedno z nich usunąć z definicji, uzyskamy wtedy definicję ryzyka wskazaną poniżej.

– **Ryzyko** naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze
– wiążące się z przetwarzaniem danych osobowych
– **jest** kombinacją naruszenia praw lub wolności osób fizycznych
– i prawdopodobieństwa przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Zaprezentowane tu podejście idealnie współgra z myślą A. Krasuskiego, który pisze, że: *Zagrożenie jest to możliwość wystąpienia określonych strat, ustalana dla sytuacji powstałej po zajściu pojedynczego zdarzenia niepożądanego w rozpatrywanym systemie człowiek–technika–środowisko*[148]. Tyle, że stratą na gruncie RODO jest naruszenie

[148] A. Krasuski, op. cit., s. 32.

nie prawa–wolności–obowiązku–zasady zapisanych w art. 5 RODO, zdarzeniem zaś jest zdarzenie wymienione w art. 32 ust. 2 RODO.

Zaprezentowane tu rozumowanie współgra nie tylko z myślą A. Krasuskiego, ale i oficjalnym stanowiskiem organów Unii Europejskiej, w którym czytamy, że: *„Ryzyko" jest scenariuszem opisującym zdarzenie i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa ryzyka*[149]. Mam tu jedynie zastrzeżenie co do określenia ryzyka jako scenariusza, nie zamierzam jednak kruszyć kopii, tym bardziej że w pełni zgadzam się ze wskazanym wyjaśnieniem ryzyka jako następstwa zdarzenia i jego konsekwencji. Pięknie pisze dalej A. Krasuski, że: *W kontekście analizy ryzyka w RODO należy zawęzić powyższe rozumienie tego pojęcia do prawdopodobieństwa wystąpienia zagrożenia w zdarzeniu niepożądanym i powstałych w związku z tym negatywnych skutków dla człowieka*[150], powołując się przy tym na M. Gumularza, mam jednak poczucie, że A. Krasuski pomija wskazywane przeze mnie w niniejszym rozdziale szczegóły dotyczące oceny ryzyka na gruncie RODO, a wynikające z art. 32 ust. 1 RODO i art. 32 ust. 1 RODO.

Wspomniany M. Gumularz wraz z T. Izydorczykiem prowadzą w swojej książce rozważanie na temat definicji ryzyka. Co ciekawe dochodzą do wniosku, że: *[...] ryzyko w RODO: jest to kombinacja prawdopodobieństwa i wagi*. Teza wskazanych autorów jest trafna, tym bardziej że na drodze półstronicowego rozważania doszli do wniosku zbieżnego z fragmentem treści art. 32 ust. 1 RODO, w którym czytamy, że: *Uwzględniając [...] ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający [...]*. Wniosek M. Gumularza i T. Izydorczyka jest o tyle wartościowszy, o ile autorzy nie zainspirowali się przepisem i do wniosku doszli sami, co jest możliwe[151], ponieważ w rozważaniach swoich przeskakują od roz-

---

[149] *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679*. Przyjęte w dniu 4 kwietnia 2017 r. Ostatnio zmienione i przyjęte w dniu 4 października 2017 r. Grupa Robocza Art. 29. 17/PL WP 248 rev.01, s. 7.

[150] A. Krasuski, op. cit., s. 35.

[151] M. Gumularz, T. Izydorczyk, op. cit., s. 45.

ważań ogólnych do wniosku, nie wskazując, że wynika on po prostu z art. 32 ust. 1 RODO.

Zaprezentowane wyżej podejście do ryzyka koresponduje też z podejściem, jakie do ryzyka wykazuje prawodawca w aktach prawnych związanych z cyberbezpieczeństwem. Zrazu w dyrektywie spotykamy nieco uproszczoną definicję ryzyka, czytamy tam, że ryzyko: *oznacza każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych*[152]. Definicja ta – mimo pewnej prostoty – zawiera sensowny przekaz, że ryzyko to coś niewłaściwego, co może się zdarzyć. W motywie 46 Preambuły tej samej dyrektywy czytamy, że: *Środki w zakresie zarządzania ryzykiem obejmują środki mające na celu identyfikację wszelkich ryzyk incydentów, zapobieganie incydentom, wykrywanie ich i postępowanie z nimi, a także łagodzenie ich wpływu*. Widać tu już nieco tę swojego rodzaju dwuczęściowość ryzyka. Koncepcja, zgodnie z którą ryzyko składa się z dwóch konkretnych części, wybrzmiewa w pełni w ustawie recypującej dyrektywę. Czytamy tam, że ryzyko stanowi *kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji*[153]. Do wskazanej dyrektywy i ustawy odnosi się A. Krasuski[154], acz raczej relacyjnie, mam poczucie, że fakt, iż we wskazanych aktach prawnych, zwłaszcza w ustawie, ryzyko ma dwa etapy, w książce, do której się odnoszę, przynajmniej w części A. Krasuskiego, nie wybrzmiewa.

Rację mają E. Bielak-Jomaa i D. Lubasz, którzy twierdzą, że:
Na szacowanie ryzyka składa się:
– identyfikowanie ryzyka,
– analiza ryzyka,
– ocena poziomu ryzyka[155].

[152] Dyrektywa 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Dz.U.UE.L.2016.194.1 z dnia 2016.07.19. Art. 4 pkt 9.

[153] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. DzU 2018.1560 ze zm. tj. Dz.U. 2022.1863. Art. 2 pkt 12.

[154] A. Krasuski, op. cit., s. 46.

[155] E. Bielak-Jomaa, D. Lubasz, op. cit., s. 31.

Rację, z tym jednak uzupełnieniem, że kluczem do identyfikacji ryzyka jest art. 32 ust. 2 RODO i art. 5 RODO, kluczem zaś do ustalenia poziomów ryzyka są art. 33 i 34 RODO.

3.30. Art. 24 Uwaga 30

Ryzyko. Pojęcie na gruncie art. 32. Stałość zależności

Andrzej Krasuski poczynił pewną ciekawą uwagę, otóż pisze on, że: *W pojęciu ryzyka może zawierać się niedobór informacji o poszczególnych elementach relacji przyczyna–skutek*[156]. W ryzyku rozumianym tak, jak rozumie je prawodawca na gruncie art. 32 RODO, nie ma tego niedoboru, wiadomo, jakie zdarzenie skutkuje naruszeniem jakiego prawa i wolności. Poszczególne zdarzenia, takie jak np. zniszczenie danych osobowych związane są z naruszeniem konkretnych praw (i wolności). Zagrożenie zdarzeniem skutkuje zagrożeniem naruszenia praw i wolności. Zajście zdarzenia skutkuje naruszeniem praw i wolności. Zależności te są stałe, mogą i powinny być wykorzystywane przy ocenianiu ryzyka na gruncie art. 32 RODO (i tym samym częściowo na gruncie art. 24 ust. 1 RODO, częściowo, ponieważ cel oceny się zmienia) i przy ocenianiu skutków naruszenia na gruncie art. 33 RODO i art. 34 RODO.

Jeśli chodzi o to, jakie prawa i wolności należy brać pod uwagę przy wszystkich ocenach, o których tu piszę, to nie mam wątpliwości, że przede wszystkim należy brać pod uwagę prawa i wolności zapisane w zasadach z art. 5 ust. 1 RODO. Wyjaśniam to w kilku miejscach tej[157] i wcześniejszych[158] książek.

Jeśli chodzi o to, czy do potrzeb ocen ryzyka należy brać pod uwagę te same zdarzenia, rozumiane jako zagrożenia, to należy wykonać pewne rozumowanie.

Do oceny ryzyka na gruncie art. 32 RODO należy brać pod uwagę zdarzenia, o których mowa w art. 32 ust. 2 RODO, co jest oczywiste

---

[156] A. Krasuski, op. cit., s. 31. A. Krasuski powołuje się na wcześniejszego autora, przypis A. Krasuskiego: T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Warszawa 2008, s. 54.

[157] Uwagi *(3. Art. 24 Uwagi. 3.1. Art. 24 Uwaga 1. Prawa i wolności*), (*3.2. Art. 24 Uwaga 2. Przykładowe prawa i wolności zasadnicze*).

[158] J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja…*; J. Rzymowski, *RODO – GDPR. Zasady…*; J. Rzymowski. *RODO – GDPR. Przedmiot i cele…*

z uwagi na treściowe związki między art. 32 ust. 1 RODO a art. 32 ust. 2 RODO. Dla uniknięcia jakichkolwiek wątpliwości zwracam uwagę, że ocena na gruncie art. 32 ust. 1 RODO jest dokonywana po to, aby wziąwszy pod uwagę wskazane w przepisie czynniki, w tym *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze,* administrator danych osobowych (podmiot przetwarzający) *zapewnił stopień bezpieczeństwa odpowiadający temu ryzyku*. I dalej w art. 32 ust. 2 RODO czytamy, że: Oceniając, czy stopień bezpieczeństwa jest odpowiedni, *uwzględnia się w szczególności ryzyko wiążące się z […]* i tu w przepisie padają kolejne zagrożenia.

Jeśli chodzi o art. 33 RODO, 34 RODO i 4 pkt 12 RODO, to zachodzą między nimi również związki treściowe. By i tu uniknąć wątpliwości, jednocześnie w art. 33 ust. 1 RODO czytamy, że: *W przypadku naruszenia ochrony danych osobowych, administrator […]* i dalej prawodawca wskazuje kolejne obowiązki administratora (danych osobowych) związane z naruszeniem ochrony danych osobowych. Dalej w art. 34 ust. 1 RODO czytamy, że: *Jeżeli naruszenie ochrony danych osobowych może powodować […]* i dalej prawodawca również prawodawca wskazuje kolejne obowiązki administratora (danych osobowych) związane z naruszeniem ochrony danych osobowych. Samo naruszenie ochrony danych osobowych zdefiniowane jest w art. 4 pkt 12 RODO.

Mając na uwadze powyższe ustalenia, należy zestawić treść art. 32 ust. 2 RODO z treścią art. 4 pkt 12 RODO. Dla uczytelnienia zestawienia czynię to poniżej w tabeli.

Art. 32 ust. 2	Art. 4 pkt 12
Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.	„naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

Art. 32 ust. 2	Art. 4 pkt 12
In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed	'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Różnica między utratą, (art. 32 ust. 2 wersja polska) a utraceniem (art. 4 pkt 12 wersja polska) i podobna różnica między modyfikacją a zmodyfikowaniem nie są to różnice, które należy brać pod uwagę. Występują one w wersji polskojęzycznej, ale w wersji anglojęzycznej ich nie ma.

Art. 32 ust. 2	Art. 4 pkt 12
Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.	„porušením zabezpečení osobních údajů“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

Jak widać, osoby odpowiedzialne za wersję czeskojęzyczną, podobnie jak ich polscy odpowiednicy, zmagały się z *disclosure of, or access to*.

Art. 32 ust. 2	Art. 4 pkt 12
Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.	„Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

Problemu tego nie miały chyba osoby odpowiedzialne za wersję niemieckojęzyczną.

Jak widać, wersja czeskojęzyczna ma swoje słabości. W art. 4 pkt 12 RODO zagubiono odpowiednik *access to*, ponieważ *poskytnutí nebo zpřístupnění* są raczej odpowiednikiem *disclosure of*. Nie wykluczam, że nie wyczuwam niuansów językowych mowy czeskiej, która jest dla mnie jednak językiem obcym.

Mając na uwadze powyższe rozważania, pomijam w dalszym wywodzie różnice między utratą a utraceniem i między modyfikacją a zmodyfikowaniem.

Wracając do pierwotnego wątku, należy poczynić pewne porządkujące podsumowania.

Zdarzenia wskazane w art. 4 pkt 12 RODO jako elementy konstytuujące naruszenie ochrony danych osobowych to te same zdarzenia, które należy brać pod uwagę przy ocenianiu ryzyka na gruncie art. 32 ust. 2 RODO.

Konkretne zdarzenia wymienione w art. 4 pkt 12 RODO i w art. 32 ust. 2 RODO są trwale związane z konkretnymi prawami (wolnościami, obowiązkami) wskazanymi w art. 5 ust. 1 RODO.

Kiedy administrator ocenia na gruncie art. 32 ust. 2 RODO prawdopodobieństwo zaistnienia konkretnych zdarzeń, to tym samym ocenia możliwość zaistnienia skutków tych zdarzeń, czyli naruszenia praw i wolności związanych z tymi zdarzeniami. Zjawisko związku między zdarzeniami z art. 32 ust. 2 RODO, a siłą rzeczy również art. 4 pkt 12 RODO a prawami i wolnościami z art. 5 RODO omawiam niżej w uwadze (*3.31. Art. 24. Uwaga 31. Zdarzenie a naruszenie prawa – zasady*).

Kiedy administrator ocenia na gruncie art. 33 RODO i art. 34 RODO skutki naruszenia ochrony danych osobowych, poprzez pryzmat art. 4 pkt. 12 RODO, to tym samym ocenia możliwość zaistnienia skutków zdarzenia, czyli możliwość naruszenia praw i wolności związanych z tymi zdarzeniem.

Mirosław Gumularz i T. Izydorczyk nie ujęli opisanego tu zjawiska stałości związku między zasadami a naruszeniami w sposób werbalny, ale w pewnym zakresie je zauważyli. Uważam tak po lekturze sformułowanej przez nich tabeli, w której zestawili zasady z zagrożeniami. Faktem jest, że tabela ta służy raczej skonkretyzowaniu zasad, poprzez wskazanie tego, jak daną zasadę naruszyć można, ale

myśl jest analogiczna. Podobne zestawienia, tyle, że oparte nie na naruszeniu zasad, a na ich realizacji przez przepisy szczegółowe RODO, zawarłem w jednej z wcześniejszych książek[159] z cyklu, a ich wersja stabelaryzowana znajduje się w książce[160], którą miałem przyjemność napisać wspólnie z D. Spałkiem.

Model rozumowania łączącego zdarzenia z art. 32 ust. 2 RODO i z art. 4 pkt 12 RODO z zasadami z art. 5 ust. 1 RODO przedstawiam poniżej w uwadze *(3.31. Art. 24. Uwaga 31. Zdarzenie a naruszenie prawa – zasady*). Propozycje zestawienia wskazanych zdarzeń z prawami i wolnościami z art. 5 ust. 1 RODO, ukazującą zachodzące między nimi stałe związki przedstawiam na końcu książki w tabeli: **Ryzyko naruszenia praw i wolności związane z zaistnieniem zagrożenia wobec konkretnej czynności z art. 32 ust. 2 RODO.**

Analogiczną, choć nieco innego dotyczącą obserwację poczynił T. Izydorczyk. Otóż powiązał on w swojej publikacji konkretne zasady ze zjawiskami, które odpowiednio: podwyższają i obniżają ryzyko naruszenia tych zasad i niejako dołożył do tego coś, co nazwał „potencjalnymi skutkami"[161], a są to zjawiska, które zajść mogą, jeżeli zasada będzie naruszona. Zestawienia te, zwłaszcza w zakresie czynników zagrożenia dla zasad, mimo swej oczywistości są ogromnie kształcące. Uważam tak, ponieważ sama możliwość poczynienia takich zestawień jest egzemplifikacją tezy o stałości zjawisk, które zachodzą w zakresie naruszenia zasad z art. 5 RODO. Co prawda T. Izydorczyk widzi związek między zasadami a czynnikami obniżającymi i podwyższającymi ryzyko ich naruszenia, ja zaś widzę związek między zdarzeniami z art. 4 pkt 12 RODO i z art. 32 ust. 2 RODO, to jednak stałość zjawisk dostrzegamy obaj. Mam pewną zasadniczą wątpliwość co do tego, czy umieszczenie w tabelach również potencjalnych skutków naruszenia zasad jest rozwiązaniem poprawnym, jest to bowiem swojego rodzaju rysowanie czarnych scenariuszy, ja zaś uważam, że z tego punktu widzenia istotne jest, jakie dane są źródłem ryzyka lub przedmiotem naruszenia, ale choć z tym zastrzeżeniem, to jednak pewną wartość porządkującą i te zestawienia mają.

---

[159] J. Rzymowski, *RODO – GDPR. Zasady dotyczące...*

[160] J. Rzymowski, red., D. Spałek, *RODO – GDPR. Ochrona danych medycznych.* Łódź 2022, s. 303–333.

[161] T. Izydorczyk, op. cit., s. 133–134.

Wspomniani wyżej M. Gumularz i T. Izydorczyk trafnie zwracają uwagę, że waga ryzyka odnosi się do negatywnych konsekwencji. Jako taką konsekwencję podają dyskryminację. Dalej jednak piszą: *Z perspektywy osób, których dane dotyczą, samo wystąpienie źródła ryzyka (zagrożenia) jeszcze nie przesądza, że wpłynie ono jakoś na te osoby. Jest ono (np. naruszenie poufności czy minimalizacji danych) mniej lub bardziej poważne , dopiero gdy rodzi lub może rodzić takie a nie inne konsekwencje (np. kradzież tożsamości)*. I dalej wskazani autorzy rysują scenariusz związany z kradzieżą tożsamości[162].

Wskazani autorzy mylnie utożsamiają naruszenie zasady „naruszenie poufności czy minimalizacji danych" ze źródłem ryzyka. Źródłem ryzyka jest zdarzenie. Naruszenie zasady jest następstwem zdarzenia, nie zaś jego przyczyną. Przypominam, że czy to dla potrzeb oceny ryzyka (art. 24 ust. 1 RODO, art. 32 ust. 1 RODO), czy to dla potrzeb oceny skutków naruszenia (art. 33 ust. 1 RODO, art. 34 ust. 1 RODO) oceniamy ryzyko naruszenia praw i wolności osób, których dane dotyczą. Najłatwiej wyjaśnić to krótko na przykładzie naruszenia. Kiedy zajdzie naruszenie ochrony danych (art. 4 pkt 12 RODO), to zostają naruszone pewne konkretne prawa i wolności związane z danym rodzajem naruszenia. Załóżmy że zostają naruszone, tak jak piszą M. Gumularz i T. Izydorczyk zasada poufności i zasada minimalizacji. Jeśli zostają naruszone, to niczego więcej do podjęcia decyzji denuncjacyjnej nie trzeba. Skoro obowiązek informowania organu ochrony danych pojawia się w związku z wysokim ryzykiem naruszenia praw i wolności, to obowiązek ten pojawia się tym bardziej, jeżeli następuje naruszenie praw i wolności. Po naruszeniu konkretnych praw i wolności nie należy się zastanawiać nad tym, co się jeszcze zdarzyć może, jest to istotne, ale tylko ze względu na szczegóły informacji przekazywanej osobie, której dane dotyczą i organowi ochrony danych. Do podjęcia decyzji niepotrzebne są czarne scenariusze. Nieco inaczej rzecz się ma, kiedy zdarzenie skutkuje jedynie ryzykiem naruszenia praw i wolności, wtedy odpowiednio do poziomu tego ryzyka, podejmować należy decyzje denuncjacyjne.

Wydaje się, że pracowite i ciekawe zmagania M. Gumularza i T. Izydorczyka są wynikiem pewnego niedostatku w rozumowaniu,

[162] Ibidem, s. 83.

czy też braku chęci do zrobienia pewnego kroku interpretacyjnego. Czytamy u nich:

RODO nie wskazuje jednak czy te parametry (wagi i prawdopodobieństwa) należy odnosić do:

– *źródła ryzyka (zwanego w niniejszej publikacji „zagrożeniami", np. brak kontroli nad zakresem pozyskiwanych danych);*
– *negatywnych konsekwencji (np. dyskryminacja) wystąpienia zagrożenia;*
– *całego złożonego stanu faktycznego (źródła i negatywnych konsekwencji)*[163].

Jak widać, wskazani autorzy zastanawiają się, co ma prawdopodobieństwo i wagę. Czy zagrożenia, czy konsekwencje, czy całość. Odpowiedź na to pytanie jest przerażająco prosta. W art. 32 ust. 1 RODO widnieją słowa: *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze*. Wynika z nich, że prawdopodobieństwo i waga są cechami ryzyka naruszenia praw i wolności osób fizycznych. Przechodząc na chwilę na siatkę pojęciową M. Gumularza i T. Izydorczyka, należy stwierdzić, że „prawdopodobieństwo wystąpienia i waga zagrożenia" są cechami „całego złożonego stanu faktycznego (źródła i negatywnych konsekwencji)". Można tu oczywiście się upierać, że prawdopodobieństwo i wagę może mieć zarówno „źródło ryzyka", jak i „negatywne konsekwencje". W takim ujęciu mielibyśmy:

– prawdopodobieństwo źródła ryzyka,
– wagę źródła ryzyka (mam poczucie, że jest to bełkot, ale staram się być konsekwentny; powiedzmy, że źródło może być poważne lub nie, acz nie mam pojęcia nawet, jakie przykłady tu wskazać),
– prawdopodobieństwo negatywnych konsekwencji wystąpienia zagrożenia,
– wagę negatywnych konsekwencji wystąpienia zagrożenia.

Poprowadziłem to rozumowanie konsekwentnie w duchu wątpliwości M. Gumularza i T. Izydorczyka. I muszę przyznać, że zwłaszcza po rozpisaniu zagadnienia, widzę, że takie podejście nie ma sensu. Jest to podejście usilnie konsekwentne, jednak przypomnijmy sobie o zasadzie ekonomiki myślenia. Wiemy, że ryzyko ma prawdopodobieństwo i wagę. Wiemy to z tekstu prawnego i tego arystotelesow-

[163] Ibidem, s. 82.

sko-ockhamowską brzytwą nie zetniemy. Ryzyko ma prawdopodobieństwo i wagę. Wracając więc do siatki M. Gumularza i T. Izydorczyka pozostaje stwierdzić, że mamy do czynienia z:
– prawdopodobieństwem źródła ryzyka,
– wagą negatywnych konsekwencji wystąpienia zagrożenia.

Dodatkowo należy zwrócić uwagę na jedno jeszcze, otóż jeżeli uświadomimy sobie, że takie samo zdarzenie skutkuje zawsze takim samymi skutkami, to prawdopodobieństwo zaistnienia zdarzenia staje się siłą rzeczy prawdopodobieństwem zaistnienia jego skutków, a o zdarzeniu i skutkach mówimy osobno, raczej ze względów jasności przekazu. Do takiego podejścia zmusza nas też prawodawca, który wskazuje zarówno zdarzenia, które należy brać pod uwagę, jak i ich skutki, czyli naruszenie jakich zasad należy brać pod uwagę.

Tytułem uzupełnienia trzeba jeszcze dodać, że kluczem do ustalenia źródła ryzyka jest art. 32 ust. 2 RODO, jeśli zaś chodzi o prawa i wolności, to zarówno koncepcja racjonalnego prawodawcy[164], jak i dyrektywa języka prawnego[165] prowadzą do praw i wolności zapisanych w art. 5 RODO, czyli do zasad.

Ciekawe ustalenia językowe, dotyczące pojęcia ryzyka, znaleźć można u Ch. Poszwińskiego, pomijam je z uwagi na prowadzone wyżej ustalenia o charakterze raczej prawniczym, uważam je jednak za warte odnotowania, tym bardziej że wspomniany autor dalej, po tych ustaleniach przechodzi do ustaleń analogicznych do tych. jakie ja prowadzę wyżej[166].

3.31. Art. 24 Uwaga 31

Zdarzenie a naruszenie prawa – zasady

Wyżej w uwadze (*3.30. Art. 24. Uwaga 30 Ryzyko. Pojęcie na gruncie art. 32. Stałość zależności*) zwracam uwagę na fakt, że zależności między zdarzeniami z art. 32 ust. 2 RODO a prawami i wolnościami, są stałe. Podkreślam, że odnoszę się do praw i wolności z art. 5 RODO, podobna zależność zachodzi prawdopodobnie też w odniesieniu do praw z KPP UE, nie jestem tego jednak pewien i sprawa

[164] L. Morawski, op. cit., s. 159–162.

[165] Ibidem, s. 93–95.

[166] Ch. Poszwiński, op. cit., s. 31–34.

wymaga zbadania. Mając na uwadze stałość zależności, prezentuję niżej, jakie zdarzenie z art. 32 ust. 2 RODO z naruszeniem jakich praw i wolności jest związane. Zdarzenia upraszczam do ich wersji podstawowych. Pełne zestawienie prezentuję w wersji tabelarycznej na końcu książki w części *Tabele pomocnicze. Zestawienia*.

Poniżej – raczej dla zaprezentowania koncepcji niż do dokładnej jej eksploracji – biorę pod uwagę jedynie pięć rodzajów ryzyka, bez dookreślających je cech, takich jak przypadkowość czy niezgodność z prawem. Również analizuję tylko fragment. Treść analiz ma charakter oczywisty, wynika z treści zasad z art. 5 RODO.

– Zniszczenie danych osobowych
– Utrata danych osobowych
– Modyfikacja danych osobowych
– Ujawnienie danych osobowych
– Dostęp do danych osobowych

Zniszczenie danych osobowych skutkuje naruszeniem wymienionych poniżej praw. We wskazanym niżej opisie biorę pod uwagę zniszczenie przypadkowe lub niezgodne z prawem oraz zniszczenie przypadkowe i niezgodne z prawem.

– Prawo do przetwarzania danych osobowych w sposób zgodny z prawem. (Zniszczenie danych poza procedurami administratora nie da się ująć w ramy art. 6 RODO, więc jest niezgodne z prawem.)
– Prawo do przetwarzania danych osobowych w sposób rzetelny. (Zniszczenie danych jest – przynajmniej do momentu poinformowania o nim osoby, której dane dotyczą – na gruncie art. 34 RODO, czynnością, o której osoba, której dane dotyczą, nie wie, co narusza zasadę rzetelności.)
– Prawo do przetwarzania danych osobowych w sposób przejrzysty. (Jeżeli dane zostają zniszczone, to osoba, której dane dotyczą, nie zna szczegółów zniszczenia danych, przynajmniej do momentu poinformowania jej o tym fakcie.)
– Prawo do przetwarzania danych osobowych w sposób ograniczony co do celu. (Zniszczenie danych może mieć jakiś cel, na przykład związany z atakiem cybernetycznym, jednak nie jest to cel, w jakim dane przetwarza administrator.)
– Prawo do przetwarzania danych osobowych w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania. (Zniszczenie danych, o którym tu mowa, nie jest

zapewne niezbędne do osiągnięcia celu przetwarzania, jakikolwiek on jest.)
– Prawo do przetwarzania danych osobowych w sposób ograniczony co do przechowywania. (Dane należy przechowywać przez czas, nieco rzecz upraszczając, określony przez administratora, zniszczenie zachodzi w innym celu lub bez jakiegokolwiek celu.)
– Prawo do przetwarzania danych osobowych w sposób integralny. (Tu naruszenie prawa jest oczywiste, nieautoryzowane zniszczenie danych wręcz idealnie narusza integralność danych.)

Utrata danych osobowych skutkuje naruszeniem wymienionych poniżej praw. Bierzemy pod uwagę utratę przypadkową lub niezgodną z prawem oraz utratę przypadkową i niezgodną z prawem.
– Prawo do przetwarzania danych osobowych w sposób zgodny z prawem.
– Prawo do przetwarzania danych osobowych w sposób rzetelny.
– Prawo do przetwarzania danych osobowych w sposób przejrzysty
– Prawo do przetwarzania danych osobowych w sposób ograniczony co do celu.
– Prawo do przetwarzania danych osobowych w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania.
– Prawo do przetwarzania danych osobowych w sposób ograniczony co do przechowywania.
– Prawo do przetwarzania danych osobowych w sposób integralny.
– Prawo do przetwarzania danych osobowych w sposób poufny.

Modyfikacja danych osobowych skutkuje naruszeniem wymienionych poniżej praw. Bierzemy pod uwagę modyfikację przypadkową lub niezgodną z prawem oraz modyfikację przypadkową i niezgodną z prawem.
– Prawo do przetwarzania danych osobowych w sposób zgodny z prawem.
– Prawo do przetwarzania danych osobowych w sposób rzetelny.
– Prawo do przetwarzania danych osobowych w sposób przejrzysty
– Prawo do przetwarzania danych osobowych w sposób ograniczony co do celu.

– Prawo do przetwarzania danych osobowych w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania.
– Prawo do przetwarzania danych osobowych w sposób prawidłowy.
– Prawo do przetwarzania danych osobowych w sposób integralny.

Ujawnienie danych osobowych skutkuje naruszeniem wymienionych poniżej praw. Bierzemy pod uwagę ujawnienie przypadkowe lub niezgodne z prawem oraz ujawnienie przypadkowe i niezgodne z prawem.
– Prawo do przetwarzania danych osobowych w sposób zgodny z prawem.
– Prawo do przetwarzania danych osobowych w sposób rzetelny.
– Prawo do przetwarzania danych osobowych w sposób przejrzysty
– Prawo do przetwarzania danych osobowych w sposób ograniczony co do celu.
– Prawo do przetwarzania danych osobowych w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania.
– Prawo do przetwarzania danych osobowych w sposób prawidłowy.
– Prawo do przetwarzania danych osobowych w sposób ograniczony co do przechowywania.
– Prawo do przetwarzania danych osobowych w sposób integralny.

Dostęp danych osobowych skutkuje naruszeniem wymienionych poniżej praw. Bierzemy pod uwagę dostęp przypadkowy lub niezgodny z prawem oraz dostęp przypadkowy i niezgodny z prawem.
– Prawo do przetwarzania danych osobowych w sposób zgodny z prawem.
– Prawo do przetwarzania danych osobowych w sposób rzetelny.
– Prawo do przetwarzania danych osobowych w sposób przejrzysty
– Prawo do przetwarzania danych osobowych w sposób ograniczony co do celu.
– Prawo do przetwarzania danych osobowych w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania.
– Prawo do przetwarzania danych osobowych w sposób poufny.

Możliwe jest też inne podejście, np. takie, jakie prezentują M. Gumularz i T. Izydorczyk. W sferze prawdopodobieństw widzą oni *zagrożenie prawa lub wolności*. Jako przykład podają *zagrożenie polegające na niewydaniu kopii danych (naruszenie art. 15 ust. 3 RODO)* i dają tu oznaczenie (zapewne prawdopodobieństwa) *niskie*. Dalej jako wagę widzą *stopień skutku (wpływu) na osobę fizyczną w przypadku wystąpienia zagrożenia.* Jako przykład wagi podają *podirytowanie osoby związane z brakiem możliwości uzyskania kopii swoich podstawowych danych* i dają tu oznaczenie (zapewne wagi) *niskie*. Jako ryzyko podają *brak wydania kopii danych skutkujące* (sic!) *podirytowaniem osoby*[167]. Dostrzegam tu elementy podejścia, które ja proponuję, ale zupełnie inaczej poukładane. Przede wszystkim naruszenie szczegółowego prawa i wolności wskazani autorzy widzą jako „prawdopodobieństwo" i oceniają je jako niskie. Fakt, jest to sprawa błaha, ale gdyby iść drogą wskazaną przez M. Gumularza i T. Izydorczyka, to należałoby być konsekwentnym i ocenić ryzyko naruszenia wszystkich praw i wolności szczegółowych, które wynikają z RODO, czyli wszystkich obowiązków nałożonych na administratora. Nie mówię, że jest to podejście niewłaściwe, co więcej jest ono zgodne z moją koncepcją, w której prawa i wolności szczegółowe na gruncie RODO składają się niejako na prawa i wolności zasadnicze wskazane w art. 5 RODO. Tyle tylko, że naruszenie takiego prawa nie jest prawdopodobieństwem, ale skutkiem. Skutkiem czynności z rejestru lub skutkiem naruszenia ochrony danych osobowych.

4. Art. 24 Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

Art. 24 ust. 1 RODO **ustanawia obowiązki**, które spoczywają na administratorze, obowiązki te są wskazane poniżej.

Administrator ma obowiązek wdrożyć i uwzględnić okoliczności wskazane w przepisie.

---

[167] M. Gumularz, T. Izydorczyk, op. cit., s. 45. Wszystkie cytaty w akapicie, do którego odnosi się przypis, pochodzą ze wskazanego miejsca.

Administrator ma obowiązek uwzględnić dwie grupy okoliczności/zjawisk przy wdrożeniu, łącznie zaś z wdrożeniem administrator ma obowiązek wziąć pod uwagę trzy grupy zjawisk.

Pierwsza grupa zjawisk, jakie administrator ma obowiązek uwzględnić, to: charakter przetwarzania, zakres przetwarzania, kontekst przetwarzania i cele przetwarzania danych osobowych.

Druga grupa zjawisk, jakie administrator ma obowiązek uwzględnić, to: ryzyko naruszenia praw i wolności osób fizycznych.

Administrator ma obowiązek uwzględnić fakt, że ryzyko naruszenia, praw i wolności osób fizycznych może mieć różne prawdopodobieństwo i różną wagę.

Tym, co administrator ma obowiązek wdrożyć, są środki odpowiednie do charakteru przetwarzania i zakresu przetwarzania, i kontekstu przetwarzania, i celów przetwarzania, i ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

Administrator ma obowiązek wdrożyć wskazane środki w konkretnym celu, a mianowicie po to, by przetwarzanie danych osobowych odbywało się zgodnie z RODO.

Administrator ma również obowiązek wdrożyć wskazane środki w drugim konkretnym celu, a mianowicie po to, by móc wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z RODO.

Jednocześnie

– art. 24 ust. 1 RODO **ustanawia uprawnienia**, które przysługują każdej osobie, której dane dotyczą, uprawnienia te są wskazane poniżej.

Osoba, której dane dotyczą, ma prawo do tego, by okoliczności wskazane w przepisie zostały uwzględnione przez administratora.

Osoba, której dane dotyczą, ma prawo do tego, by dwie grupy okoliczności/zjawisk (a łącznie z wdrożeniem, trzy grupy zjawisk) zostały uwzględnione przez administratora.

Osoba, której dane dotyczą ma prawo do tego, by administrator uwzględnił charakter przetwarzania, zakres przetwarzania, kontekst przetwarzania i cele przetwarzania danych osobowych jako pierwszą grupę zjawisk.

Osoba, której dane dotyczą, ma prawo do tego, by administrator uwzględnił ryzyko naruszenia praw i wolności osób fizycznych jako drugą grupę zjawisk.

Osoba, której dane dotyczą, ma prawo do tego, by administrator uwzględnił, że ryzyko naruszenia praw i wolności osób fizycznych może mieć różne prawdopodobieństwo i różną wagę.

Osoba, której dane dotyczą, ma prawo do tego, by administrator wdrożył środki odpowiednie do charakteru przetwarzania i zakresu przetwarzania, i kontekstu przetwarzania, i celów przetwarzania, i ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

Osoba, której dane dotyczą, ma prawo do tego, by środki, które wdraża administrator, były środkami technicznymi i organizacyjnymi.

Osoba, której dane dotyczą, ma prawo do tego, by administrator wdrożył wskazane środki w konkretnym celu, a mianowicie po to, by przetwarzanie danych osobowych odbywało się zgodnie z RODO.

Osoba, której dane dotyczą, ma prawo do tego, by administrator wdrożył wskazane środki w drugim konkretnym celu, a mianowicie po to, by mógł wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z RODO.

Osoba, której dane dotyczą, ma prawo do tego, by administrator poddawał wskazane wyżej środki techniczne i organizacyjne przeglądom, i aby administrator wskazane środki uaktualniał.

Osoba, której dane dotyczą ma prawo do tego, by administrator poddawał środki przeglądom w razie potrzeby. Potrzeba ta może wynikać z różnych okoliczności, a to ze zmian w otoczeniu faktycznym lub prawnym, lub z przepisów, lub ich zmian.

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

Art. 24 ust. 2 RODO **ustanawia obowiązki**, które spoczywają na administratorze, obowiązki te są wskazane poniżej. Przepis ten **ustanawia również uprawnienia**, te również są wskazane poniżej.

Administrator ma obowiązek zrealizować przepis, jeżeli przedmiot realizacji przepisu jest proporcjonalny do okoliczności wskazanych w przepisie.

Osobie, której dane dotyczą, przysługuje prawo (uprawnienie) polegające na tym, że jeżeli przedmiot realizacji przepisu jest proporcjonalny do okoliczności wskazanych w przepisie, to administrator musi ten przepis zrealizować.

Administrator ma obowiązek dokonania oceny, czy wdrożenie polityk ochrony danych jest proporcjonalne do czynności przetwarzania.

Osobie, której dane dotyczą, przysługuje prawo (uprawnienie) polegające na tym, że administrator ma obowiązek dokonać oceny, czy wdrożenie polityk ochrony danych jest proporcjonalne do czynności przetwarzania.

Administrator ma obowiązek dokonania oceny, jakie polityki ochrony danych będą odpowiednie.

Osobie, której dane dotyczą, przysługuje prawo (uprawnienie) polegające na tym, że administrator ma obowiązek dokonać oceny, jakie polityki ochrony danych będą odpowiednie.

Jeżeli administrator dokonawszy oceny, ustali, że polityki ochrony danych powinny być wdrożone, to ma on obowiązek je wdrożyć i zachować dowody na potwierdzenie faktu, że polityki zostały wdrożone.

Osobie, której dane dotyczą, przysługuje prawo (uprawnienie) polegające na tym, że jeżeli z dokonanej przez administratora oceny wynika, że polityki ochrony danych powinny być wdrożone, to ma on obowiązek je wdrożyć i zachować dowody na potwierdzenie faktu, że polityki zostały wdrożone.

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

Art. 24 ust. 3 RODO **ustanawia obowiązki**, które spoczywają na administratorze, obowiązki te są wskazane poniżej. Przepis **ustanawia również uprawnienia**, które również są wskazane poniżej.

W sytuacji, kiedy administrator stosuje zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji, na administratorze spoczywa obowiązek polegający na tym, że jeden lub drugi ze wskazanych elementów, lub obydwa jednocześnie mogą być wykorzystane, jedynie jako element służący wykazaniu realizacji obowiązków ciążących na nim.

W sytuacji, kiedy administrator stosuje zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji, osobie, której dane dotyczą, przysługuje prawo (uprawnienie) polegające na tym, że jeden lub drugi ze wskazanych elementów, lub obydwa jednocześnie mogą być wykorzystane przez administratora jedynie jako element służący wykazaniu realizacji obowiązków ciążących na nim.

W sytuacji, kiedy administrator stosuje zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji, na administratorze lub na organie kontrolnym, lub na sądach spoczywa obowiązek polegający na tym, że jeden lub drugi ze wskazanych elementów, lub obydwa jednocześnie mogą być wykorzystane jedynie jako element służący do stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

W sytuacji, kiedy administrator stosuje zatwierdzony kodeks postępowania lub zatwierdzony mechanizm certyfikacji, osobie, której dane dotyczą, przysługuje prawo (uprawnienie) polegające na tym, że jeden lub drugi ze wskazanych elementów, lub obydwa jednocześnie mogą być wykorzystane przez administratora lub przez organ kontrolny, lub przez sądy jedynie jako element służący wykazaniu realizacji obowiązków ciążących na administratorze.

5. Art. 24 ust. 1 Konkretyzacja zasad

Art. 24 RODO konkretyzuje wymienione poniżej zasady.

Przy omawianiu konkretyzacji zasad korzystam z ustaleń, które poczyniłem dla potrzeb książki *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*[168].

Zasada zgodności z prawem

Artykuł 24 ust. 1 RODO sprzyja realizacji zasady zgodności z prawem[169]. Świadczą o tym słowa *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]* Przetwarzanie danych osobowych zgodne z RODO to zjawisko szersze niż przetwarzanie zgodne z zasadą zgodności z prawem.

Przetwarzanie zgodne z zasadą zgodności z prawem to przetwarzanie zgodne z art. 6 RODO i ewentualnie z art. 9 RODO, i czasem z art. 10 RODO. Przetwarzanie zgodne z RODO, o którym mowa w art. 24 RODO, to po prostu przetwarzanie z poszanowaniem przepisów RODO.

---

[168] J. Rzymowski, *RODO – GDPR. Zasady dotyczące...* Nie zamieszczam przypisu do każdej z zasad we wskazanej książce, bo przypisy te wskazywałyby nieustannie prawie w te same miejsca, co nie ma sensu. Czytelników nieprzekonanych do przyjętego tu rozumienia zasad z art. 5 RODO zachęcam do lektury wskazanej książki.

[169] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679...*, Kom. do art. 24.

To poszanowanie powinna właśnie sprawdzać ocena wykonywana na podstawie ar. 24 RODO.

Niezwykle ciekawą myśl sformułował P. Fajgielski, brzmi ona: *Obowiązek zapewnienia zgodności przetwarzania danych z prawem wynika z zasady legalności przetwarzania, określonej w art. 5 ust. 1 lit. a, przy czym nie jest on ograniczony jedynie do oparcia przetwarzania na odpowiedniej podstawie prawnej […], ale obejmuje szeroko rozumianą zgodność z wszystkimi wymogami określonymi w przepisach o ochronie danych*[170]. Myśl wyrażona przez P. Fajgielskiego nie wymaga szczególnych komentarzy ni rozwinięcia – jest precyzyjna, jednak czuję potrzebę pewnego uzupełnienia. Otóż P. Fajgielski pisze o zgodności *z wszystkimi wymogami określonymi w przepisach o ochronie danych*, podczas gdy w art. 24 ust. 1 RODO mowa jest o tym, że przetwarzanie odbywać ma się *zgodnie z niniejszym rozporządzeniem*, czyli z RODO. Różnica ta jest o tyle istotna, że o ile należy przetwarzać dane zgodnie nie tylko z RODO, ale również właśnie z innymi niż RODO przepisami, o tyle art. 24 RODO dotyczy przetwarzania zgodnego z RODO.

Zasada rzetelności

Artykuł 24 RODO sprzyja również realizacji zasady rzetelności. Świadczą o tym słowa przepisu: *[…] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem […]* Przetwarzanie zgodne z RODO to m. in. przetwarzanie zgodne z zasadą rzetelności, czyli w takich warunkach, w których osoba, której dane dotyczą, wie, że jej dane są przetwarzane i wie, kto jest administratorem tych danych. Zasada ta jest stosowana przez realizację obowiązków wynikających odpowiednio z art. 13 RODO i z art. 14 RODO. Sprawdzenie, czy przetwarzanie odbywa się zgodnie z RODO, powinno m.in. objąć sprawdzenie, czy przetwarzania odbywa się zgodnie z art. 13 i z art. 14 RODO, w zakresie zasady rzetelności.

[170] Ibidem.

Zasada przejrzystości

Artykuł 24 RODO sprzyja również realizacji zasady przejrzystości. Świadczą o tym słowa przepisu: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]*

Przetwarzanie zgodne z RODO to m. in. przetwarzanie zgodne z zasadą przejrzystości, czyli w takich warunkach, w których osoba, której dane dotyczą, zna szczegóły dotyczące przetwarzania jej danych. Zasada ta jest stosowana przez realizację obowiązków wynikających odpowiednio z art. 13 RODO i z art. 14 RODO. Sprawdzenie, czy przetwarzanie odbywa się zgodnie z RODO, powinno m.in. objąć sprawdzenie, czy przetwarzania odbywa się zgodnie z art. 13 i z art. 14 RODO, w zakresie zasady przejrzystości.

Zasada ograniczenia celu

Artykuł 24 RODO sprzyja również realizacji zasady ograniczenia celu. Świadczą o tym słowa przepisu: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]* Przetwarzanie zgodne z RODO to m.in. przetwarzanie zgodne z zasadą ograniczenia celu. *Przetwarzanie danych osobowych zgodne z zasadą ograniczenia celu to przetwarzanie w taki sposób, że administrator przetwarza dane w celach określonych odpowiednio w rejestrze czynności przetwarzania danych osobowych oraz na gruncie art. 13 RODO lub 14 RODO lub 15 RODO*.

Zasada minimalizacji danych

Artykuł 24 RODO sprzyja również realizacji zasady minimalizacji danych. Świadczą o tym słowa przepisu: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]* Przetwarzanie zgodne z RODO to m.in. przetwarzanie zgodne z zasadą minimalizacji danych. *Przetwarzanie danych osobowych zgodne z zasadą minimalizacji danych oznacza obowiązek przetwarzania danych osobowych w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane*.

Zasada prawidłowości

Artykuł 24 RODO sprzyja również realizacji zasady prawidłowości. Świadczą o tym słowa przepisu: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]* Przetwarzanie zgod-

ne z RODO to m.in. przetwarzanie zgodne z zasadą prawidłowości. Przetwarzanie danych osobowych zgodne z zasadą prawidłowości oznacza przetwarzanie *danych osobowych w taki sposób, by były one prawidłowe i w razie potrzeby uaktualniane. Zasada prawidłowości danych oznacza również obowiązek podjęcia wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.*

Zasada ograniczenia przechowywania

Artykuł 24 RODO sprzyja również realizacji zasady ograniczenia przechowywania. Świadczą o tym słowa przepisu: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]* Przetwarzanie zgodne z RODO to m.in. przetwarzanie zgodne z zasadą ograniczenia przechowywania. Przetwarzanie danych osobowych zgodne z zasadą ograniczenia przechowywania oznacza przetwarzanie *danych osobowych przez ograniczony czas*.

Zasada integralności

Artykuł 24 RODO sprzyja również realizacji zasady integralności. Świadczą o tym słowa przepisu: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]* Przetwarzanie zgodne z RODO to m.in. przetwarzanie zgodne z zasadą integralności. Przetwarzanie danych osobowych zgodne z zasadą integralności oznacza przetwarzanie *danych osobowych w taki sposób, by modyfikacja danych, w tym zniszczenie lub uszkodzenie, zachodziły jedynie w sposób autoryzowany przez administratora.*

Zasada poufności

Artykuł 24 RODO sprzyja również realizacji zasady poufności. Świadczą o tym słowa przepisu: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]* Przetwarzanie zgodne z RODO to m.in. przetwarzanie zgodne z zasadą poufności. Przetwarzanie danych osobowych zgodne z zasadą poufności oznacza przetwarzanie *danych osobowych w taki sposób, by były one ujawniane jedynie uprawnionym podmiotom lub osobom*.

Szczególnie zwracają na to uwagę P. Barta, M. Kawecki, P. Litwiński, u których znajdujemy stwierdzenie, zgodnie z którym art. 24

RODO jest *emanacją* zasady integralności i zasady poufności[171]. Wskazani autorzy piszą co prawda o jednej zasadzie, łącząc integralność i poufność w jedno, mimo że są to zjawiska odmienne i osobne, a jedynie wspomniane w tym samym przepisie RODO.

Zasada odpowiedzialności administratora (danych osobowych)

Artykuł 24 RODO sprzyja szczególnie realizacji zasady odpowiedzialności administratora danych (osobowych). Świadczą o tym słowa przepisu: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]* Przetwarzanie zgodne z RODO to m.in. przetwarzanie zgodne z zasadą odpowiedzialności administratora danych (osobowych).

Zasada odpowiedzialności administratora oznacza, że administrator ma obowiązek przestrzegać zasad z art. 5 ust. 1 RODO. Zasady z art. 5 ust. 1 RODO są realizowane przez przepisy szczegółowe RODO, czyli zasada odpowiedzialności administratora oznacza, że administrator ma obowiązek przestrzegać przepisów RODO. W związku z treścią zasady, realizacja art. 24 RODO sprzyja realizacji tej zasady w szczególny sposób.

Zasada rozliczalności

Artykuł 24 RODO sprzyja również realizacji zasady rozliczalności i w dodatku czyni to w szczególnie widoczny sposób. Świadczą o tym słowa przepisu: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]* Szczególnie świadczą o tym słowa: *i aby móc to wykazać.* Przetwarzanie zgodne z RODO to m.in. przetwarzanie zgodne z zasadą rozliczalności. Jednocześnie obowiązek wykazania zgodności przetwarzania danych osobowych z prawem jest w zasadzie powtórzeniem obowiązku wykazania realizacji zasad z art. 5 ust. 1 RODO, zapisanego w art. 5 ust. 2 RODO. Sam obowiązek przetwarzania w zgodzie z RODO jest niejako powtórzeniem obowiązku zawartego w części wprowadzającej art. 5 ust. 1 RODO.

Zasada rozliczalności oznacza, że administrator ma obowiązek **wykazania przestrzegania zasad wynikających z art. 5 ust. 1 RODO**. Zasady z art. 5 ust. 1 RODO są realizowane przez przepisy szczegóło-

[171] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 283.

we RODO, czyli obowiązek wykazania przestrzegania zasada oznacza obowiązek wykazania przestrzegania przepisów szczegółowych RODO.

Realizacja art. 24 RODO umożliwia wykazanie realizacji przepisów RODO i tym samym właśnie w sposób szczególny sprzyja realizacji zasady rozliczalności. Jednocześnie z zasady rozliczalności wynika obowiązek zachowywania dowodów na to, że zrealizowano art. 24 RODO. Jeżeli art. 24 RODO jest realizowany w praktyce łącznie z art. 32 ust. 1 RODO i 32 ust. 2 RODO, to zachowanie dowodów na jednoczesną realizację obydwu obowiązków wydaje się wystarczające.

Istotny związek art. 24 RODO z zasadą rozliczalności dostrzegają autorzy czeskiego komentarza. Mylą, co prawda zasady, czy też może raczej łączą, tak jak łączy je przepis, zasadę odpowiedzialności z zasadą rozliczalności, zwracają oni jednak, przy omawianiu art. 24 RODO uwagę na pewien fakt. Wskazują otóż, że obowiązkiem administratora jest dbałość o zgodność z RODO, jak również wskazują na obowiązek możliwości wykazania tej zgodności, co jest – jak uważam – istotą zasady rozliczalności[172].

6. Art. 24 Postulaty *de lege ferenda*

6.1. Art. 24 Postulat 1

Zastąpienie przecinków literami „i”

Fragment przepisu, którego dotyczy niniejszy postulat ma następującą treść: *Uwzględniając charakter, zakres, kontekst*. Uważam, że niewłaściwe jest użycie w zacytowanym fragmencie przepisu przecinków. Przecinki te można rozumieć jako wyrazy „lub” albo jako wyrazy „i”, a to z kolei prowadzi do wniosku, zgodnie z którym w wyniku interpretacji przepisu uzyskać można jego znaczenie, z którego wyłączone są niektóre fragmenty przepisu połączone odpowiednimi przecinkami, kiedy przecinki uznamy za „lub”.

Faktem jest, że w przedmiotowym fragmencie przecinki powinny być rozumiane jako „i”[173], jednak niewłaściwe ich zrozumienie, czyli jako „lub” może prowadzić do poważnego wypaczenia treści przepisu. Szerzej analizuję to w podrozdziale (*2. Art. 24. Analiza),*

[172] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit., s. 247.

[173] A. Malinowski, op. cit., s. 89.

przy okazji analizy słów: *uwzględniając charakter, zakres, kontekst i cele przetwarzania*.

Dla uniknięcia niekorzystnej sytuacji interpretacyjnej należy zastąpić znajdujące się w cytowanym fragmencie przepisu przecinki literami „i" lub ich odpowiednikami. W związku z powyższym postuluję nowelizację art. 24 ust. 1 RODO we wskazany poniżej sposób.

Postuluję, by fragment przepisu, o którym tu mowa, miał postać: „Uwzględniając charakter **i** zakres **i** kontekst"
(Czcionką pogrubioną i podkreśloną zaznaczam elementy wstawione do przepisu.)

6.2. Art. 24 Postulat 2

Zastąpienie słowa „lub" słowem „i"

Wyżej w uwadze (*3.1. Art. 24 Uwaga 1. Co regulują zasady z art. 5 RODO*), podnoszę, że zasady z art. 5 ust. 1 RODO to w istocie obowiązki administratora, czyli prawa (uprawnienia) osób, których dane dotyczą, czyli wolności tych osób. Można się spierać, że z zasady niesprzeczności wynika, że obowiązek jest czym innym niż prawo i że obowiązek jest czym innym niż wolność i że prawo jest czym innym niż wolność. Owszem, można. Trzeba jednak jednocześnie przyznać, że zasady z art. 5 ust. 1 RODO regulują obowiązki i prawa i wolności. Skoro zasady regulują obowiązki i prawa i wolności, to nie ma sensu mówić o prawach w oderwaniu od wolności. Jak piszę wyżej: poprawniej jest mówić o „prawach i wolnościach", nie zaś o „prawach lub wolnościach", ponieważ kiedy chronimy jedne, to chronimy również drugie.

W związku z powyższym postuluję nowelizację art. 24 ust. 1 RODO we wskazany poniżej sposób.

Postuluję, by fragment przepisu, o którym tu mowa, miał postać: „ryzyko naruszenia praw ~~lub~~ **i** wolności osób fizycznych".

(Czcionką przekreśloną zaznaczam element usunięty z przepisu, czcionką wytłuszczoną i podkreśloną zaznaczam element wstawiony do przepisu.)

6.3. Art. 24 Postulat 3

Korekta treści przepisu

Wyżej, w podrozdziale (*2.2 Art. 24.ust. 2 Analiza*), zajmuję się przepisem w zakresie: *Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych*.

Dochodzę tam do wniosku, że użycie liczby mnogiej może stworzyć mylne wrażenie, że należy nie wdrażać żadnej polityki ochrony danych (jeżeli jest to proporcjonalne), natomiast (również jeżeli jest to proporcjonalne) należy stworzyć co najmniej dwie polityki ochrony danych. Zauważam tam też, że nie ma powodu, by uważać, że niewłaściwe jest wdrożenie na przykład jednej takiej polityki.

W związku z powyższym postuluję nowelizację art. 24 ust. 2 RODO we wskazany poniżej sposób.

Postuluję, by fragment przepisu, o którym tu mowa, miał postać: „Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora **odpowiedniej polityki albo** odpowiednich polityk ochrony danych.

(Czcionką pogrubioną zaznaczam element wstawiony do przepisu.)

6.4. Art. 24 Postulat 4

Poprawienie tłumaczenia polskiego

Artykuł 24 ust. 1 RODO stanowi: *Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze […]*

Artykuł 32 ust. 1 RODO stanowi: U*względniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie* ***wystąpienia*** *i wadze […]*

Wskazane przepisy we wskazanym zakresie niemal się pokrywają. Niemal. Niestety w art. 32 ust. 1 RODO, nie wiedzieć czemu, znalazło się słowo „wystąpienia”. Dla jasności przekazu, pogrubiłem to słowo. Wersja anglojęzyczna przepisów nie zawiera tego słowa czy słowa mu odpowiadającego, również wersji czeskiej nie wzbogacono o dodatkowe słowo. Trudno mówić tu o postulacie *de lege ferenda*. Tym niem-

niej nie ma powodu, by przepisy się różniły. Najprostszym sposobem ujednolicenia wskazanych fragmentów przepisów jest usunięcie słowa wystąpienia z art. 24 ust. 1 RODO w wersji polskojęzycznej.

7. Art. 24 Rozważania historyczne

7.1. Art. 24. Rozważanie 1

Odpowiedniki w dawnej legislacji

Odpowiednikiem art. 24 ust. 1 RODO jest, w pewnym zakresie, art. 6. ust. 2 Dyrektywy 95/46/WE. Zwraca na to – do pewnego stopnia – uwagę Ch. Docksey[174]. Wskazany autor trafnie łączy obowiązek wykazania realizacji RODO z art. 24 ust. 1 RODO z obowiązkiem zapewnienia przestrzegania przepisów ze wspomnianego art. 6 ust. 2 RODO Dyrektywy 95/46/WE. Obowiązek z art. 6 ust. 2 Dyrektywy 95/46/WE jest raczej odpowiednikiem zasady odpowiedzialności administratora z art. 6 ust. 2 RODO niż zasady rozliczalności z tego samego przepisu, ale nawet choćby z uwagi na niekonsekwentne nazewnictwo warto na spostrzeżenia Ch. Dockseya zwrócić uwagę.

[174] Podobnie: Ch. Docksey, op. cit., s. 558.

Rozdział 2
Ocena ryzyka
na gruncie art. 32 RODO

Artykuł 32
Bezpieczeństwo przetwarzania

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieupraw-

nionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.

4. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

Rozważania zamieszczone poniżej dotyczą art. 32 ust 1 i ust. 2 i ust. 3 RODO. Artykuł 32 RODO zawiera cztery ustępy, czwarty dotyczy zjawisk, które w polskiej wersji językowej RODO noszą nazwę upoważnienia i polecenia. Zjawisko upoważnienia i polecenia omówione zostało w książce mojego autorstwa: *Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*[175]. Nie widzę sensu prowadzenia wywodu równoległego lub cytowania zawartych tam tez.

[175] J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja…*, s. 57–106.

1. Art. 32 ust. 1 i 2 i 3 Analiza

1.1. Art. 32 ust. 1 Analiza

Ze słów pogrubionych w art. 32 ust. 1 RODO: ***Uwzględniając*** *[...]* ***administrator i podmiot przetwarzający wdrażają*** *[...]* wynika, że na administratorze i na podmiocie przetwarzającym spoczywa obowiązek dokonania wdrożenia wskazanego w przepisie, przy jednoczesnym uwzględnieniu okoliczności wskazanych w przepisie.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *Uwzględniając* ***stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania*** *[...]* wynika, że *stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania* to okoliczności, które administrator ma obowiązek wziąć pod uwagę przy wykonywaniu oceny ryzyka. Można powiedzieć, że wymienione zjawiska, czyli właśnie *stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania* to parametry, pod kątem poziomu których, administrator ma obowiązek wykonywać ocenę ryzyka.

Ze słów pogrubionych w art. 32 ust. 1 RODO: ***Uwzględniając*** *[...]* ***ryzyko naruszenia praw lub wolności osób fizycznych*** *[...]* wynika, że *ryzyko naruszenia praw lub wolności osób fizycznych* to kolejna okoliczność, którą administrator ma obowiązek wziąć pod uwagę przy wykonywaniu oceny ryzyka. Ryzyko naruszenia praw lub wolności osób fizycznych jest kolejnym parametrem, pod kątem poziomu którego administrator ma obowiązek wykonywać ocenę ryzyka. Prawa i wolności osób fizycznych, jakie należy brać pod uwagę, to przede wszystkim prawa i wolności zapisane jako zasady w art. 5 RODO. Piszę o nich szeroko w innej książce z cyklu, którego niniejsza książka jest częścią, a to w książce *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*[176]. W niniejszej książce problem ten poruszam w uwagach: (*3.2. Art. 24 Uwaga 2. Przykładowe prawa i wolności zasadnicze*), (*3.3. Art. 24 Uwaga 3. Przykładowe prawa i wolności szczegółowe*), (*3.4. Art. 24 Uwaga 4. Inne prawa i wolności*).

Ze słów pogrubionych w art. 32 ust. 1 RODO: *Uwzględniając stan wiedzy technicznej, koszt wdrażania* ***oraz*** *charakter, zakres, kontekst i cele przetwarzania* ***oraz*** *ryzyko naruszenia praw lub wolności*

[176] J. Rzymowski, *RODO – GDPR. Przedmiot i cele...*

osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze […] wynika, że przy dokonywaniu oceny administrator ma za każdym razem brać pod uwagę wszystkie wymienione w przepisie grupy elementów.

– Pierwsza grupa to *stan wiedzy technicznej, koszt wdrażania*.
– Druga grupa to *charakter, zakres, kontekst i cele przetwarzania*.
– Trzecia grupa to *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze*.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[…]* ***naruszenia*** *praw lub wolności osób fizycznych* ***o różnym prawdopodobieństwie wystąpienia i wadze*** *[…]* wynika, że naruszenia praw i wolności mogą mieć różne prawdopodobieństwo wystąpienia i różną wagę. Słowo: „wystąpienia" jest ewidentnie dodatkiem tłumacza. Nie powinno go być w polskiej wersji przepisu. Piszę o tym niżej w uwadze (*3.1. Art. 32 ust. 1. Uwaga 1. Niezgodność wersji językowych*). Pominięcie niepotrzebnego słowa we fragmencie przepisu każe sądzić, że z przepisu wynika, że naruszenia praw i wolności mogą mieć różne prawdopodobieństwo i wagę.

Ze słów pogrubionych w art. 32 ust. 1 RODO: ***Uwzględniając*** *[…]* ***administrator i podmiot przetwarzający wdrażają*** *[…]* wynika, że kiedy administrator i podmiot przetwarzający uwzględnią wskazane w przepisie okoliczności, czyli dokonają stosownej oceny, to mają oni obowiązek dokonać wdrożenia.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[…]* ***wdrażają*** *odpowiednie* ***środki techniczne i organizacyjne*** *[…]* wynika, że wdrożenie, którego mają obowiązek dokonać administrator i podmiot przetwarzający, jest wdrożeniem środków technicznych i organizacyjnych.

Nie ma co ukrywać, że o ile wartości skrajne pojęć: „środki techniczne" i „środki organizacyjne" leżą daleko od siebie, to każde z tych pojęć zawiera znaczenia, które należą również do drugiego z pojęć. Wydaje się, że podobne stanowisko prezentują P. Barta, M. Kawecki i P. Litwiński, którzy odnoszą się[177] do środków technicznych i do środków organizacyjnych jednocześnie, choć jednocześnie cytują stanowisko P. Fajgielskiego, który środki te stara się rozgraniczyć, do tego poziomu, że wskazuje przykłady należące do jednej, bądź do dru-

[177] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 344.

giej grupy[178]. Świadomie nie wdaję się tu w rozważania szczegółowe nad rozróżnieniem środków technicznych od organizacyjnych, uważam bowiem jak powyżej, że środki te często są trudne do rozróżnienia, a na pewno do uczciwego rozróżnienia. Z tego względu stawiam niżej postulat nowelizacyjny (*6.2. Art. 32 ust. 1 i 2 i 3 Postulat 2. Uczytelnienie przepisu*). Trafna jest uwaga D. Nowak, która twierdzi, że *Przepisy RODO nie zawierają […] wymogów co do konkretnych wymaganych środków technicznych i organizacyjnych czy standardów technicznych, które powinny zostać implementowane*[179]. Na tym etapie analizy przepisu wypada dodać, że wskazane przez autorkę środki i standardy powinny być odpowiednie.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]* ***odpowiednie środki techniczne i organizacyjne*** *[...]* wynika, że środki techniczne i organizacyjne, jakie wdroży administrator, mają być odpowiednie. Innymi słowy, administrator i podmiot przetwarzający mają obowiązek wdrożyć środki techniczno-organizacyjne, które są odpowiednie. Odpowiednie do dokonanej oceny, a precyzyjniej – odpowiednie do wyników dokonanej oceny.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]* ***wdrażają*** *odpowiednie środki techniczne i organizacyjne,* ***aby*** *[...]* wynika, że wdrożenie, o którym mowa w przepisie, ma swój cel.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]* ***aby zapewnić stopień bezpieczeństwa*** *[...]* wynika, że celem wdrożenia jest zapewnienie stopnia bezpieczeństwa.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]* ***stopień bezpieczeństwa odpowiadający temu ryzyku*** *[...]* wynika, że stopień bezpieczeństwa, którego zapewnienie jest celem wdrożenia, ma odpowiadać ryzyku, o którym mowa w przepisie, czyli ryzyku ocenianemu, czyli ryzyku *naruszenia praw* i *wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze*. Stopień bezpieczeństwa odpowiadający ryzyku to zatem stopień bezpieczeństwa, jaki administrator uzyskuje po wykonaniu oceny ryzyka. Forma „stopień bezpieczeństwa odpowiadający *[...]* ryzyku" nie jest najszczęśliwsza. W wersji

---

[178] P. Barta, M. Kawecki, P. Litwiński na wskazanej w poprzednim przypisie stronie swojej książki powołują dzieło P. Fajgielskiego następująco: „P. Fajgielski, *Ogólne rozporządzenie o ochronie danych*, s. 373".

[179] D. Nowak, op. cit., s. 36.

anglojęzycznej widnieje: *a level of security appropriate to the risk*, czyli raczej nie „stopień" ale „poziom" i raczej nie „odpowiadający *[...]* ryzyku" ale „odpowiedni do ryzyka". Odpowiedni do ryzyka, czyli do tego ryzyka dostosowany. Dostosowany tak, by wynikiem zastosowania środków technicznych, o których mowa wyżej, administrator uzyskiwał pożądany poziom ryzyka. Pożądany czyli niski (*3.13. Art. 32. Uwaga 13. Niski poziom ryzyka jako pożądany*).

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...] administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku,* ***w tym między innymi*** *w stosownym przypadku:* wynika, że środki techniczne i organizacyjne, jakie mają obowiązek wdrożyć administrator i podmiot przetwarzający to między innymi środki wymienione dalej w przepisie. Z użycia słów „między innymi" wnosimy, że administrator może wdrożyć inne środki niż te wymienione w przepisie, ale te wymienione w przepisie wdrożyć musi. Kolejna część przepisu sytuację obowiązku wdrożenia środków wymienionych w przepisie zmienia jednak dramatycznie.

Przy analizie art. 32 ust. 1 RODO należy wspomnieć o treści art. 30 ust. 1 lit. g RODO i o treści art. 30 ust. 12 lit. d RODO.

Artykuł 30 ust. 1 RODO stanowi o tym, jakie informacje administrator ma obowiązek zamieścić w rejestrze czynności przetwarzania danych osobowych. W rejestrze tym między innymi należy zamieścić *jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1*.

Artykuł 30 ust. 2 RODO stanowi o tym, jakie informacje *Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego* ma obowiązek zamieścić w rejestrze wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora. W rejestrze tym, między innymi, należy zamieścić *jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1*.

Pojawiają się tu dwie grupy zagadnień.

– Pierwsza związana jest z tym, czy stworzenie obydwu (oczywiście odpowiednio) opisów jest obowiązkiem odpowiednich podmiotów.
– Druga grupa zagadnień dotyczy zawartości opisów.

Jeśli chodzi o to, czy stworzenie opisów jest obowiązkiem, to sprawa wygląda ciekawie. Z art. 30 ust. 5 RODO wynika katalog pod-

miotów, które mają obowiązek stworzyć *rejestr czynności przetwarzania danych osobowych*. Podmioty te – o czym piszę wyżej – mają obowiązek zamieścić w rejestrze *czynności przetwarzania danych osobowych ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1*, przy czym mają to uczynić *jeżeli jest to możliwe.* Uważam, że jeżeli zamieszczenie ogólnego opisu *technicznych i organizacyjnych środków bezpieczeństwa* w rejestrze *czynności przetwarzania danych osobowych* jest niemożliwe, to nie znaczy to, że podmiot, w przypadku którego jest to niemożliwe, bo np. *ogólny opis technicznych i organizacyjnych środków bezpieczeństwa* jest zbyt duży, by go w rejestrze zamieścić, że podmiot taki nie ma obowiązku sporządzić ogólnego opisu *technicznych i organizacyjnych środków bezpieczeństwa*. Podmiot sporządza *ogólny opis technicznych i organizacyjnych środków bezpieczeństwa* tyle tylko, że nie zamieszcza go w rejestrze *technicznych i organizacyjnych środków bezpieczeństwa*.

Nieco inaczej rzecz się ma w odniesieniu do podmiotów, które nie mają obowiązku tworzyć rejestru *czynności przetwarzania danych osobowych*. Podmioty takie nie mogą zamieścić opisu *technicznych i organizacyjnych środków bezpieczeństwa* w rejestrze *czynności przetwarzania danych osobowych*, ponieważ nie posiadają rejestru. Nie uważam jednak, że nieposiadanie rejestru zwalnia z posiadania opisu. Podmiot, który nie posiada rejestru i tak powinien posiadać opis, tyle tylko, że nie załączy go do rejestru, bo tegoż nie posiada.

Jeśli chodzi o zawartość – treść ogólnego opisu *technicznych i organizacyjnych środków bezpieczeństwa*, to z art. 32 ust. 1 RODO ani z art. 30 ust. 1 lit g RODO, ani z art. 30 ust. 2 lit d RODO nie wynika, jakie dane administrator ma obowiązek umieścić w opisie, ale… Ale w art. 30 ust. 1 RODO prawodawca wymienia przykładowe środki techniczne i organizacyjne, które administrator może zastosować. Są to środki przykładowe, administrator nie ma obowiązku ich stosować, jednak faktu, że prawodawca środki te w tekście prawnym zawarł, bagatelizować nie sposób. Uważam, że należy je uznać za pewną sugestię prawodawcy.

Środki techniczne i organizacyjne, które są wymienione w art. 32 ust. 1 RODO można zatem uznać za pewien przewodnik, na podstawie którego można tworzyć *rejestr czynności przetwarzania danych osobowych* i oczywiście uprzednio czynności te należy wdrażać. Innymi słowy, art. 32 ust. 1 RODO stanowi krótki przewodnik po

technicznych i organizacyjnych sposobach zabezpieczeń dobrze widzianych przez prawodawcę.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...] w tym między innymi* ***w stosownym przypadku****: [...]* wynika, że administrator ma obowiązek użycia środków wymienionych w przepisie, ale jedynie w sytuacji, która określona została w przepisie słowami „w stosownym przypadku". W wersji anglojęzycznej użyto tu „as appropriate", czyli „odpowiednio". Odpowiednio do ryzyka i do zagrożeń.

Podkreślenia wymaga, że wskazane w przepisie środki mają charakter przykładowy. Przykładowy, ponieważ co prawda prawodawca użył słów „między innymi", co mogłoby sugerować obowiązek stosowania środków wymienionych po „między innymi", ale dalej napotykamy „w stosownym przypadku", co sprawia, że wybór środków zostaje złożony w ręce administratora lub podmiotu przetwarzającego. Podobne, choć zdecydowanie krócej wyrażone, zdanie w opisywanej sprawie prezentuje[180] K. Wygoda.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]*
a) ***pseudonimizację*** *[...]* ***danych osobowych****; [...]* wynika, że pseudonimizacja danych osobowych jest jednym ze środków technicznych i organizacyjnych, jakie administrator może wdrożyć po wykonaniu oceny ryzyka i po ustaleniu, że wdrożenie tego środka pozwala na zapewnienie stopnia bezpieczeństwa, który jest odpowiedni do ryzyka.

Administrator nie ma obowiązku wdrażać pseudonimizacji. Środki wymienione w przepisie są środkami przykładowymi. Miejsce w przepisie, na tle kolejności wskazanych środków, nie ma znaczenia.

Pseudonimizacja zdefiniowana jest w art. 4 pkt 5 RODO. Definicję pseudonimizacji omawiam w odpowiednim miejscu publikacji[181] z cyklu, którego częścią jest niniejsza. Nie ma sensu powtarzać prowadzonych tam rozważań, tu zwracam jedynie uwagę na fakt, że definicja pseudonimizacji nie jest doskonała, nie wiadomo bowiem, jak należy rozumieć osobne przechowywanie informacji, które mogą służyć do odwrócenia pseudonimizacji. Należy również zwrócić uwagę na fakt, że zarówno pseudonimizacja, jak i odwrócenie pseudonimizacji są to czynności na danych osobowych, czyli są one przetwarza-

[180] K. Wygoda, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie…*, s. 355.

[181] J. Rzymowski, *RODO – GDPR. Przedmiot i cele…*, s. 309–317.

niem. O ile pseudonimizacja może być objęta tak czy inaczej rozumianym upoważnieniem (i poleceniem) przetwarzania danych osobowych, o tyle osoba, która odwraca pseudonimizację powinna być do tego wskazana jako osoba uprawniona. Wynika to z motywu 29 Preambuły RODO.

Ze słowa pogrubionego w art. 32 ust. 1 RODO: *[...]*
a) [...] ***i*** *[...]* wynika, że prawodawca użył tu funktora „i", co mogłoby sugerować, że administrator powinien wprowadzać obydwa środki, a nigdy jednego z nich. Jednak w świetle znaczenia słów wprowadzających do tej części przepisu „w stosownym przypadku", rozumowanie takie jest nieuzasadnione. Można oczywiście próbować przedkładać, że racjonalny prawodawca przewidział, że jeżeli zostanie wprowadzony jeden ze środków łączonych przez „i", to koniecznie drugi ze środków też wybrany być musi. Uważam to za nadinterpretację, mimo że uzasadnioną na tle zasad wykładni, jednak nieuzasadnioną, a co najwyżej ratującą niedbale napisany przepis. Ponieważ nie jestem zwolennikiem uzasadniania przypadkowych poglądów prawodawcy, to stwierdzam jak powyżej, dodając że administrator może użyć albo tylko jednego środka, albo tylko drugiego, albo obydwu, albo żadnego z wymienionych.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]*
a) [...] ***szyfrowanie danych osobowych****; [...]* wynika, że szyfrowanie danych osobowych jest jednym ze środków technicznych i organizacyjnych, jakie administrator może wdrożyć po wykonaniu oceny ryzyka i po ustaleniu, że wdrożenie tego środka pozwala na zapewnienie stopnia bezpieczeństwa, który jest odpowiedni do ryzyka.

Administrator nie ma obowiązku wdrażać szyfrowania. Środki wymienione w przepisie są środkami przykładowymi. Miejsce w przepisie na tle kolejności wskazanych środków nie ma znaczenia.

Prawodawca nie wskazuje, jaka metoda szyfrowania powinna być stosowana. Należy tu zwrócić uwagę na fakt, że szyfrowanie nie powinno być mylone z podpisywaniem podpisem elektronicznym. Podpis elektroniczny z kluczem publicznym (znany obecnie między innymi jako kwalifikowany podpis elektroniczny) wykorzystuje techniki kryptograficzne, jednak podpisanie podpisem elektronicznym nie jest szyfrowaniem.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]*

b) ***zdolność do ciągłego zapewnienia*** *[...]* wynika, że kolejna grupa środków technicznych i organizacyjnych, jakie administrator może wdrożyć po wykonaniu oceny ryzyka i po ustaleniu, że wdrożenie tego środka pozwala na zapewnienie stopnia bezpieczeństwa, który jest odpowiedni do ryzyka, składa się ze środków technicznych i organizacyjnych, które zostały wskazane w inny sposób niż środki w art. 32 ust. 1 lit. a RODO i w art. 32 ust. 1 lit. d RODO. Otóż w art. 32 ust. 1 lit. b RODO wymienione są nie konkretne rozwiązania techniczne i organizacyjne, ale cele, wyniki, efekty. jakie administrator powinien osiągnąć przy wykorzystaniu wybranych przez siebie środków.

Podkreślenia wymaga, że o ile administrator nie ma obowiązku wdrażać środków wskazanych w art. 32 ust. 1 lit. a RODO, o tyle jeśli chodzi o środki wskazane w art. 32 ust. 1 lit. b RODO, sytuacja kształtuje się nieco inaczej, ponieważ administrator nie ma ich co prawda obowiązku wdrażać na podstawie art. 32 RODO, jednak na podstawie innych przepisów RODO już tak – piszę o tym niżej.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]*

b) [...] zapewnienia ***poufności, integralności, dostępności i odporności systemów i usług przetwarzania****; [...]* wynika, że wymienione tu zjawiska, są to zjawiska, do których na podstawie omawianego przepisu, administrator powinien dążyć, oczywiście o ile uzna to za stosowne po przeprowadzeniu oceny ryzyka. Należy zwrócić uwagę, że z poszczególnych wskazanych w przepisie celów do osiągnięcia przez administratora, część ma charakter obowiązków administratora, nakładają się one bowiem z analogicznymi obowiązkami z innych przepisów RODO. Rzecz objaśniam szczegółowo poniżej.

– Zdolność do ciągłego zapewnienia poufności. Poufność ma sens, kiedy jest zachowywana w sposób ciągły. Poufność z przerwami, w których dane nie są poufne, sensu nie ma. Zapewnienie poufności jest obowiązkiem administratora, wynika to z zasady poufności zdefiniowanej w art. 5 ust. 1 lit. f RODO. Zasadę poufności omawiam szczegółowo w odpowiednim miejscu publikacji[182] z cyklu, którego częścią jest niniejsza.
– Zdolność do ciągłego zapewnienia **integralności**. Integralność, podobnie jak poufność, ma sens, kiedy jest zachowywana w sposób

[182] J. Rzymowski, *RODO – GDPR. Zasady dotyczące…*, s. 281–288.

ciągły, aczkolwiek tyczy się to danych, którymi administruje administrator, zwłaszcza danych, które przechowuje, zwłaszcza, gdyby przechowywał je w jednym egzemplarzu. Jeżeli dane przestaną być poufne, bo np. zostaną ujawnione osobie nieupoważnionej, to właśnie dane przestają być poufne. Z integralnością rzecz ma się nieco inaczej. Może się zdarzyć, że dane rzeczywiście przestaną być integralne, kiedy na przykład ktoś zniszczy dane przechowywane przez administratora. Może się jednak zdarzyć, że zniszczony zostanie któryś z egzemplarzy danych. W takim wypadku pojawią się jakieś zagrożenie dla integralności, jeżeli jednak administrator posiada integralne egzemplarze danych osobowych (na przykład kopie bezpieczeństwa), to trudno mówić o naruszeniu integralności danych osobowych.

Zasadę integralności omawiam szczegółowo w odpowiednim miejscu publikacji[183] z cyklu, którego częścią jest niniejsza.

– Zdolność do ciągłego zapewnienia **dostępności i odporności systemów i usług przetwarzania**. Jeśli chodzi o wskazane tu dostępność i odporność systemów i usług przetwarzania, to należy zwrócić uwagę na występujące w przepisie funktory „i", co powoduje, że wszystkie występujące w przepisie cechy powinny być brane pod uwagę. Piszę o braniu pod uwagę, bo o tym, czy administrator dane środki wdraża, by dane cele uzyskać, decyduje sam administrator.

Nie można ukrywać, że o ile można się domyślić co oznacza dostępność, o tyle odporność jest raczej w sferze wyczucia niż nawet domysłu.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]*

*c) **zdolność do szybkiego przywrócenia** [...] **w razie incydentu fizycznego lub technicznego** [...]* wynika, że administrator danych osobowych powinien brać pod uwagę możliwość zaistnienia zdarzenia określonego tu jako incydent fizyczny lub techniczny. I następnie, w związku z zaistnieniem takiego incydentu, administrator powinien brać pod uwagę to, by był zdolny do szybkiego przywrócenia funkcjonalności wskazanych w przepisie.

Po raz kolejny nie ma co ukrywać, że tego, czym jest incydent wspomniany w przepisie, należy się jedynie domyślać, podobnie jak

[183] Ibidem, s. 269–279.

domyślać się należy, co stanowi różnicę między incydentem (czymkolwiek on jest) fizycznym a technicznym.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]*
c) zdolność do szybkiego ***przywrócenia dostępności danych osobowych i dostępu do nich w razie*** *incydentu fizycznego lub technicznego [...]* wynika, że administrator powinien brać pod uwagę dbałość o przywrócenie dostępności danych osobowych i dostępu do danych osobowych. Trudno powiedzieć, jaka jest różnica między dostępnością danych a dostępem do danych, zwłaszcza na gruncie polskojęzycznej wersji przepisu. Wersja polskojęzyczna jest zbieżna z wersją anglojęzyczną, w której widnieją słowa: *the ability to restore the availability and access to personal data*. Lektura wersji anglojęzycznej pozwala na postawienie tezy, że dostępność to cecha leżąca po stronie danych, a dostęp to cecha leżąca po stronie administratora.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]*
d) ***regularne*** *[...]* ***środków technicznych i organizacyjnych*** *[...]* wynika, że administrator powinien wziąć pod uwagę podjęcie regularnych działań wobec środków technicznych i organizacyjnych. Działania te wymienione są w przepisie.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]*
d) regularne ***testowanie, mierzenie i ocenianie skuteczności*** *[...]* wynika, że działania o których mowa w przepisie i których podjęcie administrator powinien brać pod uwagę to:
– testowanie skuteczności,
– mierzenie skuteczności,
– ocenianie skuteczności.

W przepisie użyto przecinka i funktora „i". Przecinek jest odpowiednikiem funktora „lub". Użycie „lub" i „i" pozwala na przeprowadzenie rozumowania, wynikiem którego byłoby wskazanie, że czasem trzeba tylko testować, czasem tylko mierzyć i oceniać, a czasem trzeba testować i mierzyć i oceniać. Możliwość rozumowani sygnalizuję, jednak szczegóły pomijam, ponieważ należy pamiętać, że stosowne wdrożenie środków wskazanych w przepisie jest pozostawione do decyzji administratora, więc o obowiązku trudno tu mówić.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]*
d) [...] ***środków technicznych i organizacyjnych mających*** *[...]* wynika, że to, czego skuteczność administrator ma obowiązek badać

w sposób wskazany w przepisie to środki techniczne i organizacyjne. Środki te mają pewną wspólną cechę.

Ze słów pogrubionych w art. 32 ust. 1 RODO: *[...]*
d) [...] ***mających zapewnić bezpieczeństwo przetwarzania***. wynika, że wspólną cechą środków, o których mowa w przepisie, jest zapewnienie bezpieczeństwa przetwarzania danych osobowych.

1.2. Art. 32 ust. 2. Analiza

Przepis wymienia ryzyka, jakie administrator ma obowiązek brać pod uwagę przy dokonywaniu oceny ryzyka technicznego i organizacyjnego, które jest etapem oceny ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.

Uważam, że ocena ryzyka, której obowiązek dokonania wynika z art. 32 ust. 2 RODO, jest etapem oceny ryzyka, której obowiązek dokonania wynika z art. 32 ust. 1 RODO. Uważam tak ze względu na klauzulę odsyłającą, która znajduje się w art. 32 ust. 1 RODO. Widnieją tam słowa: *wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku*. Jednocześnie art. 32 ust. 2 RODO rozpoczyna się od słów: *Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się*.

Nieco skracając wywód… Administrator (danych osobowych) ma wdrożyć środki, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności. Ryzyko naruszenia praw i wolności należy ocenić, ale najpierw należy ocenić stopień bezpieczeństwa i uwzględnić przy tym ryzyka, parametry, okoliczności, które wymienione są w art. 32 ust. 2 RODO.

Ze słów pogrubionych w art. 32 ust. 2 RODO: ***Oceniając*** *[...]* ***uwzględnia się*** *[...]* wynika, że przy dokonywaniu oceny administrator danych osobowych ma obowiązek uwzględnić okoliczności, parametry wymienione w przepisie.

Ze słów pogrubionych w art. 32 ust. 2 RODO: ***Oceniając, czy stopień bezpieczeństwa jest*** *[...]* wynika, że ocena, o której mowa w przepisie to ocena bezpieczeństwa. Ocena bezpieczeństwa, tego samego bezpieczeństwa, o którym mowa jest w art. 32 ust. 1 RODO, w słowach: *by zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku*.

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...]* ***jest odpowiedni*** *[...]* wynika, że celem oceny, o której mowa jest w przepisie, jest ocena odpowiedniości stopnia bezpieczeństwa. Odpowiedni stopień bezpieczeństwa to stopień bezpieczeństwa *odpowiadający [...] ryzyku*, o czym mowa jest w art. 32 ust. 1 RODO.

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...]* ***uwzględnia się ryzyko*** *[...]* wynika, że administrator ma obowiązek uwzględnić ryzyko, o którym mowa w przepisie.

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...]* ***ryzyko wiążące się z przetwarzaniem*** *[...]* wynika, że przepis odnosi się do ryzyka, które związane jest z wykonywaniem czynności na danych osobowych.

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...]* ***uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem*** *[...]* ***wynikające z*** *[...]* wynika, że administrator danych osobowych ma obowiązek brać pod uwagę ryzyko, które wiąże się z przetwarzaniem danych osobowych i wynika z okoliczności wskazanych w przepisie. Administrator może brać pod uwagę również inne ryzyko, ale to wiążące się z przetwarzaniem – musi. Wydaje się, że prawodawca odnosi się tu do ryzyka naruszenia przepisów.

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...]* ***w szczególności wynikające z*** *[...]* wynika, że administrator danych osobowych ma obowiązek uwzględnić ryzyko związane z okolicznościami wymienionymi w przepisie. Należy pamiętać, że administrator może brać również pod uwagę inne okoliczności, ale te wskazane w przepisie – musi.

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...]* ***w szczególności*** *ryzyko wiążące się z przetwarzaniem [...]* ***w szczególności*** *wynikające z [...]* wynika, że ryzyka, o których mowa w przepisie, administrator danych osobowych musi przy dokonywaniu oceny uwzględnić. Inne może, te musi.

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego lub niezgodnego z prawem*** *[...]* wynika, że okoliczności, które administrator ma obowiązek brać pod uwagę przy wykonywaniu oceny ryzyka, muszą być przypadkowe lub niezgodne z prawem.

Z użycia funktora ***lub*** wynika, że okoliczności te muszą być:
– jedynie przypadkowe albo

– jedynie niezgodne z prawem, albo
– przypadkowe i niezgodne z prawem.

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...]* ***wynikające z*** *przypadkowego lub niezgodnego z prawem* ***zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych*** *[...]* wynika, że okoliczności, które administrator ma obowiązek brać pod uwagę przy wykonywaniu oceny ryzyka, muszą wynikać ze zdarzeń wskazanych w przepisie.
Zdarzenia te to:
– zniszczenie danych osobowych,
– utrata danych osobowych,
– modyfikacja danych osobowych,
– nieuprawnione ujawnienie danych osobowych,
– nieuprawniony dostęp do danych osobowych.

Zdarzenia te wymieniam niżej, bardziej szczegółowo w uwagach (*3.3 Art. 32 ust. 1 i 2 i 3 Uwaga 3. Zagrożenia uporządkowane w oparciu o kryterium czynności*) i (*3.2. Art. 32 ust. 1 i 2 i 3 Uwaga 2. Zagrożenia uporządkowane w oparciu o kryterium konkretnego zagrożenia*).

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...]* ***danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych*** wynika, że administrator ma obowiązek brać pod uwagę przy wykonywaniu oceny ryzyka okoliczności dotyczące danych osobowych, które są:
– przesyłane albo
– przechowywane, albo
– przetwarzane w inny sposób niż przesyłanie lub przechowywanie.

Z faktu, że administrator musi brać pod uwagę m.in. okoliczności dotyczące danych osobowych, które są *przetwarzane w inny sposób niż przesyłanie lub przechowywanie* wynika, że administrator ma po prostu brać pod uwagę okoliczności dotyczące danych osobowych, które są przetwarzane.

1.2.1 Art. 32 ust. 2. Analiza szczegółowa

Omówienie przepisu z podziałem na kategorie ryzyk

Poniżej omawiam przepis z podziałem na kategorie ryzyk. Ryzyka omawiam w kolejności wskazanej poniżej.
– Ryzyka związane ze zniszczeniem danych osobowych.

– Ryzyka związane z utratą danych osobowych.
– Ryzyka związane z modyfikacją danych osobowych.
– Ryzyka związane z ujawnieniem danych osobowych.
– Ryzyka związane z dostępem do danych osobowych.

Ryzyka można również oczywiście uporządkować inaczej. Ważne, by administrator miał świadomość, że wzięcie ich pod uwagę przy wykonywaniu oceny ryzyka, jest jego obowiązkiem. Jednocześnie należy pamiętać, że jeżeli czynność oceniana polega, np. na przechowywaniu danych osobowych, to wobec tej czynności nie trzeba oceniać, np. przesyłania danych osobowych. Z drugiej strony, jeżeli administrator posługuje się przy wykonywaniu oceny ryzyka stałymi pomocami, np. w postaci tabel zawierających wszystkie wymienione poniżej zagrożenia, to może z powodzeniem tych tabel nie modyfikować, a używać ich do wykonywania ocen każdej z czynności branych pod uwagę. Poszczególne zagrożenia są równie doniosłe, zapisane są one w tym samym przepisie. Równorzędność zagrożeń podkreślam również sposobem wywodu, w którym staram się jeszcze bardziej niż w innych miejscach książki, zachowywać rygory języka prawnego.

Pod każdym z omawianych poniżej fragmentów przepisu zamieszczam nazwę zdarzenia, które administrator ma obowiązek brać pod uwagę. Nazwy te formułuję w taki sposób, by administrator mógł korzystać z nich łatwo przy wykonywaniu oceny ryzyka.

Należy zwrócić uwagę na pewne zjawisko, ryzyka dotyczą danych, które są przedmiotem pewnej czynności. Różnych czynności. Odnoszę się tu do przesyłania, przechowywania i przetwarzania w inny sposób niż przesyłanie i przechowywanie. Jeżeli administrator nie ocenia czynności, która jest przesyłanie lub której elementem jest przesyłanie, lub która jest elementem przesyłania, to może nie brać pod uwagę danego ryzyka, które właśnie z przesyłaniem jest związane. Podobnie rzecz się ma z przechowywaniem i z przetwarzaniem w inny sposób niż przesyłanie i przechowywanie.

Prezentowane tu poglądy są – jak mniemam – zgodne ze stanowiskiem A. Krasuskiego, u którego czytamy, że: *[...] prawodawca unijny wskazuje, aby ryzyko to oceniać z punktu widzenia skutków powyższych zdarzeń dla osoby fizycznej z punktu widzenia ograniczenia lub pozbawienia tych osób praw lub wolności osób fizycznych, przy*

czym podkreślenia wymaga, że zdarzenia te nie muszą wystąpić w rzeczywistości. Wystarczy, że powstanie ryzyko ich wystąpienia[184].

Zdarzenia, o których pisze tu A. Krasuski, to zdarzenia wskazane w art. 32 ust. 2 RODO. Z myślą A. Krasuskiego się zgadzam, między innymi dlatego ją cytuję, choć przyznam, że słowa o tym, że zdarzenie wystąpić nie musi, że wystarczy ryzyko samo, nieco mnie niepokoją. Są trafne, ale niepokoi mnie, czemu A. Krasuski to podkreśla, być może dlatego, by wskazać, że ryzyko na gruncie art. 32 ust. 2 RODO to ryzyko potencjalne, ale przecież ryzyko zawsze jest potencjalne, kiedy ryzyko się zrealizuje, to mamy do czynienia ze zdarzeniem, nie z ryzykiem.

1.2.1.1 Art. 32 ust. 2 Analiza szczegółowa dalsza

Ryzyka związane ze zniszczeniem danych osobowych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *[...]* ***zniszczenia*** *[...]* ***danych osobowych przesyłanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowe zniszczenie danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *[...]* ***zniszczenia*** *[...]* ***danych osobowych*** *[...]* ***przechowywanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowe zniszczenie danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *[...]* ***zniszczenia*** *[...]* ***danych osobowych*** *[...] przesyłanych, przechowywanych lub* ***w inny sposób przetwarzanych*** wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Wydaje się, że administrator może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Przypadkowe zniszczenie danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z [...]* ***niezgodnego z prawem zniszczenia*** *[...]* ***danych***

[184] A. Krasuski, [w:] A. Krasuski, P. Siembida, op. cit., s. 73.

osobowych przesyłanych *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodne z prawem zniszczenie danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające [...]* ***niezgodnego z prawem zniszczenia*** *[...]* ***danych osobowych*** *[...]* ***przechowywanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodne z prawem zniszczenie danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z [...]* ***niezgodnego z prawem zniszczenia*** *[...]* ***danych osobowych*** *przesyłanych, przechowywanych lub* ***w inny sposób przetwarzanych*** wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. I tu wydaje się, że administrator może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Niezgodne z prawem zniszczenie danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem zniszczenia*** *[...]* ***danych osobowych przesyłanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem zniszczenia*** *[...]* ***danych osobowych*** *[...]* ***przechowywanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem zniszczenia*** *[...]* ***danych osobowych*** *przesyłanych, przechowywanych lub* ***w inny sposób przetwarzanych*** wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Tu również wydaje się, że administrator może rozważyć niebranie pod uwagę wskazanego ry-

zyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie

1.2.1.2 Art. 32 ust. 2 Analiza szczegółowa dalsza

Ryzyka związane z utratą danych osobowych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *[...]* ***utraty*** *[...]* ***danych osobowych przesyłanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowa utrata danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego****[...]* ***utraty*** *[...]* ***danych osobowych*** *[...]* ***przechowywanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowa utrata danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *[...]* ***utraty*** *[...]* ***danych osobowych*** *przesyłanych, przechowywanych lub* ***w inny sposób przetwarzanych***. wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. W tym miejscu również administrator może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Przypadkowa utrata danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z [...]* ***niezgodnego z prawem*** *[...]* ***utraty*** *[...]* ***danych osobowych przesyłanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodna z prawem utrata danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z [...]* ***niezgodnego z prawem*** *[...]* ***utraty*** *[...]* ***danych osobowych*** *[...]* ***przechowywanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodna z prawem utrata danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z [...]* ***niezgodnego z prawem*** *[...]* ***utraty*** *[...]* ***danych osobowych*** *przesyłanych, przechowywanych lub* ***w inny sposób przetwarzanych***. wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Tu też administrator może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Niezgodna z prawem utrata danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem*** *[...]* ***utraty*** *[...]* ***danych osobowych przesyłanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowa i niezgodna z prawem utrata danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem*** *[...]* ***utraty*** *[...]* ***danych osobowych*** *[...]* ***przechowywanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowa i niezgodna z prawem utrata danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem*** *[...]* ***utraty*** *[...]* ***danych osobowych*** *przesyłanych, przechowywanych lub* ***w inny sposób przetwarzanych***. wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Tu również administrator może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Przypadkowa i **niezgodna z prawem utrata danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie**

1.2.1.3 Art. 32 ust. 2 Analiza szczegółowa dalsza

Ryzyka związane z modyfikacją danych osobowych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *[...]* ***modyfikacji*** *[...]* ***danych osobowych***

***przesyłanych** […]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowa modyfikacja danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[…] ryzyko […] wynikające z **przypadkowego** […] **modyfikacji** […] **danych osobowych** […] **przechowywanych** […]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowa modyfikacja danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[…] ryzyko […] wynikające z **przypadkowego** […] **modyfikacji** […] **danych osobowych** przesyłanych, przechowywanych lub **w inny sposób przetwarzanych*** wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. I w tym miejscu administrator może rozważyć nie branie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Przypadkowa modyfikacja danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[…] ryzyko […] wynikające […] **niezgodnego z prawem** […] **modyfikacji**, […] **danych osobowych przesyłanych** […]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodna z prawem modyfikacja danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[…] ryzyko […] wynikające z […] **niezgodnego z prawem** […] **modyfikacji**, […] **danych osobowych** […] **przechowywanych** […]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodna z prawem modyfikacja danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[…] ryzyko […] wynikające z […] **niezgodnego z prawem** […] **modyfikacji** […] **danych osobowych** przesyłanych, przechowywanych lub **w inny sposób przetwarzanych*** wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Również w tym miejscu administrator może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Niezgodna z prawem modyfikacja danych osobowych w inny sposób niż przez przesyłanie lub przechowywanie

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem*** *[...]* ***modyfikacji*** *[...]* ***danych osobowych przesyłanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem*** *[...]* ***modyfikacji*** *[...]* ***danych osobowych*** *[...]* ***przechowywanych*** *lub w inny sposób przetwarzanych.* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem*** *[...]* ***modyfikacji*** *[...]* ***danych osobowych*** *przesyłanych, przechowywanych lub* ***w inny sposób przetwarzanych*** wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Administrator tu też może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Przypadkowa i niezgodna z prawem modyfikacja danych osobowych w inny sposób niż przez przesyłanie lub przechowywanie

1.2.1.4 Art. 32 ust. 2 Analiza szczegółowa dalsza

Ryzyka związane z ujawnieniem danych osobowych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *[...]* ***nieuprawnionego ujawnienia*** *[...]* ***danych osobowych przesyłanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *[...]* ***nieuprawnionego ujawnienia*** *[...]*

***danych osobowych** […] **przechowywanych** […]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[…] ryzyko […] wynikające z **przypadkowego** […] **nieuprawnionego ujawnienia** […] **danych osobowych** przesyłanych, przechowywanych lub **w inny sposób przetwarzanych*** wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Administrator i w tym miejscu może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Przypadkowe i nieuprawnione ujawnienie danych osobowych w inny sposób niż przez przesyłanie lub przechowywanie

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[…] ryzyko […] wynikające z […] **niezgodnego z prawem** […] **nieuprawnionego ujawnienia** […] **danych osobowych przesyłanych** […]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[…] ryzyko […] wynikające z […] **niezgodnego z prawem** […] **nieuprawnionego ujawnienia** […] **danych osobowych** […] **przechowywanych** […]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[…] ryzyko […] wynikające z […] **niezgodnego z prawem** […] **nieuprawnionego ujawnienia** […] **danych osobowych** […] **w inny sposób przetwarzanych**.* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Administrator tu też może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób niż przez przesyłanie lub przechowywanie

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[…] ryzyko […] wynikające z **przypadkowego** lub **niezgodnego z prawem** […] **nieuprawnionego ujawnienia** […] **danych osobowych przesyłanych** […]* wy-

nika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowe i niezgodne z prawem i **nieuprawnione ujawnienie danych osobowych przesyłanych**

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z **przypadkowego** lub **niezgodnego z prawem** [...] **nieuprawnionego ujawnienia** [...] **danych osobowych** [...] **przechowywanych** [...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowe i niezgodne z prawem i **nieuprawnione ujawnienie danych osobowych przechowywanych**

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z **przypadkowego** lub **niezgodnego z prawem** [...] **nieuprawnionego ujawnienia** [...] **danych osobowych** przesyłanych, przechowywanych lub **w inny sposób przetwarzanych***. wynika, administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Wydaje się, że administrator może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób niż przez przesyłanie lub przechowywanie

1.2.1.5 Art. 32 ust. 2 Analiza szczegółowa dalsza

Ryzyka związane z dostępem do danych osobowych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z **przypadkowego** [...] **nieuprawnionego dostępu** do **danych osobowych przesyłanych** [...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowy i nieuprawniony dostęp do danych osobowych przesyłanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z **przypadkowego** [...] **nieuprawnionego dostęp** do **danych osobowych** [...] **przechowywanych** [...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowy i nieuprawniony dostęp do danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *[...]* ***nieuprawnionego dostępu*** *do* ***danych osobowych*** *przesyłanych, przechowywanych lub* ***w inny sposób przetwarzanych*** wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Wydaje się, że administrator może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Przypadkowy i nieuprawniony dostęp do danych osobowych w inny sposób niż przez przesyłanie lub przechowywanie

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z [...]* ***niezgodnego z prawem*** *[...]* ***nieuprawnionego dostępu*** *do* ***danych osobowych przesyłanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z [...]* ***niezgodnego z prawem*** *[...]* ***nieuprawnionego dostępu*** *do* ***danych osobowych*** *[...]* ***przechowywanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z [...]* ***niezgodnego z prawem*** *[...]* ***nieuprawnionego dostępu*** *do* ***danych osobowych*** *przesyłanych, przechowywanych lub* ***w inny sposób przetwarzanych***. wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób niż przez przesyłanie lub przechowywanie

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem*** *[...]* ***nieuprawnionego dostępu*** *do* ***danych osobowych przesyłanych*** *[...]* wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowy i **niezgodny z prawem i nieuprawniony dostęp** do **danych osobowych przesyłanych**

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem*** *[...]* ***nieuprawnionego dostępu*** *do* ***danych osobowych*** *[...]* ***przechowywanych***

[...] wynika, że administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko.

Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych

Ze słów pogrubionych w art. 32 ust. 2 RODO: *[...] ryzyko [...] wynikające z* ***przypadkowego*** *lub* ***niezgodnego z prawem*** *[...]* ***nieuprawnionego dostępu*** *do* ***danych osobowych*** *przesyłanych, przechowywanych lub* ***w inny sposób przetwarzanych***. wynika, administrator ma obowiązek wziąć pod uwagę wskazane w przepisie ryzyko. Wydaje się, że administrator może rozważyć niebranie pod uwagę wskazanego ryzyka, jeżeli oczywiste jest, że ryzyko dotyczy danych osobowych przechowywanych lub przesyłanych.

Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób niż przez przesyłanie lub przechowywanie

1.3. Art. 32 ust. 3 Analiza

Ze słów pogrubionych w art. 32 ust. 3 RODO: ***Wywiązywanie się z obowiązków*** *[...]* wynika, że przepis dotyczy wywiązywania się z obowiązków.

Ze słów pogrubionych w art. 32 ust. 3 RODO: *Wywiązywanie się z* ***obowiązków, o których mowa w ust. 1 niniejszego artykułu*** *[...]* wynika, że obowiązki, o których mowa, to obowiązki nałożone na administratora i na podmiot przetwarzający w art. 32 ust. 1 RODO.

Ze słów pogrubionych w art. 32 ust. 3 RODO: ***Wywiązywanie się*** *[...]* ***można wykazać*** *[...]* wynika, że wywiązywanie się, o którym mowa, może być wykazane w sposób opisany w przepisie.

Ze słów pogrubionych w art. 32 ust. 3 RODO: *Wywiązywanie się [...] można* ***wykazać między innymi poprzez*** *[...]* wynika, że sposób, czy też raczej sposoby wykazania wywiązywania się z obowiązków nie są jedynymi sposobami to umożliwiającymi. Oczywiście pozostaje tu pytanie o to, jakie to inne niż wskazane w przepisie sposoby są możliwe. Odpowiedź na to pytanie jest prosta. Administrator (danych osobowych) i podmiot przetwarzający, którzy chcą wykazać realizację obowiązków, mogą po prostu sporządzić własną dokumentację służącą temu wykazaniu.

Inaczej mówiąc, można na zagadnienie spojrzeć jak poniżej.

– Administrator (podmiot przetwarzający) ustala listę czynności, więc również sporządza odpowiednią dokumentację, czyli zwykle po prostu jeden z rejestrów, o których mowa jest w art. 30 RODO. Są to odpowiednio: rejestr czynności przetwarzania danych osobowych, za które odpowiada administrator lub rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.
– Administrator (podmiot przetwarzający) wykonuje ocenę stopnia bezpieczeństwa i w związku z tym sporządza i zachowuje dokumentację, jakiej użył w związku z dokonywaniem ocen. (Przykłady takiej dokumentacji zamieszczone są na końcu niniejszej książki.)
– Administrator (podmiot przetwarzający) wykonuje ocenę ryzyka naruszenia praw lub wolności osób fizycznych i dokumentuje wykonanie tej oceny w sposób analogiczny, jak dokonuje wykonanie oceny, o której mowa wyżej. (Przykłady takiej dokumentacji również zamieszczone są na końcu niniejszej książki.)
– Administrator (podmiot przetwarzający) dokonuje wdrożenia środków technicznych i organizacyjnych i sporządza odpowiedni dokument (dokumenty) wdrożeniowy, który wskazuje na związek między wynikami oceny ryzyka a środkami technicznymi i organizacyjnymi opisanymi w ogólnym opisie *technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1* RODO. Do omawianego tu zagadnienia wracam poniżej w uwadze (*3.11 Art. 32 ust. 1 i 2 i 3 Uwaga 11 Kolejność czynności*).

Zwracam uwagę na fakt, że w przeciwieństwie do metody opartej na kodeksie lub certyfikacie, metoda wykazania realizacji obowiązków dzięki prowadzonej dokumentacji jest uzależniona tylko od administratora lub podmiotu przetwarzającego[185]. Metoda oparta na certyfikacie lub kodeksie wymaga interakcji z odpowiednim podmiotem i poniesienia kosztów. Metoda oparta na dokumentacji wymaga jedynie kompetentnego pracownika.

Ze słów pogrubionych w art. 32 ust. 3 RODO: *Wywiązywanie się […] można* ***wykazać*** *między innymi* ***poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42***

[185] K. Wygoda, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie…,* s. 356.

wynika, że przykładowe sposoby wykazania wywiązywania się z obowiązków, o których mowa, to:
– zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO lub
– zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO.

Podkreślenia wymaga, że stosowanie wskazanych przez prawodawcę sposobów wykazania realizacji obowiązków nie jest obowiązkowe, na co zwraca uwagę[186] K. Wygoda. Należy jednocześnie pamiętać, że stosowanie któregokolwiek ze wskazanych dwóch sposobów, nie zwalnia administratora ani podmiotu przetwarzającego ze stosowania RODO. Innymi słowy, stosowanie tych sposobów to jedynie dodatkowe koszty dla administratora. Uważam tak, ponieważ administrator, który poniesie koszty certyfikatu lub zgodności z kodeksem i tak będzie musiał ponosić koszty związane z zapewnieniem zgodności z RODO.

2.1. Art. 32 ust. 1 i 2 i 3 Wnioski z analizy

Na administratorze (danych osobowych) i na podmiocie przetwarzającym spoczywa obowiązek dokonania wdrożenia wskazanego w przepisie, przy jednoczesnym uwzględnieniu okoliczności wskazanych w przepisie.

Celem wdrożenia, o którym mowa w przepisie, jest zapewnienie pewnego stopnia bezpieczeństwa.

Z przepisu wynika obowiązek wykonywania oceny ryzyka.

Stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania to okoliczności, które administrator ma obowiązek wziąć pod uwagę przy wykonywaniu oceny ryzyka. Można powiedzieć, że wymienione zjawiska, czyli właśnie *stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania* to parametry, pod kątem poziomu których, administrator ma obowiązek wykonywać ocenę ryzyka.

Ryzyko naruszenia praw lub wolności osób fizycznych to kolejna okoliczność, którą administrator ma obowiązek wziąć pod uwagę przy wykonywaniu oceny ryzyka. Jest kolejnym parametrem, pod ką-

[186] Ibidem, s. 355.

tem poziomu którego administrator danych osobowych ma obowiązek wykonywać ocenę ryzyka. Prawa i wolności osób fizycznych, jakie należy brać pod uwagę, to przede wszystkim prawa i wolności zapisane jako zasady w art. 5 RODO. Piszę o nich szeroko w innej książce z cyklu, którego niniejsza książka jest częścią[187]. W niniejszej książce problem ten poruszam w uwadze (*3.2. Art. 24 Uwaga 2. Przykładowe prawa i wolności zasadnicze*).

Przy dokonywaniu oceny ryzyka administrator danych osobowych ma za każdym razem brać pod uwagę wszystkie wymienione w przepisie grupy elementów.

– Pierwsza grupa to *stan wiedzy technicznej, koszt wdrażania*.
– Druga grupa to *charakter, zakres, kontekst i cele przetwarzania*.
– Trzecia grupa to *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze*.

Naruszenia praw i wolności mogą mieć różne prawdopodobieństwo wystąpienia i różną wagę. Słowo: „wystąpienia" jest ewidentnie dodatkiem tłumacza. Nie powinno go być w polskiej wersji przepisu. Piszę o tym niżej w uwadze (*3.1. Art. 32 ust. 1. Uwaga 1. Niezgodność wersji językowych*). Pominięcie niepotrzebnego słowa we fragmencie przepisu każe sądzić, że z przepisu wynika, że naruszenia praw i wolności mogą mieć różne prawdopodobieństwo i wagę.

Kiedy administrator i podmiot przetwarzający uwzględnią wskazane w przepisie okoliczności, czyli dokonają stosownej oceny, to mają oni obowiązek dokonać wdrożenia, jednak konkretne wymienione w art. 32 RODO środki zabezpieczające nie mają charakteru obowiązków. Innymi słowy – wdrożenie jest obowiązkiem, zastosowanie wymienionych w przepisie środków nie jest obowiązkiem.

Wdrożenie, którego mają obowiązek dokonać administrator i podmiot przetwarzający, jest wdrożeniem środków technicznych i organizacyjnych.

Nie ma tu co ukrywać, że o ile wartości skrajne pojęć: „środki techniczne" i „środki organizacyjne" leżą daleko od siebie, to każde z tych pojęć zawiera znaczenia, które należą również do drugiego z pojęć.

[187] J. Rzymowski, *RODO – GDPR. Przedmiot i cele…*, s. 7–118.

Próbę analizy pojęć „środki techniczne" i „środki organizacyjne" dostrzec można u A. Krasuskiego[188], jednak wskazany autor prowadzi głównie rozważania słownikowe, mam więc poczucie, że miał ten sam problem ze zdefiniowaniem jednych i drugich.

Środki techniczne i organizacyjne, jakie wdroży administrator, mają być odpowiednie. Innymi słowy, administrator i podmiot przetwarzający, mają obowiązek wdrożyć środki techniczno-organizacyjne, które są odpowiednie. Odpowiednie do dokonanej oceny, a precyzyjniej, odpowiednie do wyników dokonanej oceny.

Stopień bezpieczeństwa, którego zapewnienie jest celem wdrożenia, ma odpowiadać ryzyku, o którym mowa w przepisie, czyli ryzyku ocenianemu, czyli ryzyku *naruszenia praw* i *wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze*. Stopień bezpieczeństwa odpowiadający ryzyku, to zatem stopień bezpieczeństwa, jaki administrator uzyskuje po wykonaniu oceny ryzyka. Forma: *stopień bezpieczeństwa odpowiadający [...] ryzyku* nie jest najszczęśliwsza. W wersji anglojęzycznej widnieje: *a level of security appropriate to the risk*, czyli raczej nie stopień ale poziom i raczej nie *odpowiadający [...] ryzyku* ale „odpowiedni do ryzyka". Odpowiedni do ryzyka, czyli do tego ryzyka dostosowany. Dostosowany tak, by wynikiem zastosowania środków technicznych, o których mowa wyżej, administrator uzyskiwał pożądany poziom ryzyka.

Środki techniczne i organizacyjne, jakie mają obowiązek wdrożyć administrator i podmiot przetwarzający, to między innymi środki wymienione dalej w przepisie. Z użycia słów *między innymi* wnosimy, że administrator może wdrożyć inne środki niż te, wymienione w przepisie, ale te wymienione w przepisie wdrożyć musi. Kolejna część przepisu sytuację obowiązku wdrożenia środków wymienionych w przepisie zmienia jednak dramatycznie.

Przy analizie art. 32 ust. 1 RODO należy wspomnieć o treści art. 30 ust. 1 lit g RODO i o treści art. 30 ust. 2 lit d RODO.

Artykuł 30 ust. 1 RODO stanowi o tym, jakie informacje administrator ma obowiązek zamieścić w rejestrze czynności przetwarzania danych osobowych. W rejestrze tym, między innymi, należy zamieścić *jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1*.

---

[188] A. Krasuski, [w:] A. Krasuski, P. Siembida, op. cit., s. 66–68.

Artykuł 30 ust. 2 RODO stanowi o tym, jakie informacje *Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego* ma obowiązek zamieścić w rejestrze wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora. W rejestrze tym, między innymi, należy zamieścić *jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1*.

Pojawiają się tu dwie grupy zagadnień.

– **Pierwsza** grupa zagadnień związana jest z tym, czy stworzenie obydwu (oczywiście odpowiednio) opisów jest obowiązkiem odpowiednich, wskazanych podmiotów.
– **Druga** grupa zagadnień dotyczy zawartości opisów.

Jeśli chodzi o to, czy stworzenie opisów jest obowiązkiem, to sprawa wygląda ciekawie. Z art. 30 ust. 5 RODO wynika katalog podmiotów, które mają obowiązek stworzyć *rejestr czynności przetwarzania danych osobowych*. Podmioty te – o czym piszę wyżej – mają obowiązek zamieścić w rejestrze *czynności przetwarzania danych osobowych ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1*, przy czym mają to uczynić, *jeżeli jest to możliwe.*

Uważam, że jeżeli zamieszczenie ogólnego opisu *technicznych i organizacyjnych środków bezpieczeństwa* w rejestrze *czynności przetwarzania danych osobowych* jest niemożliwe, to nie znaczy to, że podmiot, w przypadku którego jest to niemożliwe, bo np. *ogólny opis technicznych i organizacyjnych środków bezpieczeństwa* jest zbyt duży, by go w rejestrze zamieścić, że podmiot taki nie ma obowiązku sporządzić ogólnego opisu *technicznych i organizacyjnych środków bezpieczeństwa*. Podmiot sporządza *ogólny opis technicznych i organizacyjnych środków bezpieczeństwa* tyle tylko, że nie zamieszcza go w rejestrze *czynności przetwarzania danych osobowych*.

Nieco inaczej rzecz się ma w odniesieniu do podmiotów, które nie mają obowiązku tworzyć rejestru *czynności przetwarzania danych osobowych*. Podmioty takie nie mogą zamieścić opisu *technicznych i organizacyjnych środków bezpieczeństwa* w rejestrze *czynności przetwarzania danych osobowych*, ponieważ nie posiadają tego rejestru. Nie uważam jednak, że nieposiadanie rejestru zwalnia z posiadania opisu. Podmiot, który nie posiada rejestru i tak powinien posiadać opis, tyle tylko, że nie załączy go do rejestru, bo tegoż nie posiada.

Jeśli chodzi o zawartość – treść ogólnego opisu *technicznych i organizacyjnych środków bezpieczeństwa*, to z art. 32 ust. 1 RODO ani z art. 30 ust. 1 lit. g RODO, ani z art. 30 ust. 2 lit. d RODO nie wynika, jakie dane administrator ma obowiązek umieścić w opisie, ale… Ale w art. 32 ust. 1 RODO prawodawca wymienia przykładowe środki techniczne i organizacyjne, które administrator może zastosować. Są to środki przykładowe, administrator nie ma obowiązku ich stosować, jednak faktu, że prawodawca środki te w tekście prawnym zawarł, bagatelizować nie sposób. Uważam, że należy je uznać za pewną sugestię prawodawcy.

Środki techniczne i organizacyjne, wymienione w art. 32 ust. 1 RODO, można zatem uznać za pewien przewodnik, na którym opierając się, można tworzyć *rejestr czynności przetwarzania danych osobowych* i oczywiście uprzednio czynności te wdrażać. Innymi słowy, art. 32 ust. 1 RODO stanowi krótki przewodnik po technicznych i organizacyjnych sposobach zabezpieczeń dobrze widzianych przez prawodawcę.

Administrator (danych osobowych) ma obowiązek użycia środków wymienionych w przepisie, ale jedynie w sytuacji, która określona została w przepisie słowami „w stosownym przypadku". W wersji anglojęzycznej użyto tu *as appropriate* czyli „odpowiednio". Odpowiednio do ryzyka i do zagrożeń.

Pseudonimizacja danych osobowych jest jednym ze środków technicznych i organizacyjnych, jakie administrator może wdrożyć po wykonaniu oceny ryzyka i po ustaleniu, że wdrożenie tego środka pozwala na zapewnienie stopnia bezpieczeństwa, który jest odpowiedni do ryzyka.

Administrator nie ma obowiązku wdrażać pseudonimizacji. Środki wymienione w przepisie są środkami przykładowymi. Miejsce w przepisie na tle kolejności wskazanych środków nie ma znaczenia.

Pseudonimizacja zdefiniowana jest w art. 4 pkt 5 RODO. Definicję pseudonimizacji omawiam w innej książce[189] z cyklu, którego częścią jest niniejsza. Nie ma sensu powtarzać prowadzonych tam rozważań[190], tu zwracam jedynie uwagę na fakt, że definicja pseudo-

[189] J. Rzymowski, *RODO – GDPR. Przedmiot i cele…* s. 319–329.

[190] Szerzej również: M. Kołodziej, *Pseudonimizacja w RODO – kiedy i jak stosować*. ABI Expert 2(7) 2018, s. 44–47.

nimizacji nie jest doskonała, nie wiadomo bowiem, jak należy rozumieć osobne przechowywanie informacji, które mogą służyć do odwrócenia pseudonimizacji.

Należy również zwrócić uwagę na fakt, że zarówno pseudonimizacja, jak i odwrócenie pseudonimizacji są to czynności na danych osobowych, czyli są one przetwarzaniem. O ile pseudonimizacja może być objęta – tak czy inaczej rozumianym – upoważnieniem (i poleceniem) przetwarzania danych osobowych, o tyle osoba, która odwraca pseudonimizację, powinna być do tego wskazana jako osoba uprawniona. Wynika to z motywu 29 Preambuły RODO.

Prawodawca użył w zwrocie *pseudonimizację i szyfrowanie danych osobowych* funktora „i", co mogłoby sugerować, że administrator powinien wprowadzać obydwa rodzaje środków, a nigdy jeden z nich. Jednak w świetle znaczenia słów wprowadzających do tej części przepisu „w stosownym przypadku", rozumowanie takie jest nieuzasadnione. Można oczywiście próbować przedkładać, że racjonalny prawodawca przewidział, że jeżeli zostanie wprowadzony jeden ze środków łączonych przez „i", to koniecznie drugi ze środków też wybrany być musi. Uważam to za nadinterpretację, mimo że uzasadnioną na tle zasad wykładni, jednak nieuzasadnioną, a co najwyżej ratującą niedbale napisany przepis. Nie będąc zwolennikiem uzasadniania przypadkowych poglądów prawodawcy, stwierdzam jak powyżej, dodając że administrator może użyć albo tylko jednego środka, albo tylko drugiego, albo obydwu, albo żadnego z wymienionych.

Szyfrowanie danych osobowych jest jednym ze środków technicznych i organizacyjnych, jakie administrator może wdrożyć po wykonaniu oceny ryzyka i po ustaleniu, że wdrożenie tego środka pozwala na zapewnienie stopnia bezpieczeństwa, który jest odpowiedni do ryzyka.

Administrator nie ma obowiązku wdrażać szyfrowania. Środki wymienione w przepisie są środkami przykładowymi. Miejsce w przepisie na tle kolejności wskazanych środków nie ma znaczenia.

Prawodawca nie wskazuje, jaka metoda szyfrowania powinna być stosowana. Należy tu zwrócić uwagę na fakt, że szyfrowanie nie powinno być mylone z podpisywaniem podpisem elektronicznym. Podpis elektroniczny z kluczem publicznym (znany obecnie jako kwalifikowany podpis elektroniczny i jako zaawansowany podpis elektro-

niczny) wykorzystuje techniki kryptograficzne, jednak podpisanie podpisem elektronicznym nie jest szyfrowaniem.

Kolejna grupa środków technicznych i organizacyjnych, jakie administrator może wdrożyć po wykonaniu oceny ryzyka i po ustaleniu, że wdrożenie tego środka pozwala na zapewnienie stopnia bezpieczeństwa, który jest odpowiedni do ryzyka, składa się ze środków technicznych i organizacyjnych, które zostały wskazane w inny sposób niż środki w art. 32 ust. 1 lit. a RODO i w art. 32 ust. 1 lit. d RODO. Otóż w art. 32 ust. 1 lit. b RODO wymienione są nie konkretne rozwiązania techniczne i organizacyjne, ale cele, wyniki, efekty, jakie administrator powinien osiągnąć przy wykorzystaniu wybranych przez siebie środków.

Podkreślenia wymaga, że o ile administrator nie ma obowiązku wdrażać środków wskazanych w art. 32 ust. 1 lit. a RODO, o tyle jeśli chodzi o środki wskazane w art. 32 ust. 1 lit. b RODO, sytuacja kształtuje się nieco inaczej, ponieważ administrator nie ma ich co prawda obowiązku wdrażać na podstawie art. 32 RODO, jednak na podstawie innych przepisów RODO już tak – piszę o tym niżej.

Wymienione tu zjawiska, są to zjawiska o charakterze stanów, do których na podstawie omawianego przepisu, administrator powinien dążyć, oczywiście, o ile uzna to za stosowne po przeprowadzeniu oceny ryzyka. Należy zwrócić uwagę, że z poszczególnych, wskazanych w przepisie celów do osiągnięcia przez administratora, część ma charakter obowiązków administratora, nakładają się one bowiem z analogicznymi obowiązkami z innych przepisów RODO. Rzecz objaśniam detalicznie poniżej.

– Zdolność do ciągłego zapewnienia **poufności**. Poufność ma sens, kiedy jest zachowywana w sposób ciągły. Poufność z przerwami, w których dane nie są poufne, sensu nie ma. Zapewnienie poufności jest obowiązkiem administratora, wynika to z zasady poufności, zdefiniowanej w art. 5 ust. 1 lit. f RODO. Zasadę poufności omawiam szczegółowo w odpowiednim miejscu publikacji[191] z cyklu, którego częścią jest niniejsza.
– Zdolność do ciągłego zapewnienia **integralności**. Integralność, podobnie jak poufność, ma sens, kiedy jest zachowywana w sposób ciągły, aczkolwiek tyczy się to danych, którymi administruje ad-

[191] J. Rzymowski, *RODO – GDPR. Zasady dotyczące…*, s. 281–289.

ministrator, zwłaszcza danych, które przechowuje, zwłaszcza, gdyby przechowywał je w jednym egzemplarzu. Jeżeli dane przestaną być poufne, bo np. zostaną ujawnione osobie nieupoważnionej, to właśnie dane przestają być poufne, jednak jedynie właśnie poufne być przestają i naruszenie poufności nie oznacza wcale automatycznie naruszenia integralności.

Z integralnością rzecz ma się nieco inaczej niż z poufnością. Może się zdarzyć, że dane rzeczywiście przestaną być integralne, kiedy na przykład ktoś zniszczy dane przechowywane przez administratora. Może się jednak zdarzyć, że zniszczony zostanie któryś z egzemplarzy danych. W takim przypadku pojawią się jakieś zagrożenie dla integralności, jeżeli jednak administrator posiada integralne egzemplarze danych osobowych (na przykład kopie bezpieczeństwa), to trudno mówić o naruszeniu integralności danych. Naruszenie integralności jednej kopii czy też jednego kompletu, egzemplarza danych osobowych w sytuacji, w której administrator posiada inną kopię tych danych i to o nienaruszonej integralności, nie oznacza naruszenia integralności danych jako takich, a jedynie co najwyżej naruszenie integralności jednej z kopii danych osobowych.

Zasadę integralności omawiam szczegółowo w odpowiednim miejscu innej książki[192] z cyklu, którego częścią jest niniejsza.

– Zdolność do ciągłego zapewnienia **dostępności i odporności systemów i usług przetwarzania**. Jeśli chodzi o wskazane tu dostępność i odporność systemów i usług przetwarzania, to należy zwrócić uwagę na występujące w przepisie funktory „i", co powoduje, że wszystkie występujące w przepisie cechy powinny być brane pod uwagę. Piszę o braniu pod uwagę, bo o tym, czy administrator dane środki wdraża, by dane cele uzyskać, decyduje sam administrator.

Nie można ukrywać, że o ile można się domyślić, co oznacza dostępność, o tyle odporność jest raczej w sferze wyczucia niż nawet domysłu.

Administrator powinien brać pod uwagę możliwość zaistnienia zdarzenia określonego tu jako incydent fizyczny lub techniczny. I następnie, w związku z zaistnieniem takiego incydentu, administrator

[192] Ibidem, s. 269–280.

powinien brać pod uwagę to, by był zdolny do szybkiego przywrócenia funkcjonalności wskazanych w przepisie.

Po raz kolejny nie ma co ukrywać, że tego, czym jest incydent wspomniany w przepisie, należy się jedynie domyślać, podobnie jak domyślać się należy, co stanowi różnicę między incydentem (czymkolwiek on jest) fizycznym a incydentem technicznym.

Administrator powinien brać pod uwagę dbałość o przywrócenie dostępności danych osobowych i dostępu do danych osobowych. Trudno powiedzieć, jaka jest różnica między dostępnością danych a dostępem do danych, zwłaszcza na gruncie polskojęzycznej wersji przepisu. Wersja polskojęzyczna jest zbieżna z wersją anglojęzyczną, w której widnieją słowa: *the ability to restore the availability and access to personal data*. Lektura wersji anglojęzycznej pozwala na postawienie tezy, że dostępność to cecha leżąca po stronie danych, a dostęp to cecha leżąca po stronie administratora.

Administrator powinien wziąć pod uwagę podjęcie regularnych działań wobec środków technicznych i organizacyjnych. Działania te wymienione są w przepisie.

Działania, o których mowa w przepisie i których podjęcie administrator powinien brać pod uwagę, to:
– testowanie skuteczności,
– mierzenie skuteczności,
– ocenianie skuteczności.

W przepisie użyto przecinka i funktora „i". Przecinek jest odpowiednikiem funktora „lub". Użycie „lub" i „i" pozwala na przeprowadzenie rozumowania, wynikiem którego byłoby wskazanie, że czasem trzeba tylko testować, czasem tylko mierzyć i oceniać, a czasem trzeba testować i mierzyć, i oceniać. Możliwość rozumowania sygnalizuję, jednak szczegóły pomijam, ponieważ należy pamiętać, że stosowanie, wdrożenie środków wskazanych w przepisie jest pozostawione do decyzji administratora, więc o obowiązku trudno tu mówić.

To, czego skuteczność administrator ma obowiązek badać w sposób wskazany w przepisie, to środki techniczne i organizacyjne. Środki te mają pewną wspólną cechę.

Wspólną cecha środków, o których mowa w przepisie, jest zapewnienie bezpieczeństwa przetwarzania danych osobowych.

2.2. Art. 32 ust. 2 Wnioski z analizy

Przepis ten wskazuje ryzyka, jakie administrator ma obowiązek brać pod uwagę przy dokonywaniu oceny ryzyka technicznego i organizacyjnego, które jest etapem oceny ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.

Uważam, że ocena ryzyka, której obowiązek dokonania wynika z art., 32 ust. 2 RODO, jest etapem oceny ryzyka, której obowiązek dokonania wynika z art. 32 ust. 1 RODO. Uważam tak, ze względu na klauzulę odsyłającą, która znajduje się w art. 32 ust. 1 RODO. Widnieją tam słowa *wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku*. Jednocześnie art. 32 ust. 2 rozpoczyna się od słów *Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się*.

Nieco skracając wywód… Administrator ma wdrożyć środki, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności. Ryzyko naruszenia praw i wolności należy ocenić, ale najpierw należy ocenić stopień bezpieczeństwa i uwzględnić przy tym ryzyka, parametry, okoliczności, które wymienione są w art. 32 ust. 2 RODO.

Przy dokonywaniu oceny administrator ma obowiązek uwzględnić okoliczności, parametry wymienione w przepisie.

Ocena, o której mowa w przepisie, to ocena bezpieczeństwa. Ocena bezpieczeństwa, tego samego bezpieczeństwa, o którym mowa jest w art. 32 ust. 1 RODO, w słowach: *by zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku*.

Celem oceny, o której mowa jest w przepisie, jest ocena odpowiedniości stopnia bezpieczeństwa. Odpowiedni stopień bezpieczeństwa to stopień bezpieczeństwa *odpowiadający […] ryzyku*, o czym mowa jest w art. 32 ust. 1 RODO.

Administrator ma obowiązek uwzględnić ryzyko, o którym mowa w przepisie.

Przepis odnosi się do ryzyka, które związane jest z wykonywaniem czynności na danych osobowych.

Administrator ma obowiązek brać pod uwagę ryzyko, które wiąże się z przetwarzaniem danych osobowych i wynika z okoliczności wskazanych w przepisie. Administrator może brać pod uwagę również

inne ryzyko, ale to wiążące się z przetwarzaniem – musi. Wydaje się, że prawodawca odnosi się tu do ryzyka naruszenia przepisów.

Administrator ma obowiązek uwzględnić ryzyko związane z okolicznościami wymienionymi w przepisie. Należy pamiętać, że administrator może brać również pod uwagę inne okoliczności, ale te wskazane w przepisie – musi.

Ryzyka, o których mowa w przepisie, administrator musi przy dokonywaniu oceny uwzględnić. Inne może, te musi.
Ryzyka te wymieniam poniżej w uwagach (*3.2. Art. 32 ust. 1 i 2 i 3 Uwaga 2. Zagrożenia uporządkowane w oparciu o kryterium konkretnego zagrożenia*) i (*3.3 Art. 32 ust. 1 i 2 i 3 Uwaga 3. Zagrożenia uporządkowane w oparciu o kryterium czynności*) oraz na końcu książki w części: *Tabele pomocnicze, zestawienia*.

Na szczegóły dotyczące ryzyka zawarte w art. 32 ust. 2 RODO trafnie zwraca uwagę A. Krasuski. Zrazu czytamy, że: *W art. 32 ust. 2 RODO prawodawca unijny odniósł się do przedmiotu ryzyka naruszenia praw lub wolności osób fizycznych, wskazując, że do oceny, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem danych osobowych*[193]. Słowa A. Krasuskiego są tu powtórzeniem fragmentu przepisu, w którym czytamy, że: *Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem*. Nie jest to w najmniejszym stopniu zarzut, tym bardziej że sam często stosuję metodę umieszczania w tekście prawniczym fragmentów tekstu prawnego.

Dalej A. Krasuski stosuje tę samą metodę, czytamy bowiem u niego, że: *W szczególności należy uwzględnić ryzyko, które wynika z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych*[194]. Te słowa są z kolei powtórzeniem fragmentu przepisu, w którym czytamy, że: *w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób prze-*

[193] A. Krasuski, [w:] A. Krasuski, P. Siembida, op. cit., s. 73.

[194] Ibidem.

twarzanych. I tu również cenne jest, że wskazany autor zwrócił uwagę na doniosłość słów przepisu. Dalej, jako kolejne dwa zdania czytamy, że: *Innymi słowy, prawodawca unijny wskazuje, aby ryzyko to oceniać z punktu widzenia skutków powyższych zdarzeń dla osoby fizycznej z punktu widzenia ograniczenia lub pozbawienia tych osób praw lub wolności osób fizycznych, przy czym podkreślenia wymaga, że zdarzenia te nie muszą wystąpić w rzeczywistości. Wystarczy, że powstanie ryzyko ich wystąpienia*[195]. Wskazuję na słowa A. Krasuskiego, aby podkreślić ich wartość i wagę, które płyną z tego, że wskazują doniosłość zapisanych w przepisie zjawisk, których zaistnienie oraz sama nawet możliwość wystąpienia (na co słowami o ryzyku zwraca uwagę A. Krasuski) administrator powinien brać pod uwagę.

2.3. Art. 32 ust. 3 Wnioski z analizy

Przepis dotyczy wywiązywania się z obowiązków nałożonych na administratora i na podmiot przetwarzający w art. 32 ust. 1 RODO.

Wywiązywanie, o którym mowa, może być wykazane w sposób opisany w przepisie. Przykładowe sposoby wykazania wywiązywania się z obowiązków, o których mowa, to:

– zatwierdzony kodeks postępowania, o którym mowa w art. 40 RODO lub
– zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 RODO.

Stosowanie sposobów wykazania realizacji obowiązków ze wskazanych przez prawodawcę nie jest obowiązkowe i nie zwalnia ze stosowania RODO, wydaje się więc być ozdobnikiem i niczym więcej.

Sposoby wykazania wywiązywania się z obowiązków nie są jedynymi sposobami to umożliwiającymi. Administrator i podmiot przetwarzający, którzy chcą wykazać realizację obowiązków, mogą po prostu sporządzić własną dokumentację służącą temu wykazaniu.

[195] Ibidem.

3. Art. 32 ust. 1 i 2 i 3 Uwagi

3.1. Art. 32 ust. 1 i 2 i 3 Uwaga 1

Niezgodność wersji językowych

Wywód prowadzony jest pod tabelą umieszczoną na następnej stronie, tabela zawiera zestawione różne wersje językowe tego samego fragmentu art. 32 ust. 1 RODO.

Art. 32 ust. 1. Fragment.		
Język angielski	Język polski	Język czeski.
the risk	ryzyko naruszenia praw lub wolności osób fizycznych	
of varying likelihood	o różnym prawdopodobieństwie	různě pravděpodobným
	wystąpienia	
and severity	i wadze	a různě závažným
		rizikům
for the rights and freedoms of natural persons,		pro práva a svobody fyzických osob

Umieszczona powyżej tabela zawiera fragment art. 32 ust. 1 RODO w trzech językach. Na tyle, na ile to jest możliwe, słowa umieszczone w tych samych wersach mają to samo znaczenie. Niestety wersja polskojęzyczna, przy bliższej lekturze, ma nieco inne znaczenie niż wersja anglojęzyczna. Wersję czeskojęzyczną wskazuję jako pewien punkt odniesienia, jest ona bowiem zbieżna z wersją angielskojęzyczną.

Dokładne tłumaczenie wersji angielskojęzycznej na język polski powinno brzmieć (używam, na ile to możliwe słów z wersji oficjalnej): „ryzyko o różnym prawdopodobieństwie i wadze dla praw i wolności osób fizycznych". Wersja czeska przetłumaczona na polski brzmi: „różnie prawdopodobnym i o różnej wadze ryzykom dla praw i wolności osób fizycznych".

Jak zatem widać, wskazany fragment przepisu dotyczy ryzyka dla praw i wolności osób fizycznych. Ryzyko dla praw i wolności

osób fizycznych może mieć różne prawdopodobieństwo (o*f varying likelihood, různě pravděpodobným*) i różną wagę (*and severity*, *a různě závažným*). Patrząc jeszcze prościej: ryzyko ma różne prawdopodobieństwo i wagę. Jest to proste i dość zrozumiałe. Niestety tylko do momentu przejścia do wersji polskojęzycznej. Gdyby wersja polskojęzyczna miała znaczyć to samo co pozostałe dwie, to brzmiałaby „ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze". Jak widać, usunąłem z oficjalnej wersji słowo: „wystąpienia". Z tak przekształconej wersji wynika to samo, co z wersji anglojęzycznej i czeskojęzycznej. Jest ryzyko. Ryzyko ma różne prawdopodobieństwo i wagę. Niestety, wersja oficjalna zawiera zaskakujące dodatki. Brzmi ona *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze*. W tej wersji prawdopodobieństwo jest cechą wystąpienia. Prawdopodobieństwo, które w wersji czeskiej i angielskiej jest cechą ryzyka, w wersji polskiej jest cechą wystąpienia. (wcześniej jeszcze, przed oficjalną poprawką tekstu, waga była cechą zagrożenia).

Oczywiste jest tu postawienie postulatu *de lege ferenda*, czynię to niżej (*6.1. Art. 32 ust. 1 i 2 i 3 Postulat 1. Uproszczenie przepisu*).

3.2. Art. 32 ust. 1 i 2 i 3 Uwaga 2

Zagrożenia uporządkowane

oparte na kryterium konkretnego zagrożenia

Wyżej, w Analizie prowadzę rozważania dotyczące między innymi wykonywania ocen ryzyka naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Częścią tej oceny jest ocena ryzyka przetwarzania, której dotyczy zwłaszcza art. 32 ust. 2 RODO. W Analizie ustalam, jakie ryzyka należy brać pod uwagę przy tej ocenie. W niniejszej uwadze prezentuję je w kolejności takiej samej, jak kolejność prowadzenia rozważań powyżej.
Patrząc przez pryzmat treści, ryzyka są wymienione grupami w sposób wskazany poniżej.
– Ryzyka związane ze zniszczeniem danych osobowych.
– Ryzyka związane z utratą danych osobowych.
– Ryzyka związane z modyfikacją danych osobowych.
– Ryzyka związane z ujawnieniem danych osobowych.
– Ryzyka związane z dostępem do danych osobowych.

Możliwe jest uporządkowanie ryzyk zgodnie z innym kryterium porządkującym, a to w kolejności opartej na czynności na danych osobowych, wobec której dane ryzyko jest oceniane. Czynię to w uwadze (*3.3 Art. 32 ust. 1 i 2 i 3 Uwaga 3. Zagrożenia uporządkowane oparte na kryterium czynności*).

Ryzyka związane ze zniszczeniem danych osobowych.
– Przypadkowe zniszczenie danych osobowych przesyłanych.
– Przypadkowe zniszczenie danych osobowych przechowywanych.
– Przypadkowe zniszczenie danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.
– Niezgodne z prawem zniszczenie danych osobowych przesyłanych.
– Niezgodne z prawem zniszczenie danych osobowych przechowywanych.
– Niezgodne z prawem zniszczenie danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.

Ryzyka związane z utratą danych osobowych.
– Przypadkowa utrata danych osobowych przesyłanych.
– Przypadkowa utrata danych osobowych przechowywanych.
– Przypadkowa utrata danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.
– Niezgodna z prawem utrata danych osobowych przesyłanych.
– Niezgodna z prawem utrata danych osobowych przechowywanych.
– Niezgodna z prawem utrata danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.
– Przypadkowa i niezgodna z prawem utrata danych osobowych przesyłanych.
– Przypadkowa i niezgodna z prawem utrata danych osobowych przechowywanych.
– Przypadkowa i niezgodna z prawem utrata danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.

Ryzyka związane z modyfikacją danych osobowych

– Przypadkowa modyfikacja danych osobowych przesyłanych.
– Przypadkowa modyfikacja danych osobowych przechowywanych.
– Przypadkowa modyfikacja danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.
– Niezgodna z prawem modyfikacja danych osobowych przesyłanych.
– Niezgodna z prawem modyfikacja danych osobowych przechowywanych.
– Niezgodna z prawem modyfikacja danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przesyłanych.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przechowywanych.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.

Ryzyka związane z ujawnieniem danych osobowych

– Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.

– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.

Ryzyka związane z dostępem do danych osobowych

– Przypadkowy i nieuprawniony dostępu do danych osobowych przesyłanych.
– Przypadkowy i nieuprawniony dostęp do danych osobowych przechowywanych.
– Przypadkowy i nieuprawniony dostęp do danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przetwarzanych w inny sposób niż przesyłaniem lub przechowywaniem.

Niżej porządkuję zagrożenia oparte na kluczu czynności, podczas której mogą zaistnieć. Wydaje się, że uporządkowanie w ten właśnie sposób jest prostsze do wykorzystania, choć jest to też zapewne kwestią przyzwyczajenia osoby dokonującej ocen.

3.3 Art. 32 ust. 1 i 2 i 3 Uwaga 3 Zagrożenia uporządkowane oparte na kryterium czynności

Wyżej w uwadze (*3.2. Art. 32 ust. 1 i 2 i 3 Uwaga 2. Zagrożenia uporządkowane oparte na kryterium konkretnego zagrożenia*) wymieniam zagrożenia w sposób uporządkowany, opierając się na kryterium

konkretnego zagrożenia, czyli w sposób uzależniony od tego, co konkretnie stanowi zagrożenie. W niniejszej uwadze prezentuję te same zagrożenie uporządkowane w sposób uzależniony od tego, jakiej konkretnie czynności tyczy dane zagrożenie. Ten sposób uporządkowania jest – przynajmniej dla mnie – prostszy do stosowania w praktyce.

Ryzyka dotyczące danych osobowych przesyłanych

– Przypadkowe zniszczenie danych osobowych przesyłanych.
– Niezgodne z prawem zniszczenie danych osobowych przesyłanych.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych.
– Przypadkowa utrata danych osobowych przesyłanych.
– Niezgodna z prawem utrata danych osobowych przesyłanych.
– Przypadkowa i niezgodna z prawem utrata danych osobowych przesyłanych.
– Przypadkowa modyfikacja danych osobowych przesyłanych.
– Niezgodna z prawem modyfikacja danych osobowych przesyłanych.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przesyłanych.
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Przypadkowy i nieuprawniony dostępu do danych osobowych przesyłanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.

Ryzyka dotyczące danych osobowych przechowywanych

– Przypadkowe zniszczenie danych osobowych przechowywanych.
– Niezgodne z prawem zniszczenie danych osobowych przechowywanych.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych.
– Przypadkowa utrata danych osobowych przechowywanych.

– Niezgodna z prawem utrata danych osobowych przechowywanych.
– Przypadkowa i niezgodna z prawem utrata danych osobowych przechowywanych.
– Przypadkowa modyfikacja danych osobowych przechowywanych.
– Niezgodna z prawem modyfikacja danych osobowych przechowywanych.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przechowywanych.
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Przypadkowy i nieuprawniony dostęp do danych osobowych przechowywanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.

Ryzyka dotyczące danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie

– Przypadkowe zniszczenie danych osobowych w inny sposób przetwarzanych.
– Niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych.
– Przypadkowa utrata danych osobowych w inny sposób przetwarzanych.
– Niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych.
– Przypadkowa i niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych.
– Przypadkowa modyfikacja danych osobowych w inny sposób przetwarzanych.

– Niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych.
– Przypadkowe i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.
– Przypadkowy i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.

Jak widać powyżej, zwłaszcza, kiedy ryzyka są tak uporządkowane jak w niniejszej uwadze, ryzyka się powtarzają.

Podkreślam, że dane osobowe *w inny sposób przetwarzane*, to dane osobowe przetwarzane w sposób inny niż przez przesyłanie i przechowywanie.

Podkreślić należy, że wskazane tu „ryzyka" nie mają charakteru przykładowego, w przeciwieństwie do tego co piszą[196] P. Barta, M. Kawecki, P. Litwiński. Są to elementy nie „przykładowe", ale „obowiązkowe". Administrator i podmiot przetwarzający mają obowiązek ująć je w przeprowadzanych ocenach ryzyka. Prawodawca nie umieścił tych elementów w przepisie w celach rozrywkowych ani zdobniczych. Ich ujęcie jest obowiązkiem. Przepis ma charakter konkluzywny.

3.3 Art. 32 ust. 1 i 2 i 3 Uwaga 3

Składowe oceny ryzyka

Przy wykonywaniu oceny ryzyka należy pamiętać, że ocena ryzyka wykonywana na podstawie art. 32 RODO to ocena ryzyka *naru-*

[196] P. Barta, M. Kawecki, P. Litwiński op. cit., s. 344 i 345.

szenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.

Prawodawca nie wskazuje, jak dokładnie powinno wyglądać ocenianie ryzyka. Prawodawca nie wskazuje dokładnie, ale daje jednak pewne wskazówki, które dotyczą tego, co należy w ocenie ująć. Co więcej, wskazówki te mają charakter obowiązków. Piszę o tym wyżej w Analizie. Tu zwracam uwagę na kilka podstawowych faktów.

– Administrator ma obowiązek dokonać oceny ryzyka *naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze*. (art. 32 ust. 1 RODO).
– Administrator ma obowiązek dokonać oceny, czy stopień bezpieczeństwa jest odpowiedni (Art. 32 ust. 2 RODO).
– Przy dokonywaniu oceny ryzyka *naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze* administrator ma obowiązek uwzględnić przy dokonywaniu tej oceny prawa i wolności, które widnieją w art. 5 RODO jako zasady. Administrator ma obowiązek uwzględnić te prawa i wolności, ponieważ wynika to z dyrektywy języka prawnego[197].
– Przy dokonywaniu oceny, czy stopień bezpieczeństwa jest odpowiedni, administrator ma obowiązek uwzględnić ryzyka zapisane w art. 32 ust. 2 RODO, ponieważ wynika to z zakazu wykładni *per non est*[198]. Suche słowa o zakazie wykładni *per non est* aż proszą się o rozwinięcie. Zakaz ten w ujęciu L. Morawskiego brzmi: *Nie wolno jest interpretować przepisów prawnych tak, by pewne ich fragmenty okazały się zbędne*[199]. Zakaz ten jest prosty do zrozumienia. Prawodawca działa celowo. Prawodawca nadaje przepisom pewną treść po to, by interpretatorzy treść tę odczytywali, nie po to, by zastępowali ją własnymi imaginacjami. Imaginacjami czy czymkolwiek innym – parametrami zaczerpniętymi z norm, wiedzą pochodzącą ze specjalistycznych studiów czy innych fachowych źródeł. Podkreślam, że nie podważam wartości wskazanych źródeł, jednak oceny ryzyka wykonywane na ich podstawie mogą uzupełniać oceny wykonywane na podstawie RODO, natomiast oceny wyko-

[197] L. Morawski, op. cit., s. 93–95.

[198] Ibidem, s. 106.

[199] Ibidem.

nywane na podstawie tych źródeł nie mogą zastąpić oceny wykonywanej na podstawie RODO.

Ciekawą myśl, która koresponduje z poruszanymi wyżej zagadnieniami, zawiera publikacja Ch. Poszwińskiego. Autor ten pisze, że: *Badanie należy rozpocząć od zidentyfikowania zasad przetwarzania panujących w danej organizacji. Nieprawidłowa identyfikacja może prowadzić do błędnych konkluzji na temat potencjalnego ryzyka, a to z kolei będzie negatywnie wpływać na osoby, których dane dotyczą*[200]. Z poglądem wskazanego autora w zasadzie się zgadzam, z tym jednak uzupełnieniem, że zasady, o których pisze Ch. Poszwiński, zostały wskazane przez prawodawcę w art. 5 RODO.

3.4 Art. 32 ust. 1 i 2 i 3 Uwaga 4

Błędy w ocenie ryzyka

– Błędem jest pominięcie oceny ryzyka naruszenia praw i wolności we własnej, stosowanej przez administratora procedurze oceny ryzyka.
– Błędem jest ocena ryzyka naruszenia praw i wolności traktowanych jako całość. Podkreślenia wymaga, że administrator ma obowiązek ocenić konkretne prawa i konkretne wolności, które przysługują konkretnym osobom.
– Błędem jest pominięcie praw i wolności zapisanych w art. 5 RODO. Jeśli chodzi o pozostałe prawa i wolności zapisane w RODO, czyli o prawa i wolności szczegółowe, związane z przepisami szczegółowymi RODO, to wydaje się, że pominięcie tych praw i wolności w ocenie jest błędem mniejszej wagi, o ile w ogóle jest błędem. Zasady z art. 5 RODO są konkretyzowane przez przepisy szczegółowe RODO, jeżeli zatem administrator kompetentnie oceni ryzyko naruszenia praw i wolności z art. 5 RODO, to można założyć, że tym samym dokonał oceny ryzyka naruszenia praw i wolności zapisanych w przepisach szczegółowych RODO.
– Błędem jest pominięcie w ocenie ryzyka, zagrożeń wymienionych w art. 32 ust. 2 RODO. Zagrożenia te wymieniam wyżej w uwagach (*3.2. Art. 32 ust. 1 i 2 i 3 Uwaga 2. Zagrożenia uporządkowane w oparciu o kryterium konkretnego zagrożenia*) i (*3.3 Art. 32*

[200] Ch. Poszwiński, op. cit., s. 34.

ust. 1 i 2 i 3 Uwaga 3. Zagrożenia uporządkowane w oparciu o kryterium czynności).

Tytułem smutnego komentarza muszę odnieść się do publikacji A. Kaczmarka, A. Łapińskiej, A. Miłochy i M. Młotkiewicz. Autorzy ci, w artykule *Nowa optyka w ocenie ryzyka*[201] usiłują odnieść się do oceny ryzyka na gruncie RODO. Piszę, że usiłują, ponieważ autorzy ci poruszają się w miarę sprawnie w siatce pojęciowej RODO i nie jest moim celem recenzowanie tego artykułu, ale na jeden fragment muszę zwrócić uwagę. Wspomniani autorzy piszą: *Rodo nie odnosi się wprost do procesu zarządzania ryzykiem*. Co pozwoliło autorom na sformułowanie takiej myśli, pozostanie dla mnie tajemnicą. W RODO mowa jest o ryzyku w art. 24 ust. 1, w art. 32 ust. 1, w art. 33 (ryzyko jest tu oceniane, co prawda po fakcie, ale przecież przez pryzmat oceny tych samych praw i wolności co na gruncie art. 24 i 32) w art. 34 (sytuacja podobna jak w art. 33). Prawodawca wskazuje prawa i wolności w art. 5 RODO, prawodawca wskazuje zagrożenia techniczne w art. 32 ust. 2 RODO. Wymieniłem tu przepisy najbardziej – z punktu widzenia ryzyka naruszenia praw i wolności na gruncie RODO – oczywiste. Jest ich znacznie więcej. Prawodawca wskazuje zatem, kiedy ryzyko oceniać należy i jakie parametry należy brać pod uwagę. Cóż jeszcze miałby wskazać prawodawca, jak jaśniej napisać przepisy, by wskazani autorzy je zrozumieli, a zwłaszcza zrozumieli, że RODO w przeciwieństwie do tego, co piszą, odnosi się do procesu zarządzania ryzykiem i to odnosi się wprost.

Dalej wskazani autorzy piszą, że RODO *[...] nie wskazuje konkretnej metody przeprowadzania oceny w tym zakresie*. Fakt, metody może i RODO nie wskazuje, jednak składowe takiej metody, RODO podaje na tacy.

I jeszcze: *Niewątpliwie jednak jednym ze skutecznych, systemowych sposobów dokonywania takiej oceny jest wdrożenie procesu zarządzania ryzykiem w danej jednostce. Obecnie jest dostępnych wiele metod, z których można czerpać inspirację i dobre przykłady dla tworzenia własnych rozwiązań*. Dalej wskazani autorzy odnoszą się do metod podmiotów, takich jak Ministerstwo cyfryzacji, CNIL, ISACA i do metod zbudowanych na podstawie normy ISO. I wszystko byłoby

[201] A. Kaczmarek, A. Łapińska, A. Miłocha, M. Młotkiewicz, *Nowa optyka w ocenie ryzyka*, „ABI Expert" 2017, nr 4(5), s. 24–25.

dobrze, gdyby wspomniani autorzy choć napomknęli w swoim artykule o prawach i wolnościach z art. 5 RODO i o zagrożeniach z art. 32 ust. 2 RODO. Niestety, tego nie uczynili.

Tak artykułów pisać nie wolno. Nie wolno odsyłać do metod tworzonych przez różne, choćby szacowne podmioty i jednocześnie nie wspominać przy tym, że prawodawca zapisał w RODO prawa i wolności i że prawodawca zapisał w RODO zagrożenia techniczne. Nie wolno, bo tak napisany artykuł może mniej kompetentnych czytelników skierować do tamtych metod i skłonić do pominięcia elementów, które prawodawca umieścił w RODO w sposób celowy i zdecydowanie niemetaforyczny. Innymi słowy, nie wolno zastępować prawa – praktyką.

Nie jestem zwolennikiem pisania prac naukowych opierając się na cudzych poglądach; cudze poglądy szanuję, odwołuję się do nich i czasem nawet z nich korzystam, nie jestem zwłaszcza zwolennikiem nieustannego polemizowania z mało ciekawymi poglądami czy tekstami, chyba, że te teksty są szkodliwe. Tekst przywołany zdaje się być niebezpieczny i to z trzech przyczyn. Merytorycznie, czytelnik bowiem, który tekstowi temu zawierzy, pominie przy dokonywaniu ocen, elementy, których mu pominąć nie wolno. Autorzy tekstu są przedstawieni jako pracownicy (jeszcze) GIODO, co może wzbudzić zaufanie do ich tekstu. Niestety nie do końca uzasadnione. Wreszcie tekst promuje podejście niezgodne z prawem, a przynajmniej sugerujące omijanie prawa.

Kontrowersyjny pogląd sformułowali M. Gumularz i T. Izydorczyk. Otóż wskazali oni cztery metody identyfikacji zagrożeń (źródeł ryzyka). Są to ich zdaniem:

1) korzystanie z gotowych katalogów zagrożeń,
2) korzystanie z doświadczenia źródeł zewnętrznych,
3) korzystanie z własnego doświadczenia administratora lub podmiotu przetwarzającego,
4) burza mózgów zespołu oceniającego[202].

Wskazanym w cytacie źródłom nie sposób nic zarzucić. Pozornie. Jeżeli bowiem wnikliwie przeczytamy cytowane zalecenia, to musimy zadać pytanie o to, dlaczego wskazani autorzy nie odesłali również do zagrożeń wymienionych przez prawodawcę w art. 32 ust. 2 RODO.

[202] M. Gumularz, T. Izydorczyk, op. cit., s. 68–69.

Można próbować uzasadnić pogląd wskazanych autorów i twierdzić, że konieczność korzystania z art. 32 ust. 2 RODO wynika np. *z doświadczenia źródeł zewnętrznych*, czy *z doświadczenia administratora lub podmiotu przetwarzającego*, ale powiedzmy otwarcie, że wskazani autorzy o art. 32 ust. 2 RODO ewidentnie zapomnieli.

Pozostaje podkreślić, że administratorowi danych osobowych o przepisie zapomnieć nie wolno! Dalej wskazani autorzy polecają źródła, z których można korzystać jako z list kontrolnych[203] i nadal nie wskazują na art. 32 ust. 2 RODO. To pominięcie jest dla mnie niezrozumiałe. Niezrozumiałe tym bardziej, że stronę dalej trafnie wskazują na prawa i wolności z art. 5, jako na coś, na co należy zwracać uwagę przy ocenianiu ryzyka. Co prawda, nie używają tam podejścia opartego na systemie prawo/obowiązek/wolność, ale posługują się nazwami zasad z art. 5 RODO[204], a nawet w tabeli używają określenia „Zasady ogólne", także mimo wszystko do zasad się odnoszą.

Podobne, nieco ignorujące szczegóły RODO, podejście do oceniania ryzyka dostrzegam u Ch. Poszwińskiego. Autor ten nie wyjaśnia w swojej książce, jak należy oceniać ryzyko, odnosi się on jednak do metod oceniania ryzyka, po prostu je wymienia. Niestety, wśród metod wymienionych przez wskazanego autora nie znajdujemy metody opartej na stosowaniu art. 32 ust. 2 RODO w połączeniu z art. 5 RODO. Chrystian Poszwiński powołuje się na wystąpienie RODO, na normę techniczną, jednak na RODO – nie. Podobnie jak w odniesieniu do pozostałych autorów, uważam to za bolesne pominięcie.

3.5 Art. 32 ust. 1 i 2 i 3 Uwaga 5

Prawa i wolności

R*yzyko naruszenia praw i wolności osób fizycznych* jest okolicznością, którą administrator ma obowiązek wziąć pod uwagę przy wykonywaniu oceny ryzyka. W związku z tym istotne jest, jakie prawa i wolności należy brać pod uwagę przy dokonywaniu oceny ryzyka.

Uważam, że przede wszystkim należy brać pod uwagę prawa i wolności wskazane w RODO. W RODO wskazane są dwie kategorie praw i wolności.

---

[203] Ibidem, s. 70.

[204] Ibidem, s. 71.

– Pierwsza z nich to prawa i wolności, które zapisane są w art. 5 RODO, jako zasady, przeto najlepiej zwać je prawami i wolnościami zasadniczymi.
– Druga to prawa i wolności szczegółowe, które tak nazywam, związane są one bowiem z przepisami szczegółowymi RODO.

Jedne i drugie wypisałem w książce wydanej w tym samym cyklu co książka niniejsza, a to w książce *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*[205]. Nie powtarzam ich tutaj, ponieważ nie widzę sensu, by rzecz tak prostą umieszczać w wywodzie w kolejnej książce. Dla ułatwienia prowadzenia oceny ryzyka w praktyce, na końcu niniejszej książki zamieszczam przykładowe tabele.

Na wskazane wyżej dwie kategorie praw i wolności trzeba zwrócić uwagę z uwagi na dyrektywę języka prawnego[206]. Poza tym, przy ocenie ryzyka można brać pod uwagę prawa podstawowe, które są wymienione w karcie praw podstawowych. Również wypisałem je (prawdopodobnie) wszystkie w książce wydanej jednocześnie z niniejszą[207], nie uważam jednak, by ocenianie prawdopodobieństwa naruszenia tych praw było celowe przy wykonywaniu oceny ryzyka na gruncie art. 32 RODO. Pogląd ten wyrasta z analizy poszczególnych praw podstawowych, które – z bardzo małymi wyjątkami – nie mają nic wspólnego z ochroną danych osobowych.

Pewne prawa i wolności wymienione są w motywie 4 Preambuły RODO, jednak mam ambiwalentny stosunek do koncepcji brania ich pod uwagę przy dokonywaniu oceny ryzyka. Ambiwalencja moja wynika z faktu, że co prawda prawodawca wymienia je w RODO, ale jednak wymienia je jedynie jako prawa i wolności przykładowe i prócz tego wskazuje, że *Niniejsze rozporządzenie nie narusza praw podstawowych, wolności i zasad uznanych w Karcie praw podstawowych – zapisanych w Traktatach*. Czyli na dobrą sprawę wskazane w przepisie prawa i wolności, wskazane są jedynie jako przykład praw i wolności, których RODO nie narusza. Innymi słowy, z przepisu tego wynika, że inne niż wskazane w RODO prawa i wolności również funkcjonują i że RODO ich nie niweczy, nie oznacza to jednak –jak uważam – że te właśnie prawa i wolności należy brać pod uwagę przy do-

[205] L. Morawski, op. cit., s. 93–95.

[206] Ibidem.

[207] J. Rzymowski, *RODO – GDPR. Przedmiot…*, s. 126–143.

konywaniu oceny ryzyka i to właśnie dlatego, że prawodawca wskazuje je w motywie 4 Preambuły RODO – bo cel tego wymienienia był inny. Nic nie stoi na przeszkodzie, by prawa i wolności wymienione w Karcie Praw Podstawowych Unii Europejskiej brać pod uwagę przy dokonywaniu oceny ryzyka, jednak nie dlatego, że prawodawca je rzekomo w motywie 4 Preambuły RODO wskazuje, ale raczej dlatego, że taką decyzję podejmuje administrator.

Ciekawy pogląd sformułował R. Kania. Stwierdził on mianowicie, że ryzyko naruszenia praw i wolności (autor pisze „lub") materializuje się na trzech poziomach. Podział R. Kani przytaczam poniżej.

– *Poziom pierwszy to ryzyko naruszenia praw podstawowych wskazanych w traktatach (motyw 4 rodo) […]*
– *Poziom drugi to naruszenia praw wynikające wprost z rodo, m.in. takie jak prawo do bycia poinformowanym, prawo do bycia zapomnianym […]*
– *Poziom trzeci to poziom najbardziej przyziemny związany z naruszeniem praw i wolności osobistych w przetwarzaniu danych osobowych. Najpełniejsza ich listę wskazuje motyw 75. Są wśród nich konsekwencje takie jak dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości […]*[208]

Przytaczam powyżej wypowiedzi R. Kani, nie znaczy to jednak, że się z nim w całości zgadzam. Odnoszę się do tego posługując się terminologią autora. Uważam, że błąd czyni R. Kania, wskazując na prawa i wolności poziomu pierwszego. Istotę błędu wyjaśniam wyżej w niniejszej uwadze. Błąd czyni R. Kania, pomijając prawa i wolności wynikające z art. 5 RODO. Patrząc przychylnie na słowa R. Kani, można próbować wyprowadzić konieczność wzięcia tych praw i wolności pod uwagę z opisu praw i wolności poziomu drugiego, jednak będąc szczerym – o zasadach R. Kania nie wspomniał. Co do praw i wolności poziomu trzeciego – są one w RODO, co nakazywałoby wziąć je pod uwagę, jednak faktem jest, że są one wymienione w przepisie w sposób dość chaotyczny, prawodawca – moim zdaniem – miesza tam prawa i wolności z zagrożeniami technicznymi, a wszystko czyni w sposób nieuporządkowany. Co więcej, dokładna lektura przepisu każe sądzić, że prawodawca do praw i wolności jedynie się w nim odnosi,

[208] R. Kania, *Ryzyko, czas i cudze prawa – proces ochrony danych*, „ABIEXPERT" 2018, nr 2(7), s. 34–36.

wymienia zaś w nim zagrożenia, które mogą skutkować naruszeniem praw i wolności, czyli są to raczej zagrożenia, które – jeśli chcielibyśmy ująć w ocenie ryzyka, to nie na etapie oceny ryzyka naruszenia praw i wolności, ale na etapie oceny ryzyka technicznego, o którym mowa w art. 32 ust. 2 RODO.

Podkreślenia wymaga, że dla potrzeb realizacji obowiązków wynikających z art. 32 RODO należy brać pod uwagę te same prawa i wolności, które bierze się pod uwagę dla potrzeb realizacji obowiązków wynikających z art. 24 RODO. Na zjawisko to zwraca uwagę K. Wygoda, który pisze[209], że art. 32 RODO jest rozwinięciem (m.in.) art. 24 RODO. Ja uważam, że w art. 32 RODO chodzi raczej o bezpieczeństwo danych osobowych, a w art. 24 RODO chodzi raczej o zgodność z prawem przetwarzania danych osobowych, myślę jednak, że różnimy się tu z K. Wygodą raczej w warstwie językowego wyrażenia myśli niż w treści tychże.

Do dłuższych rozważań na temat praw i wolności odsyłam wyżej do uwagi (*3.1. Art. 24 Uwaga 1.Prawa i wolności*) i uwag kolejnych, zawierających częściowe zestawienia odpowiednich dla rozważań, praw i wolności. Odsyłam również na koniec książki do części *Tabele pomocnicze, zestawienia*, w której zamieszczone są zestawione prawa i wolności oraz odpowiednie tabele, umożliwiające dokonywanie kolejnych ocen.

3.6 Art. 32 ust. 1 i 2 i 3 Uwaga 6

Podmioty zobowiązane

Obowiązki wynikające z przepisu spoczywają na administratorze i na podmiocie przetwarzającym, odmiennie niż jest to rozwiązane w art. 24 RODO, który nakłada obowiązki wyłącznie na administratora[210]. Należy przy tym pamiętać, że o ile w przypadku współadministrowania, administratorzy mogą umówić się co do zakresu obowiązków realizowanych przez każdego z nich, o tyle podmiot przetwarzający ma obowiązek zrealizować obowiązki wynikające z art. 32 RODO i nie ma od tego żadnych odstępstw.

---

[209] K. Wygoda, [w:] M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018, s. 354.

[210] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 343.

Uwagę na to zwrócili K. Wygoda[211] oraz P. Barta, M. Kawecki i P. Litwiński[212]. I tu trzeba dokonać pewnego uzupełnienia. Otóż K. Wygoda napisał, że *Głównym adresatem norm […] jest administrator*. I dalej, że *[…] adresatem obowiązku wdrożenia […] jest również podmiot przetwarzający*. Z wypowiedzi K. Wygody można by wywnioskować, że obowiązki wynikające z art. 32 RODO spoczywają na administratorze bardziej (cokolwiek miałoby to znaczyć) niż na podmiocie przetwarzającym. Podmiot przetwarzający, który przeczytałby wypowiedź K. Wygody, mógłby nabrać mylnego przypuszczenia, że skoro administrator, który powierzył mu przetwarzanie danych, wykonał ocenę ryzyka, to on – podmiot przetwarzający, nie musi tego czynić. Byłoby to oczywiście błędem.

Podkreślić należy, że obowiązki wynikające z art. 32 RODO spoczywają na administratorze i na podmiocie przetwarzającym[213].

Pamiętając, że obowiązki wynikające z art. 32 RODO spoczywają na administratorze i na podmiocie przetwarzającym, należy zastanowić się, czy oceny ryzyka dokonywane przez administratora i przez podmiot przetwarzający powinny się różnić, a jeżeli tak, to czym się różnić powinny.

W kilku miejscach niniejszej publikacji, w tym niniejszego rozdziału, zastanawiam się nad tym, jakie parametry administrator danych osobowych ma obowiązek brać pod uwagę przy ocenie ryzyka. Należy podkreślić, że podmiot przetwarzający powinien wziąć pod uwagę te same parametry. Podmiot przetwarzający powinien wziąć pod uwagę wszystkie parametry z art. 32 ust. 2 RODO i przeanalizować je przez pryzmat wszystkich czynników z art. 32 ust. 1 RODO. Następnie podmiot przetwarzający powinien wziąć pod uwagę prawa i wolności z art. 5 RODO (zapisane w zasadach) i ewentualnie inne prawa i wolności. Wymienione elementy oceny ryzyka są takie same dla administratora i dla podmiotu przetwarzającego. Coś jednak te oceny odróżnia.

---

[211] K. Wygoda, [w:] M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO?...*, s. 356.

[212] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 343.

[213] C. Burton, op. cit., s. 634.

– Administrator powinien jako podstawę oceny ryzyka przyjąć czynności ze swojego rejestru czynności przetwarzania danych osobowych, sporządzanego na podstawie art. 30 ust. 1 RODO.
– Podmiot przetwarzający jako podstawę oceny ryzyka powinien przyjąć czynności ze swojego rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, sporządzanego na podstawie art. 30 ust. 2 RODO. Podmiot przetwarzający zwykle (o ile nie zawsze) jest również administratorem, tyle, że innych danych niż te, których przetwarzanie mu powierzono (zlecono), ocena ryzyka wykonywana w związku z tymi danymi jest oczywiście wykonywana na podstawie rejestru czynności przetwarzania danych osobowych, sporządzanego na podstawie art. 30 ust. 1 RODO.

3.7 Art. 32 ust. 1 i 2 i 3 Uwaga 7

Czynności jako podstawa oceny ryzyka

Sygnalizuję wyżej w niniejszym rozdziale – jak również w rozdziale poświęconym art. 24 RODO – że uważam, iż za podstawę wykonywanej oceny ryzyka należy przyjąć rejestr czynności. W odniesieniu do administratora jest to rejestr czynności przetwarzania danych osobowych, przygotowywany na podstawie art. 30 ust. 1 RODO; w odniesieniu do podmiotu przetwarzającego jest to rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, przygotowywany na podstawie art. 30 ust. 2 RODO. To jest podejście proste, racjonalne i jak się wydaje, spójne z jednym z ogólnych „momentów" RODO, z którego wynika, że swojego rodzaju osią przetwarzania, jak i ochrony danych osobowych jest czynność.

Możliwe jest też inne podejście, które jednak, w odniesieniu do podmiotów, które posiadają wskazane wyżej rejestry, nie wydaje się roztropne. Otóż za podstawę wykonywanej oceny ryzyka można przyjąć zbiór. Z art. 30 ust. wynika spełnienie, jakich kryteriów skutkuje obowiązkiem stworzenia rejestru czynności przetwarzania danych osobowych przez administratora lub podmiot przetwarzający. Jeżeli administrator lub podmiot przetwarzający kryteriów tych nie spełnia, to nie ma obowiązku tworzenia rejestru. Wolno mu oczywiście taki rejestr stworzyć, jednak czyni to wtedy, „bo chce", a nie „bo musi". Pokusa nietworzenia rejestru może być tak silna, że administrator lub podmiot przetwarzający rejestru nie stworzy. Wtedy nie pozostaje mu nic inne-

go, niż przyjąć zbiory za podstawę oceny ryzyka. Należy poczynić tu jeszcze pewne uwagi.

Wykonywanie oceny ryzyka na podstawie czynności jest wygodniejsze i prostsze niż wykonywanie oparte na zbiorach.

Jeżeli administrator lub podmiot przetwarzający nie ma obowiązku wykonywania oceny ryzyka, to wydaje się, że lepiej, by stworzył listę czynności i na jej podstawie wykonał ocenę ryzyka, niż by miał wykonywać ocenę ryzyka opartą na zbiorach.

Wykonywanie oceny ryzyka opartej na zbiorach jest niewygodne, ponieważ te same dane mogą należeć do różnych zbiorów.

W tym miejscu wypada odnieść się do słów P. Siembidy, który pisze, co prawda w podsumowaniu dłuższego rozważania, ale jednak pisze, że *[...] czynność przetwarzania w rozumieniu RODO składa się z operacji*[214], co jest twierdzeniem bałamutnym i zadziwiającym, które wynika – jak mniemam – z pobieżnej lektury definicji przetwarzania, która znajduje się w art. 4 pkt 2 RODO. Nie chcę tu prowadzić dłuższych polemik, ograniczę się jedynie do wskazania, że przetwarzanie danych osobowych oznacza czynność na danych osobowych.

Kluczową rolę rejestru czynności jako elementu niemal koniecznego oceny ryzyka dostrzegają E. Bielak-Jomaa i D. Lubasz. Dodatkowo cieszy mnie, że wskazani autorzy proponują[215] model rejestru czynności analogiczny wobec modelu, który w 2019 roku zaproponowałem w książce poświęconej dokumentacji ochrony danych[216]. Istotą tego modelu jest poświecenie każdej czynności przetwarzania osobnej karty rejestru. Rejestr w ujęciu wskazanych autorów jest wzbogacony o elementy dodatkowe, co chyba czyni go lepszym, ale model jest zdecydowanie ten sam. Piszę, że mnie to cieszy, widzę bowiem, że myśl prawnicza, mimo że niezależnie rozwijana, powraca do pewnych rozwiązań, a rejestr oparty na takim modelu jest praktyczniejszy od rejestru zapisanego w tabeli, zwłaszcza z punktu widzenia obowiązku prowadzenia rejestru w formie pisemnej, jakkolwiek by ten obowiązek rozumieć. Zjawisko krążenia myśli prawniczej jest niezwykle ciekawe, pozostając przy rejestrze, wskazani autorzy proponują również wersję rozwiniętą swojego rejestru,

---

[214] P. Siembida, [w:] A. Krasuski, P Siembida, *Analiza ryzyka w ochronie danych osobowych*, Warszawa 2022, s. 133.

[215] E. Bielak-Jomaa, D. Lubasz, op. cit., s. 41–42.

[216] J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja…*, s. 31–56.

która jest z kolei oparta na tym samym modelu, na którym oparta jest propozycja rejestru w książce o ochronie danych medycznych autorstwa mojego i D. Spałka[217]. Autorem modelu w naszej książce jest D. Spałek. Opisuję te zjawiska, widać bowiem, że myśl prawnicza krąży w sposób, mimo że nieskoordynowany, to podobny.

3.8 Art. 32 ust. 1 i 2 i 3 Uwaga 8

Realność obowiązku oceny ryzyka

Niniejszy podrozdział mógłby równocześnie nosić nazwę „Czy z art. 32 RODO na pewno wynika obowiązek wykonywania oceny ryzyka". Wątpliwość w tej kwestii może mieć dwa przejawy.

– Po pierwsze należy się zastanowić, czy na administratorze (tu również podmiocie przetwarzającym) spoczywa obowiązek dokonywania oceny ryzyka. Czy ten obowiązek spoczywa na nich w sensie bezwzględnym, rzec można „w ogóle".
– Po drugie, jeżeli odpowiedź na pierwsze pytanie jest twierdząca, czyli jeżeli obowiązek spoczywa, to czy wynika on na pewno z art. 32 RODO, a nie z art. 24 RODO.

Zastanawiając się nad pierwszą wątpliwością, należy stwierdzić, że na administratorze (również na podmiocie przetwarzającym) spoczywa obowiązek oceny ryzyka. Wnosimy o tym ze słów art. 32 ust. 1 RODO: *Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze […]* Analogiczne słowa znajdują się w art. 24 ust. 1 RODO. O obowiązku dokonywania oceny ryzyka mowa jest również w motywie 83 Preambuły RODO. Stanowi on, jak wskazuję poniżej. Na przepis ten jako na źródło obowiązku wykonywania oceny ryzyka zwraca uwagę[218] C. Burton i to, co ciekawe, w komentarzu do art. 32 RODO.

W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla

[217] J. Rzymowski red., D. Spałek, *RODO – GDPR. Ochrona danych medycznych,* Łódź 2022, s. 88–93.

[218] C. Burton, op. cit., s. 631.

przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej, oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

Nie chcę tu dokonywać drobiazgowej analizy cytowanego przepisu, wymieniam jednak poniżej istotne – z punktu widzenia rozważanych wątpliwości – elementy, które z niego wynikają. **Celem**, który jest wskazany jako cel do osiągnięcia, jest:
– zachowanie bezpieczeństwa i
– zapobieganie przetwarzaniu niezgodnemu z RODO.

Zwracam uwagę, że z zachowaniem bezpieczeństwa jest raczej związany art. 32 RODO, a z zapobieganiem przetwarzaniu niezgodnemu z RODO jest raczej związany art. 24 RODO. Analizuję to wyżej w uwadze *(3.12. Art. 24. Uwaga 12. Ocena ryzyka naruszenia praw i wolności z art. 24 RODO a ocena ryzyka naruszenia praw i wolności z art. 32 RODO*).

Obowiązek szacowania ryzyka spoczywa odpowiednio na:
– administratorze i
– podmiocie przetwarzającym.

Zwracam przy tym uwagę, że art. 32 RODO nakłada obowiązek wykonywania oceny ryzyka na obydwa te podmioty, czyli na administratora i podmiot przetwarzający.

Środki, jakie wdraża administrator powinny zapewnić poziom bezpieczeństwa, który jest odpowiedni do ryzyka.

Skoro poziom bezpieczeństwa ma być odpowiedni do ryzyka, to trzeba to ocenić, nie da się orzec, że coś jest odpowiednie do czegoś. bez przeprowadzenia oceny tej odpowiedniości.

We wskazanym motywie Preambuły jest też mowa o tym, że:
– *oceniając ryzyko w zakresie bezpieczeństwa danych,*

– *należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych*.

Zwracam uwagę, że w cytowanej części motywu, prawodawca traktuje ocenianie ryzyka jako coś oczywistego i jedynie uzupełnia, że wykonując tę oczywistą czynność, należy wziąć pod uwagę wskazaną okoliczność.

Jak widać z powyższych uwag, w motywie 83 Preambuły RODO są co najmniej cztery elementy, które wskazują, że oceny ryzyka dokonywać należy, a mówiąc dokładniej, że administrator i podmiot przetwarzający mają obowiązek wykonywać ocenę ryzyka.

– Po drugie, jeżeli odpowiedź na pierwsze pytanie jest twierdząca, czyli jeżeli obowiązek spoczywa, to czy wynika on na pewno z art. 32 RODO, a nie z art. 24 RODO.

Zastanawiając się nad drugą wątpliwością, należy stwierdzić, że obowiązek wykonywania oceny ryzyka wynika raczej z art. 32 RODO niż z art. 24 RODO. Drobiazgowe rozważania na ten temat prowadzę wyżej w uwadze (*3.12. Art. 24. Uwaga 12. Ocena ryzyka naruszenia praw i wolności z art. 24 RODO a ocena ryzyka naruszenia praw i wolności z art. 32 RODO*). Nie ma powodu streszczać prowadzonych wyżej rozważań, warto jedynie zwrócić uwagę na chyba najistotniejszy ich element, który wskazuje na to, że ocenie ryzyka, rozumianego jako ryzyko techniczno-organizacyjne, poświęcony jest art. 32 RODO, nie zaś art. 24 RODO. Otóż tym, co – jak uważam tu przesądza – jest cel przepisu. Celem art. 24 ust. 1 RODO jest: *aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać*. Celem art. 32 ust. 1 RODO jest *aby zapewnić stopień bezpieczeństwa odpowiadający […] ryzyku*.

3.9 Art. 32 ust. 1 i 2 i 3 Uwaga 9

Wykazanie oceny ryzyka

Jedna z różnic między art. 24 RODO a art. 32 RODO każe zastanowić się nad tym, czy administrator i podmiot przetwarzający mają obowiązek być w stanie wykazać, że wykonali oceny ryzyka. Obowiązek wykazania wspomnianej oceny jest do art. 24 ust. 1 wpisany wprost, widnieje tam bowiem: *i aby móc to wykazać*. W art. 32 nie napotykamy bezpośredniego odpowiednika takich słów, nie zna-

czy to jednak, że analogiczny obowiązek na administratorze nie spoczywa, aczkolwiek trzeba się nad tym przez chwilę pochylić.

O wykazaniu realizacji obowiązku mowa jest w art. 32 ust. 3 RODO, który stanowi: *Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42*. Jak widać, prawodawca przyjmuje tu wykazanie obowiązku jako coś oczywistego, tyle że czyni to niejako przy okazji wskazania dwóch szczególnych metod wykazania realizacji obowiązku (skracając) kodeksu lub certyfikatu. Przy pewnej dozie wyrozumiałości dla zmagań prawodawcy można uznać, że obowiązek wykazania realizacji obowiązków wynikających z art. 32 ust. 1 RODO, wynika z art. 32 ust. 3 RODO. Mając na uwadze niezliczone niekonsekwencje i (nie bójmy się tego powiedzieć), błędy w RODO, można jednak rozumieć administratora danych osobowych lub podmiot przetwarzający, którzy będą się nieufnie odnosić do interpretacji, zgodnie z którą obowiązek wykazania realizacji obowiązków wynika z art. 32 ust. 3 RODO.

Obowiązek wykazania realizacji obowiązków wynika jednak również z innego przepisu. Nie pozostaje nic innego, jak powtórzyć myśl, którą zawarłem w publikacji będącej częścią niniejszego cyklu, a to: *z art. 5 ust. 2 RODO wynika obowiązek wykazania realizacji zasad. Skoro zasady są realizowane przez przepisy szczegółowe RODO, to jedynym narzędziem, środkiem, metodą wykazania realizacji zasad jest wykazanie realizacji przepisów szczegółowych RODO, które konkretyzują odpowiednie zasady*[219]. Kontynuując tę myśl, artykuł 32 ust. 1 RODO jest konkretyzacją zwłaszcza zasady poufności i zasady integralności, aby zatem wykazać realizację tych zasad, co jest obowiązkiem, administrator (i podmiot przetwarzający) ma obowiązek wykazania realizacji między innymi art. 32 ust. 1 RODO.

Podsumowując, należy stwierdzić, że administrator danych osobowych ma obowiązek wykazania, że przeprowadził ocenę ryzyka. Obowiązek ten wynika z art. 5 ust. 2 RODO w zw. z art. 5 ust. 1 lit. f RODO. Uważam, że obowiązek ten wynika również – o czym piszę w bieżącym podrozdziale wyżej – z art. 32 ust. 3 RODO. Obowiązek ten wynika z jednego jeszcze źródła. Otóż bezsporne (jak uważam)

[219] J. Rzymowski, *RODO – GDPR. Przedmiot i cele…,* s. 55.

jest, że administrator ma obowiązek wykazania realizacji art. 24 ust. 1 RODO. Wynika to z treści tego właśnie art. 24 ust. 1 RODO. Jednocześnie można przyjąć, że realizacja art. 32 RODO stanowi etap realizacji art. 24 RODO.

Uważam, że obowiązek wykazania faktu przeprowadzenia oceny ryzyka spoczywa również na podmiocie przetwarzającym. Artykuł 32 ust. 1 RODO nakłada obowiązki nie tylko na administratora, ale na podmiot przetwarzający również. Co do tego wątpliwości nie ma, wątpliwość musi się pojawić, kiedy zastanawiamy się nad obowiązkiem wykazania przez podmiot przetwarzający realizacji obowiązków z art. 32 RODO. Rozumowanie musi tu iść podobną, choć nie dokładnie tą samą drogą jak powyżej.

Do podmiotu przetwarzającego można również odnieść słowa, które wyżej odnoszą się do administratora, a mianowicie: *można uznać, że obowiązek wykazania realizacji obowiązków wynikających z art. 32 ust. 1 RODO, wynika z art. 32 ust. 3 RODO*. Dodatkowy argument wynika z art. 28 ust. 3 lit. c RODO, z którego wynika, że podmiot przetwarzający ma obowiązek *podjąć wszelkie środki wymagane na mocy art. 32* RODO. Jeżeli zatem uznajemy, że z art. 32 RODO, a dokładnie z art. 32 ust. 3 RODO wynika obowiązek wykazania, że przeprowadzono ocenę ryzyka, to art. 28 ust. 3 lit. c RODO sprawia, że obowiązek ten spływa na podmiot przetwarzający, skutkiem czego podmiot przetwarzający również ma obowiązek wykazać, że przeprowadził ocenę ryzyka.

Kolejne źródło obowiązku wykazania realizacji obowiązku wynikającego z art. 32 RODO bije w art. 5 ust. 2DRODO, czyli w zasadzie rozliczalności. Dla podmiotu przetwarzającego bije ono tam słabo, ponieważ art. 5 ust. 2 jest skierowany do administratora. Można jednak wyprowadzić tu wniosek, że skoro podmiot przetwarzający przetwarza dane osobowe w imieniu administratora, to nie ma powodu, by uważać, że skoro administrator musi wykazać, że przeprowadził ocenę ryzyka, to podmiot przetwarzający wykazywać nie musi. Można nawet uznać, że wynika to z zasady *a fortiori*, że skoro administrator musi, to podmiot przetwarzający też, acz przyznam, że zasadę tę powołuję tu z pewnym niepokojem. Przypominam, że zastanawiam się nie nad obowiązkiem przeprowadzenia oceny ryzyka, ale nad obowiązkiem wykazania, że podmiot przetwarzający ją przeprowadził.

Ostatnia bodaj droga dotarcia do obowiązku wiedzie jeszcze inaczej. Administrator ma obowiązek wykazać, że przeprowadził ocenę ryzyka, o której mowa w art. 24 ust. 1 RODO. Celem art. 24 ust. 1 RODO jest między innymi wykazanie zgodności z prawem przetwarzania. Jeżeli część przetwarzania wykonuje podmiot przetwarzający, to obowiązek wykazania zgodności z prawem przetwarzania dotyczy również przetwarzania przez podmiot przetwarzający. Skoro administrator musi wykazać, że przetwarzanie również przez podmiot przetwarzający jest zgodne z prawem i skoro elementem oceny z art. 24 RODO jest ocena z art. 32 RODO, to wynika z tego, że podmiot przetwarzający musi wykonać ocenę i wykazać, że ją wykonał, co pozwoli administratorowi wykazać, że przetwarzanie przez podmiot przetwarzający jest zgodne z prawem. To z kolei współgra ze wskazanym wyżej art. 28 ust. 3 lit. c RODO, który nakazuje, by w zakresie realizacji art. 32 RODO podmiot przetwarzający działał tak jak administrator. Rozumowanie to zbieżne jest z treścią art. 28 ust. 3 lit. f RODO, z którego wynika, że podmiot przetwarzający ma obowiązek pomóc *administratorowi wywiązać się z obowiązków określonych w art. 32–36*.

Przyznam, że niniejsza, ostatnia „droga dotarcia do obowiązku" podoba mi się najmniej ze wskazanych, jednak nie jest to powodem, by jej nie wskazywać, tym bardziej że rozumowania w niej prowadzone nie są może eleganckie, ale wydają się być poprawne.

Nie jest sprawą pierwszorzędną, które rozumowanie podmiot przyjmie za swoje, czy może nawet przyjmie wszystkie, bez względu bowiem na to należy przyjąć wnioski, jakie wskazuję poniżej.

– Na administratorze spoczywa obowiązek wykonania oceny ryzyka, o której mowa w art. 32 RODO.
– Na administratorze spoczywa obowiązek wykazania, że wykonał ocenę ryzyka, o której mowa w art. 32 RODO.
– Na podmiocie przetwarzającym spoczywa obowiązek wykonania oceny ryzyka, o której mowa w art. 32 RODO.
– Na podmiocie przetwarzającym spoczywa obowiązek wykazania, że wykonał ocenę ryzyka, o której mowa w art. 32 RODO.

Wykazanie realizacji obowiązków jest niezwykle istotne, na co zwraca uwagę K. Wygoda, który wskazuje[220] na konieczność posiadania dokumentacji związanej z oceną ryzyka, z uwagi na fakt, że brak takowej przy jednoczesnym braku wdrożenia środków technicznych i organizacyjnych, może skutkować nałożeniem kary administracyjnej. Uważam, że można pójść nawet o krok dalej, otóż jeżeli nawet administrator wdroży środki, jednak mimo tego nastąpi zdarzenie skutkujące możliwością nałożenia kary administracyjnej, to brak dokumentacji, czy to dokumentacji oceny ryzyka, czy to dokumentu wdrożeniowego, czy odpowiedniego rejestru, będzie stanowił okoliczność obciążającą administratora lub podmiot przetwarzający.

Dziwna myśl zawarta została w publikacji P. Siembidy, który pisze, że: *RODO nie stawia przed administratorami danych osobowych zbyt wyszukanych wymagań w zakresie dokumentowania czynności przetwarzania*[221]. Dalej wskazany autor wspomina o: rejestrach czynności i politykach bezpieczeństwa (zauważmy jedynie, że obecnie, w art. 24 ust. 2 RODO czytamy, nie o politykach bezpieczeństwa, a o politykach ochrony danych)[222]. Czytamy, że *[...] warto również mieć udokumentowane inne kwestie, takie jak choćby metodyka, zgodnie z którą będzie przeprowadzona analiza ryzyka, odpowiednie klauzule w umowach ze współadministratorami i podmiotami przetwarzającymi dane w imieniu administratora, procedury, które wykażą zgodność postępowania z RODO, plany postępowania w szczególnych przypadkach (np. plan postępowania z incydentami), a także procedury, zgodnie z którymi będzie odbywało się przetwarzanie danych osobowych*. I dalej jeszcze o raportach z oceny ryzyka[223].

Podkreślenia wymaga, że dokumentacja, którą należy stworzyć na gruncie RODO, nie może ograniczać się do dokumentacji związanej z ryzykiem. To, co P. Siembida określił mianem procedur postępowania w poszczególnych przypadkach, to dokumenty bardzo często

---

[220] K. Wygoda, [w:] M. Sakowska–Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 356.

[221] P. Siembida, [w:] A. Krasuski, P Siembida, *Analiza ryzyka w ochronie danych osobowych*, Warszawa 2022, s. 135–136.

[222] Ibidem, s. 136.

[223] Ibidem.

spoza sfery ryzyka, które jednak również administrator ma obowiązek posiadać. Nawiązując do myśli P. Siembidy, nie wiem, czy wymagania w zakresie prowadzenia dokumentacji są wyszukane czy też nie, wiem jednak, że administrator ma obowiązek wykazać, że realizuje wszystkie zasady z art. 5 ust. 1 RODO. Zasady z art. 5 ust. 1 RODO są konkretyzowane przez odpowiadające im przepisy szczególne RODO, aby zatem wykazać realizację zasad, administrator danych osobowych ma obowiązek wykazać realizację przepisów, które odpowiadają zasadom.

3.10 Art. 32 ust. 1 i 2 i 3 Uwaga 10

Ustalenie kolejności czynności

Mając na uwadze ustalenia poczynione w uwadze (*3.9 Art. 32 ust. 1 i 2 i 3 Uwaga 9. Wykazanie oceny ryzyka*), należy zastanowić się nad kolejnością czynności, jakie powinien podjąć administrator (lub podmiot przetwarzający) w związku z wykonaniem oceny ryzyka, o której mowa w art. 32 ust. RODO.

Administrator (lub podmiot przetwarzający) ma obowiązek uwzględnić *stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania*. Ustalenie szczegółów przetwarzania, czyli zwłaszcza tego, jakie czynności podmiot wykonuje, wydaje się być pierwszą czynnością do wykonania. Najlepiej wykonać to, przygotowując rejestr czynności przetwarzania danych osobowych, za które odpowiada administrator, o którym to rejestrze mowa jest w art. 30 ust. 1 RODO lub jeżeli podmiot jest podmiotem przetwarzającym, to przygotowując rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, o którym to rejestrze mowa jest w art. 30 ust. 2 RODO. Jeżeli administrator nie ma obowiązku przygotować rejestru, to dobrze, by przygotował po prostu listę czynności, która stanie się podstawą wykonywanej oceny ryzyka.

Teoretycznie ocenę ryzyka można próbować wykonywać nie opierając się na czynnościach, lecz na zbiorach danych osobowych, jednak przypominam, że w art. 32 ust. 1 RODO mowa jest o przetwarzaniu, czyli o czynnościach. Radykalny zwolennik dokonywania ocen nie opierając się na czynnościach, mógłby twierdzić, że przechowywanie danych w zbiorze to też czynność, więc wykonywanie ocen ryzyka opartych na zbiorach jest dopuszczalne. Ja takim radykałem nie jestem, ba – w ogóle nie jestem zwolennikiem wykonywania ocen,

opierając się na zbiorach. Jednocześnie zwracam uwagę, że dane osobowe, które są przetwarzane w sposób zautomatyzowany, nie muszą znajdować się zbiorze ani być do zbioru przeznaczone, a i tak znajdują się w zakresie RODO, co wynika z art. 2 ust. 1 RODO, więc wykonanie oceny ryzyka opartej na zbiorach pozostawiłoby takie dane poza zakresem oceny.

W przepisie jest następnie mowa o wdrożeniu środków technicznych i organizacyjnych, jednak wdrożenie nie jest drugą czynnością. Wdrożenie następuje na końcu. Należy pamiętać, że obok wdrożenia w sensie materialnym, czyli rozpoczęcia stosowania konkretnych rozwiązań, należy przygotować wdrożenie w sensie formalnym, czyli stworzyć dokumentację wdrożeniową. Z dokumentacji tej powinno wynikać, że dany środek techniczny lub organizacyjny jest powiązany z daną czynnością i ma obniżać dane zagrożenie lub ma danemu zagrożeniu zapobiegać. Dokument wdrożeniowy to swojego rodzaju łącznik między oceną ryzyka a ogólnym opisem *technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1* RODO. Brak dokumentu wdrożeniowego czy też dokumentów wdrożeniowych, na co zwraca uwagę[224] K. Wygoda, może stanowić okoliczność obciążającą administratora lub podmiot przetwarzający w sytuacji nakładania kary administracyjnej.

Po ustaleniu, jakie czynności są wykonywane, czyli tym samym, jakie czynności będą podlegać ocenie, administrator (lub podmiot przetwarzający) dokonuje oceny ryzyka *naruszenia praw lub wolności osób fizycznych*. Przy dokonywaniu tej oceny należy brać pod uwagę (różne) prawdopodobieństwo wystąpienia i wagę.

Z art. 32 ust. 2 RODO wynika obowiązek dokonania oceny, *czy stopień bezpieczeństwa jest odpowiedni*. Ocena ta ma charakter techniczny, bardziej nieco szczegółowy niż ocena ryzyka naruszenia praw i wolności. Jednocześnie ocena odpowiedniości stopnia bezpieczeństwa wydaje się być składową czy też etapem oceny ryzyka naruszenia praw i wolności, a skoro tak, to ocena ta powinna być wykonana przed oceną ryzyka naruszenia praw i wolności.

Przed ustaleniem ostatecznej kolejności czynności należy uświadomić sobie, że każda czynność musi być udokumentowana. Piszę o tym wyżej w uwadze (*3.9 Art. 32 ust. 1 i 2 i 3 Uwaga 9 Wykazanie*

[224] K. Wygoda, op. cit.

oceny ryzyka). Poza tym napisałem o tym osobną książkę[225], będącą częścią niniejszego cyklu.

Przemysław Siembida wywodzi, że: *Modele procesów wykorzystujących dane osobowe (czynności przetwarzania danych osobowych) nie są obowiązkowe, lecz zdecydowanie pomogą w szacowaniu ryzyka i wykazywaniu zgodności*[226]. Oczywiście można stworzyć wiele różnych narzędzi, należy jednak pamiętać, że podstawowe narzędzia przewidział prawodawca w RODO, są to:

– *rejestr czynności przetwarzania danych osobowych* (art. 30 ust. 1 RODO),
– dokumenty związane z oceną ryzyka (art. 32 ust. 1 RODO w zw. z art. 32 ust. 2 RODO w zw. z art. 5 RODO).
– *ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1* (art. 30 ust. 1 lit. g RODO).

Podkreślenia wymaga, że to o czym pisze P. Siembida – administrator danych osobowych może zrobić, to o czym pisze prawodawca – administrator danych osobowych uczynić ma obowiązek.

3.11 Art. 32 ust. 1 i 2 i 3 Uwaga 11

Kolejność czynności

Czynności wykonywane w celu realizacji obowiązków wynikających z art. 32 ust. 1 i ust. 2 RODO powinny być wykonywane odpowiednio przez administratora lub przez podmiot przetwarzający we wskazanej poniżej kolejności.

1. Ustalenie listy czynności.
2. Udokumentowanie ustalenia listy czynności, czyli sporządzenie rejestru czynności przetwarzania danych osobowych, za które odpowiada administrator lub odpowiednio rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, który prowadzi podmiot przetwarzający
3. Wykonanie oceny, *czy stopień bezpieczeństwa jest odpowiedni*. Ocenę tę należy wykonać z uwzględnieniem czynników wymienionych w art. 32 ust. 2 RODO.
4. Udokumentowanie wykonania tej oceny.

---

[225] J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja… op.cit.*

[226] P. Siembida, op.cit., s. 136.

5. Dokonanie oceny ryzyka *naruszenia praw lub wolności osób fizycznych*. Należy brać pod uwagę (różne) prawdopodobieństwo realizacji ryzyka i jego wagę.
6. Udokumentowanie wykonania tej oceny.
7. Wdrożenie środków technicznych i organizacyjnych.
8. Udokumentowanie wykonania tego wdrożenia.
9. Sporządzenie ogólnego opisu *technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1* RODO.

Czynności wykonywane w celu realizacji obowiązków wynikających z art. 32 ust. 1 i ust. 2 RODO mogą być wykonywane w sposób wskazany powyżej, wydaje się jednak, że właściwsza jest kolejność oparta na innym modelu oceniania ryzyka. Odnoszę się tu do modelu, w którym ryzyko składa się z czynników wymienionych w art. 32 ust. 2 RODO i z naruszenia praw i wolności zapisanych w art. 5 ust. 1 RODO. Jeżeli przyjmiemy taki model – a taki właśnie uważam za właściwy – to czynności oceny ryzyka powinny być wykonywane odpowiednio przez administratora lub przez podmiot przetwarzający we wskazanej poniżej kolejności. Dla porządku i odróżnienia, czynności numeruję dodając wyróżnik literowy.

1a. Ustalenie listy czynności.
2a. Udokumentowanie ustalenia listy czynności, czyli sporządzenie rejestru czynności przetwarzania danych osobowych, za które odpowiada administrator lub odpowiednio rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, który prowadzi podmiot przetwarzający
3a. Wykonanie oceny ryzyka, czy stopień bezpieczeństwa jest odpowiedni i jakie prawa i wolności mogą zostać naruszone, jeżeli zrealizuje się ryzyko odpowiednie do kolejnych czynności.
4a. Udokumentowanie wykonania tej oceny.
5a. Wdrożenie środków technicznych i organizacyjnych.
6a. Udokumentowanie wykonania tego wdrożenia.
7a. Sporządzenie ogólnego opisu *technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1* RODO.

Zwracam uwagę, że w drugiej wersji opisu kolejnych czynności jedynie pozornie pomijam pewne elementy. Czynności jest mniej w sensie rachunkowym, ale dlatego, że czynności 3 i 5 z pierwotnej

listy zostały połączone w czynności 3a z drugiej listy. Druga z proponowanych list czynności związanych z oceną ryzyka jest wynikiem rozumowania, w którym na ryzyko składa się zdarzenie, czy też precyzyjniej – prawdopodobieństwo zdarzenia i skutek tego zdarzenia, czyli naruszenie konkretnych praw i wolności. Szersze rozważania prowadzę wyżej w uwadze (*3.30. Art. 24. Uwaga 29 Ryzyko. Pojęcie na gruncie art. 32*). Takie podejście do ryzyka jest zgodne z zaprezentowaną przez A. Krasuskiego definicją, w której: *ryzyko jest to iloczyn prawdopodobieństwa poniesienia straty i jej wielkości. Ryzyko = (szansa zaistnienia, czyli prawdopodobieństwo) × (konsekwencje – czyli strata)*[227] . Andrzej Krasuski powołuje się również na dokument oficjalny, w którym czytamy, że *„Ryzyko" jest scenariuszem opisującym zdarzenie i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa ryzyka*[228]. Zarówno jednak u A. Krasuskiego, jak i we wskazanym dokumencie oficjalnym brak mi odesłania do oczywistych w świetle tego rozumowania, elementów wskazanych w art. 32 RODO, czyli do zdarzeń o charakterze zagrożenia wskazanych w art. 32 ust. 2 RODO i do praw i wolności wskazanych w art. 32 ust. 1 RODO.

Wskazane powyżej wyliczenie kolejnych czynności związanych z art. 32 RODO nie jest niestety ostateczne. Należy pamiętać o pewnych zjawiskach.

– Wdrożenie środków technicznych i organizacyjnych modyfikuje ryzyko. Zarówno ryzyko techniczne, jak i ryzyko naruszenia praw i wolności osób fizycznych.
– Wprowadzenie nowych czynności modyfikuje ryzyko.
– Upływ czasu modyfikuje ryzyko.

Z uwagi na fakt, że wdrożenie środków technicznych i organizacyjnych modyfikuje ryzyko, po wdrożeniu środków należałoby wykonać powtórnie czynności poniższe.

---

[227] A. Krasuski, op. cit., s. 34. Andrzej Krasuski odwołuje się w przypisie do wcześniejszej publikacji, a to do: Terelak‑Tymczyna A., *Zarządzanie bezpieczeństwem*, Szczecin 2014, jednak bez wskazania numeru strony tejże.

[228] *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679*. Przyjęte w dniu 4 kwietnia 2017 r. Ostatnio zmienione i przyjęte w dniu 4 października 2017 r. Grupa Robocza Art. 29. 17/PL WP 248 rev.01, s. 7.

3. Wykonanie oceny, *czy stopień bezpieczeństwa jest odpowiedni*. Ocenę te należy wykonać z uwzględnieniem czynników wymienionych w art. 32 ust. 2 RODO.
4. Udokumentowanie wykonania tej oceny.
5. Dokonanie oceny ryzyka *naruszenia praw lub wolności osób fizycznych*. Należy brać pod uwagę (różne) prawdopodobieństwo realizacji ryzyka i jego wagę.
6. Udokumentowanie wykonania tej oceny.

Z uwagi na fakt, że wprowadzenie nowych czynności modyfikuje ryzyko, po wprowadzeniu nowej czynności powinny być powtórnie wykonane wszystkie czynności, w tym – jak zalecam tuż powyżej – czynności 3–4–5–6 powinny być wykonane dwukrotnie.

Z uwagi na fakt, że upływ czasu modyfikuje ryzyko, wszystkie czynności powinny być powtarzane. Jeżeli czas płynie, a nie pojawiają się nowe czynności, to powtarzane powinny być czynności 3–4–5–6 i ewentualnie, zależnie od wyniku oceny, jeśli pojawi się konieczność wprowadzenia nowych środków, powtarzane powinny być czynności 7–8–9.

Odpowiednio do prezentowanego wyżej drugiego ze stanowisk na temat oceny ryzyka, czynności, które należy powtarzać to czynności 3a i 4a, czyli czynności wskazane poniżej.

3a. Wykonanie oceny ryzyka, czy stopień bezpieczeństwa jest odpowiedni i jakie prawa i wolności mogą zostać naruszone, jeżeli zrealizuje się ryzyko odpowiednie do kolejnych czynności.
4a. Udokumentowanie wykonania tej oceny.

Jeśli chodzi o częstotliwość powtarzania czynności, to podkreślam, że pomijam tu przepisy krajowe, które nakładają w Polsce na przykład na podmioty publiczne obowiązek powtarzania ocen ryzyka. Jeśli zatem chodzi o częstotliwość powtarzania czynności, wynikającą z samego upływu czasu, to trudno wskazać, jaka ona powinna być. Wydaje się to zależne od ryzyka, od skali przetwarzania, od wielkości podmiotu itd. Przyjmowane czasem, choć nie prowadzę badań ilościowych, powtarzanie ocen raz do roku, może się okazać zbyt częste, jak i zbyt rzadkie.

Ciekawą wypowiedź, ciekawą, choć nie do końca w sprawie tu poruszanej, jednak z nią związaną, napotykamy u P. Barty, M. Kaweckiego i P. Litwińskiego. Autorzy ci piszą, że: *ustawodawca unijny wymaga regularnego testowania, mierzenia i oceniania skuteczności*

zastosowanych środków dla zapewnienia bezpieczeństwa w stopniu odpowiadającym ryzyku[229]. Uważam że wypowiedź ta ma charakter nieco życzeniowy, trudno jest mi bowiem znaleźć dla niej bezpośrednie uzasadnienie w przepisach. Wskazani autorzy też go nie podają, być może z uwagi na oszczędność miejsca w publikacji. Wypowiedź ta jest jednak cenna. Wskazani autorzy zwracają uwagę na to, że środki wdrożone przez administratora lub podmiot przetwarzający powinny odpowiadać ryzyku w sposób, który możemy nazwać ciągłym. Wypowiedź tę cytuję, ponieważ w niej dostrzegam pewną wskazówkę co do tego, jak często należy powtarzać ocenę ryzyka, o której tu piszę. Otóż ocenę tę należy powtarzać na tyle często by stosowane przez administratora środki były odpowiednie do ryzyka. Bardzo nie lubię wypowiedzi, w których wypowiadający czyni tak zwany unik i za pomocą chwytu oratorskiego w istocie omija problem, miast go rozwiązać. Mam świadomość, że nie udzielam tu, być może pożądanej przez czytelnika odpowiedzi na pytanie o to, jak często powtarzać ocenę ryzyka. W sposób uczciwy mogę odpowiedzi udzielić tylko jednej, a mianowicie, że ocenę taką należy powtarzać na tyle często, by – jak piszę wyżej – środki wdrożone przez administratora lub podmiot przetwarzający, były odpowiednie do ryzyka.

Ciekawą i bliską mi wypowiedź znajdziemy w czeskim komentarzu[230], czytamy tam bowiem, o tym, że jeżeli ryzyko ulega zmianie, to administrator powinien „zrewidować" zabezpieczenia i wprowadzić takie, które są odpowiednie do nowego poziomu ryzyka.

Przemysław Siembida w swojej publikacji opisuje kilka różnych metodyk oceny ryzyka. Czyni to w rozdziale IV książki napisanej wspólnie z A. Krasuskim[231]. Nie zamierzam tutaj wdawać się w polemikę, czy nawet dyskusję z konkretnymi zaleceniami konkretnych organów i podmiotów, dotyczącymi tego, jak oceny ryzyka czynić należy. Nie jest to celem niniejszej publikacji, poza tym – choć z uwagi na autorytet, zwłaszcza zagranicznych organów – mogę założyć, że metody te swój sens mają. Mają też jednak niestety jedną wspólną cechę, są one niezwykle skomplikowane. Skomplikowanie metod może zniechęcać administratorów do ich stosowania, a przy nieznajomości in-

[229] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 345.

[230] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit., s. 291.

[231] P Siembida, op. cit., s. 131–223.

nych metod – może zniechęcać do stosowania jakichkolwiek. Mnie metody skomplikowane zniechęcają. W ich miejsce, jak uważam, należy stosować metodę opartą na RODO. Co więcej, jeżeli nawet administrator danych osobowych nauczy się którejś z wymyślnych metod przedstawionych przez P. Siembidę, to nie wolno mu zapominać, że ma on obowiązek wykorzystać w tej metodzie listę zdarzeń z art. 32 ust. 2 RODO oraz listę praw i wolności, które związane są z zasadami z art. 5 RODO. Ma obowiązek to zrobić, ponieważ przepisy nie mają charakteru metaforycznego, przepisy ustanawiają obowiązki, uprawnienia i wolności. O tym zapominać nie wolno i nie należy.

3.12. Art. 32 Uwaga 12

Charakter, zakres, kontekst i cele przetwarzania

Uwaga o tym samym tytule zamieszczona jest wyżej, w odniesieniu do art. 24 ust. 1 RODO. Wyżej prowadzę też w osobnych uwagach, rozważania dotyczące kolejnych pojęć:

– charakteru przetwarzania (*3.10. Art. 24. Uwaga 10. Charakter przetwarzania*),
– zakresu przetwarzania (*3.8. Art. 24 Uwaga 8. Zakres*),
– kontekstu przetwarzania (*3.11. Art. 24. Uwaga 11. Kontekst przetwarzania*),
– celów przetwarzania (*3.9. Art. 24. Uwaga 9. Cele przetwarzania*).

Nie od rzeczy jest stwierdzić, że tak naprawdę, nie wiadomo, jakie znaczenia prawodawca zakodował pod poszczególnymi pojęciami. Wyjątkiem jest (może!) cel przetwarzania. Cele przetwarzania zapisywane są w rejestrze czynności przetwarzania danych osobowych, za które odpowiada administrator, prowadzonym na podstawie art. 30 ust. 1 RODO. Jeżeli nawet administrator jest zwolniony z obowiązku prowadzenia wskazanego rejestru, to z dużą dozą pewności można uznać, że wiadomo, czym są cele przetwarzania, czym są pozostałe, wymienione tu cechy przetwarzania – nie wiadomo.

W rozdziale poświęconym art. 24 RODO analizuję wskazane pojęcia szczegółowo, nie ma sensu rozważań tych tu powtarzać. Niżej zamieszczam kilka uwag, które mogą być pewnym ich uzupełnieniem.

– Należy uznać, że charakter przetwarzania, zakres przetwarzania, kontekst przetwarzania i cele przetwarzania, o których mowa w art. 24 ust. 1 RODO, to te same, o których mowa w art. 32 ust. 2 RODO.

Przemawia za tym treść obydwu przepisów oraz (bo myślę, że można tu kwestie te rozdzielać) zakaz wykładni synonimicznej[232].

– Nie ma jasności co do znaczeń poszczególnych wskazanych pojęć, nie ma również zgody przedstawicieli doktryny w tej kwestii. Jednocześnie nie sposób zignorować faktu, że zarówno w art. 24 ust. 1 RODO jak i w art. 32 ust. 2 RODO pojęcia te występują.
– Z uwagi na obecność pojęć w obu wskazanych przepisach należy pojęcia te rzeczywiście „uwzględniać" przy wykonywaniu oceny ryzyka. Wydaje się, że należy po prostu, przy wykonywaniu oceny ryzyka, dokładnie scharakteryzować czynności będące jej podstawą.

Nie jestem zwolennikiem powtarzania cudzych myśli, czasem jednak, z uwagi na ich wartość – warto. Warto zwłaszcza, kiedyś myśl taka jest umysłowo zapładniająca, pozwala przyjąć pogląd za swój i rozwinąć go. Myśl taką wyraża K. Wygoda, który pisze, że art. 32 RODO jest odejściem *od dotychczasowego statycznego, formalnego i „de facto" reaktywnego modelu ochrony danych na rzecz podejścia opartego na modelu ochrony proaktywnej, prewencyjnej, o zindywidualizowanym charakterze […]*[233]. Zgadzam się z K. Wygodą, pozwolę sobie jednak na pewne uzupełnienie. Otóż mówiąc prościej, RODO nakazuje przewidywać zagrożenia, przygotowywać się do nich. Podejście takie może wydawać się niepoważne, przewidywanie przyszłości, zwłaszcza trafne, nie jest bowiem niczym łatwym ani pewnym. To prawda. RODO nie nakazuje jednak, wbrew pozorom przewidywać przyszłości. RODO nakazuje oceniać okoliczności przez pryzmat parametrów w RODO wskazanych. Różnica jest trudno uchwytna, sam walczę z pokusą, by napisać, że „czyli jednak RODO nakazuje przewidywać przyszłość". RODO nie nakazuje przewidywać przyszłości, a jedynie oceniać okoliczności.

Administrator realizujący art. 32 ust. 2 RODO bada, czy w momencie badania zachodzi:

– ryzyko wynikające z przypadkowego zniszczenia danych osobowych przechowywanych,

---

[232] L. Morawski, op. cit., s. 103.

[233] K. Wygoda, [w:] M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO?...*, s. 354.

– ryzyko wynikające z niezgodnej z prawem modyfikacji danych osobowych przesyłanych itd. (Podkreślam, że wskazuję tu dwa przykładowe ryzyka, z wielu, które administrator ma obowiązek brać pod uwagę.

Następnie administrator bada, czy w momencie badania zachodzi:
– ryzyko naruszenia praw i wolności.

Po wykonaniu wskazanych wyżej badań, czyli wykonaniu oceny ryzyka, administrator – jeżeli to konieczne – wdraża odpowiednie środki techniczne i organizacyjne. Podkreślenia wymaga, że administrator nie ocenia tego, co może się wydarzyć w przyszłości. Administrator ocenia, co może się wydarzyć „teraz", „właśnie", w momencie dokonywania oceny. Należy unikać tworzenia wyimaginowanych scenariuszy, w których prawa i wolności grają role główne, a zalania, pożary, włamania i gradobicia grają role drugoplanowe i pełnią rolę budzących grozę dekoracji. Prowadzone tu rozważania są aktualne, w zakresie wykonywania oceny ryzyka, również w odniesieniu do podmiotu przetwarzającego. Działania administratora lub podmiotu przetwarzającego są odpowiednikiem środków zaradczych, mających na celu zmniejszenie ryzyka, o których pisze A. Krasuski[234].

3.13. Art. 32 Uwaga 13

Niski poziom ryzyka jako pożądany

Wyżej w (*1.1. Art. 32 ust. 1. Analiza*). Zastanawiam się nad pożądanym stopniem bezpieczeństwa. Prawodawca wskazuje w przepisie, że stopień bezpieczeństwa powinien odpowiadać ryzyku. Odsyłam do odpowiedniego fragmentu analizy, którą kończę konstatacją, że stopień bezpieczeństwa, który ma być uzyskany po ocenie ryzyka i po zastosowaniu środków technicznych, powinien być niski. Nad tym się właśnie chwilę pragnę zatrzymać. Dlaczego niski? Trzeba przeprowadzić pewne rozumowanie. W niniejszej książce zajmuję się art. 24 RODO, 32 RODO, 33 RODO i 34 RODO RODO. W każdym z tych przepisów istotną rolę pełni poziom ryzyka naruszenia praw i wolności. Nie

[234] A. Krasuski, op. cit., s. 33. W przypisie A. Krasuski odwołuje się do wcześniejszej publikacji: Kokot‑Stępień P., *Identyfikacja ryzyka jako kluczowy element zarządzania ryzykiem w przedsiębiorstwie*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" nr 855, „Finanse, Rynki Finansowe, Ubezpieczenia" 2015/74, t. 1, s. 533.

wyjaśniam szerzej, dlaczego – jest temu poświęcona znaczna część niniejszej książki. Najkrócej patrząc, administrator przewiduje ryzyko i wprowadza środki, by to ryzyko obniżyć. Do jakiego poziomu?

Zwracam uwagę, że jeżeli zajdzie naruszenie ochrony danych osobowych, to tylko niski poziom ryzyka naruszenia praw i wolności osób fizycznych zwalnia administratora z obowiązku zgłoszenia naruszenia ochrony danych osobowych do PUODO. Gdyby zatem administrator przetwarzał dane, akceptując przy tym poziom ryzyka wyższy niż niski, to tym samym administrator prawdopodobnie pozostawałby cały czas w warunkach naruszenia ochrony danych osobowych, a przynajmniej w stanie analogicznym do naruszenia ochrony danych osobowych. Raczej analogicznym, ponieważ dla zaistnienia naruszenia konieczne jest zdarzenie, które jest w art. 4 pkt 12 RODO nazwane „naruszeniem bezpieczeństwa". (Do tego dochodzą jeszcze dwie grupy warunków koniecznych.)

Gdyby administrator dopuszczał przetwarzanie danych przy poziomie ryzyka innym niż niski, to trudno byłoby powiedzieć, kiedy zaistniało naruszenie. Może nie każde działanie administratora mogłoby być kwalifikowane jako naruszenie, ale na pewno wiele. Głównie, by uniknąć takiej konfuzji, uważam, że jedyny poziom ryzyka naruszenia praw i wolności osób, których dane dotyczą, który jest do zaakceptowania przez administratora to poziom niski. Jednocześnie należy uczciwie przyznać, że decyzja o tym, jaki poziom ryzyka jest poziomem akceptowalnym, jest decyzją administratora, na co – jak się wydaje – uwagę zwracają M. Gumularz i T. Izydorczyk[235].

4. Art. 32 ust. 1 i 2 i 3 Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Uważam, że wskazane niżej uprawnienia mają charakter pierwotny w stosunku do odpowiadających im wskazanych niżej obowiązków. Uważam tak, ponieważ jeżeli administrator nie dysponuje danymi osobowymi, to teoretycznie jest administratorem, decyduje bowiem o celach i sposobach przetwarzania danych, jednak jest nim tylko teoretycznie, rzekłbym „in books". Kiedy przyglądamy się zarysowanej sytuacji, to okazuje się, że administrator, który nie dysponuje

[235] M. Gumularz, T. Izydorczyk, op. cit., s. 21.

danymi osobowymi, nie ma czego chronić. Skoro administrator nie ma czego chronić, to trudno powiedzieć, że w sensie funkcjonalnym, rzekłbym „in action", spoczywają na nim obowiązki w zakresie ochrony danych.

Można oczywiście wywodzić, że administrator realizuje obowiązki w zakresie ochrony danych w przewidywaniu uzyskania danych. To ma sens i – co więcej – modelowo tak się to odbywa, administrator nie ma danych, ocenia ryzyko, wdraża środki. Ma to sens jako pewien model, jeżeli jednak model ten uzupełnimy o fakt, że dany administrator nigdy żadnych danych nie przetworzy, to obowiązki administratora znowu stają się iluzoryczne. (Możemy też sporadycznie mieć do czynienia z sytuacją, w której administrator zlecił podmiotom przetwarzającym przetwarzanie wszystkich danych, które przetwarzałby sam, gdyby tego nie zlecił, sytuacja taka jest możliwa, tu ją jednak pomijam. Administrator nie przetwarza danych w sensie faktycznym, wszystkie dane, wobec których jest administratorem, są przetwarzane przez podmioty przetwarzające i w związku z tym, te właśnie podmioty przeprowadzają oceny ryzyka.)

Z uwagi na opisane wyżej zjawisko, uważam, co zasygnalizowałem, że uprawnienia są pierwotne wobec obowiązków. Chronologicznie pojawiają się one niemal jednocześnie lub jednocześnie, jednak rzecz można wyjaśnić tak, że administrator, który nie ma danych, nie ma również obowiązków (pozornie ma, ale w istocie nie ma – rzecz wykładam wyżej). Wraz z pojawieniem się danych osobowych pojawiają się obowiązki, jednak ich pojawienie się jest niejako zainicjowane przez pojawienie się uprawnień. Piszę, że uprawnienia i obowiązki pojawiają się niemal jednocześnie. Dlaczego „niemal jednocześnie", a nie jednocześnie. Otóż dlatego, że obowiązek pojawia się po stronie administratora dopiero, kiedy pojawią się tam dane. Dane zrazu nie znajdują się we władaniu administratora. Administrator nie ma danych, więc nie ma i obowiązku. Dane znajdują się wtedy zwykle we władaniu osoby, której dane dotyczą. Osoba, której dane dotyczą, dostarcza dane i niejako przynosi swoje uprawnienie ze sobą i w tej sytuacji po stronie administratora pojawia się obowiązek. Możliwa jest też sytuacja, w której administrator pozyskuje dane nie od osoby, której dane dotyczą, ale od kogoś innego. W takiej sytuacji również dopiero kiedy administrator pozyska dane, po jego stronie pojawi się obowiązek. Możliwa jest sytuacja, że obowiązek pojawi się równo-

cześnie z uprawnieniem. Ma to miejsce na przykład w nieczęstej, ale jednak spotykanej sytuacji, kiedy administrator wytwarza dane osobowe. Wytworzenie danych osobowych zachodzi, np. kiedy administrator bada próbkę płynu ustrojowego czy jakąś inną próbkę ludzkiego materiału biologicznego. Administrator otrzymuje np. krew. Administrator bada tę krew i uzyskuje informacje dotyczące jej parametrów. Informacje te mają charakter danych osobowych. W ten sposób administrator wytwarza dane osobowe. Wydaje się, że właśnie w takiej sytuacji obowiązek pojawia się jednocześnie z uprawnieniem.

Obowiązki i prawa prezentuję poniżej nieco inaczej, niż czynię to wyżej w odniesieniu do art. 24 RODO. Wyżej prezentuję je rozdzielone na obowiązki i prawa, tu prezentuję je w zestawieniach zawierających prawo i odpowiadający mu obowiązek. Powody są dwa. Mniej istotny – pozwala mi to uniknąć powtarzania niektórych części wspólnych wywodu. Bardziej istotny – metoda tu prezentowana, która polega niejako na przetłumaczeniu przepisów na język, na siatkę pojęciową praw (uprawnień) i obowiązków jest (przynajmniej stosowana z tą intensywnością) moim rozwiązaniem autorskim. Podobnie Konceptualizm Prawniczy – Ogólna Teoria Prawa, na bazie której tę metodę prezentacji stworzyłem, a na pewno dopracowałem, jest moją teorią autorską. Różne sposoby prezentacji wniosków pozwalają na pełniejsze zaprezentowanie teorii i metody.

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

Artykuł 32 RODO **ustanawia obowiązki**, które spoczywają na administratorze i na podmiocie przetwarzającym oraz **uprawnienia**, które przysługują osobom, których dane dotyczą, obowiązki te i uprawnienia są wskazane poniżej.

Administrator (podmiot przetwarzający) ma obowiązek uwzględnić okoliczności wskazane w przepisie i dokonać odpowiedniego do tego wdrożenia.

Osoba, której dane dotyczą, ma prawo do tego, by okoliczności wskazane w przepisie zostały uwzględnione przez administratora (podmiot przetwarzający) przy okazji wdrożenia, o którym mowa w przepisie.

Administrator (podmiot przetwarzający) ma obowiązek uwzględnić stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania.

Osoba, której dane dotyczą, ma prawo do tego, by stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania zostały uwzględnione przez administratora (podmiot przetwarzający) przy okazji wdrożenia, o którym mowa w przepisie.

Administrator (podmiot przetwarzający) ma obowiązek uwzględnić ryzyko naruszenia praw i[236] wolności osób fizycznych przy dokonywaniu wdrożenia.

Osoba, której dane dotyczą, ma prawo do tego, by ryzyko naruszenia praw i wolności osób fizycznych zostały uwzględnione przez administratora (podmiot przetwarzający) przy okazji wdrożenia, o którym mowa w przepisie.

Administrator (podmiot przetwarzający) ma obowiązek uwzględnić trzy grupy okoliczności przy dokonywaniu wdrożenia.

Osoba, której dane dotyczą, ma prawo do tego, by trzy grupy okoliczności zostały uwzględnione przez administratora przy okazji wdrożenia, o którym mowa w przepisie.

– Pierwsza grupa okoliczności, których wzięcie przez administratora (podmiot przetwarzający) pod uwagę jest jego obowiązkiem i jednocześnie prawem osoby, której dane dotyczą, to *stan wiedzy technicznej, koszt wdrażania.*
– Druga grupa okoliczności, których wzięcie przez administratora (podmiot przetwarzający) pod uwagę jest jego obowiązkiem i jednocześnie prawem osoby, której dane dotyczą, to *charakter, zakres, kontekst i cele przetwarzania.*
– Trzecia grupa okoliczności, których wzięcie przez administratora (podmiot przetwarzający) pod uwagę jest jego obowiązkiem i jednocześnie prawem osoby, której dane dotyczą, to *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.*

Administrator (podmiot przetwarzający) ma obowiązek dokonać wdrożenia, o którym mowa w przepisie i jednoczesny obowiązek uwzględnienia przy dokonywaniu wdrożenia, okoliczności wskazanych w przepisie.

Osoba, której dane dotyczą, ma prawo by administrator (podmiot przetwarzający) zrealizował obowiązek dokonania wdrożenia, o którym mowa w przepisie i by zrealizował jednoczesny obowiązek uw-

[236] (sic!)

zględnienia przy dokonywaniu wdrożenia, okoliczności wskazanych w przepisie.

Administrator (podmiot przetwarzający) ma obowiązek wdrożyć środki techniczne i organizacyjne.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) wdrożył środki techniczne i organizacyjne.

Administrator (podmiot przetwarzający) ma obowiązek zadbać o to, by środki techniczne i organizacyjne, które wdroży, były odpowiednie (do okoliczności, które administrator ma obowiązek wziąć pod uwagę).

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) wdrożył środki techniczne i organizacyjne, które są odpowiednie (do okoliczności, które administrator ma obowiązek wziąć pod uwagę).

Administrator (podmiot przetwarzający) ma obowiązek pamiętać o tym, że wdrożenie, którego dokonuje, ma cel, który jest wskazany w przepisie.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) dokonywał wdrożenia ze świadomością, że ma ono cel, który jest wskazany w przepisie.

Administrator (podmiot przetwarzający) ma obowiązek dokonać wdrożenia, aby zapewnić stopień bezpieczeństwa, o którym mowa w przepisie.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) dokonywał wdrożenia w celu zapewnienia stopnia bezpieczeństwa wskazanego w przepisie

Administrator (podmiot przetwarzający) ma obowiązek zadbać o to, by (dzięki wdrożeniu dokonanemu po wykonaniu oceny ryzyka) stopień bezpieczeństwa danych osobowych odpowiadał ocenionemu ryzyku.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) zadbał o to, by – dzięki wdrożeniu dokonanemu po wykonaniu oceny ryzyka – stopień bezpieczeństwa danych osobowych odpowiadał ocenionemu ryzyku.

Słowa „w tym między innymi" wskazujące na wymienione dalej środki organizacyjne i techniczne mogą skutkować wnioskiem, że środki te administrator ma obowiązek wdrożyć. Wniosek ten byłby jednak przedwczesny, z uwagi na następujące po tych słowach „słowa w stosownym przypadku". Z użycia słów „w tym między innymi

w stosownym przypadku" nie wynika zatem dla administratora żaden realny obowiązek w zakresie wdrożenia wskazanych w przepisie środków. Z jedną jednak uwagą, otóż jeżeli któryś ze środków technicznych i organizacyjnych jest odpowiedni, to administrator ma obowiązek go wdrożyć.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) wdrożył te ze środków technicznych i organizacyjnych, wymienionych w przepisie, które są odpowiednie, przy czym wdrożenie żadnego ze wskazanych w przepisie środków nie jest obowiązkowe, z tym oczywiście zastrzeżeniem, że staje się obowiązkowe, kiedy środek jest odpowiedni.

Obecność w przepisie słów: „w tym między innymi w stosownym przypadku" jako wstępu do wymienionych dalej w przepisie środków technicznych i organizacyjnych, służących zabezpieczeniu danych osobowych, skutkuje po stronie administratora i osób, których dane dotyczą, w sposób wskazany poniżej.

Administrator (podmiot przetwarzający) nie ma obowiązku stosowania wszystkich wymienionych w przepisie środków ani nawet któregokolwiek, z tym jednak zastrzeżeniem, że jeżeli w wyniku oceny ryzyka okaże się, że któryś ze środków jest odpowiedni, to wtedy ze słów „w stosownym przypadku", wynika obowiązek zastosowania tego środka.

Uprawnione jest tu twierdzenie, że wskazany przepis ustanawia po stronie administratora (podmiotu przetwarzającego) obowiązek, jednak jest to obowiązek warunkowy, czy też inaczej, obowiązek pod warunkiem zawieszającym. Jeżeli ten warunek się zrealizuje, czyli jeżeli z oceny ryzyka wyniknie, że dany środek jest odpowiedni, to wtedy warunek zawieszający zostaje zrealizowany i obowiązek po prostu funkcjonuje.

Osoba, której dane dotyczą, nie ma prawa do oczekiwania, by administrator (podmiot przetwarzający) stosował wszystkie wymienione w przepisie środki ani nawet by stosował którykolwiek, z tym jednak zastrzeżeniem, że jeżeli w wyniku oceny ryzyka okaże się, że któryś ze środków jest odpowiedni, to wtedy ze słów „w stosownym przypadku", wynika uprawnienie do oczekiwania, by administrator zastosował ten środek.

Uprawnione jest tu twierdzenie, że wskazany przepis ustanawia po stronie osoby, której dane dotyczą uprawnienie (prawo), jednak

jest to uprawnienie warunkowe, czy też inaczej, uprawnienie pod warunkiem zawieszającym. Jeżeli ten warunek się zrealizuje, czyli jeżeli z oceny ryzyka wyniknie, że dany środek jest odpowiedni, to wtedy warunek zawieszający zostaje zrealizowany i uprawnienia po prostu przysługuje (osobie, której dane dotyczą).

Administrator (podmiot przetwarzający) przy dokonywaniu wdrożenia ma obowiązek wdrożyć te z wymienionych niżej środków technicznych i organizacyjnych, które są odpowiednie do stopnia bezpieczeństwa wynikającego z oceny ryzyka. Jednocześnie zastosowanie żadnego ze wskazanych środków nie jest poza tym obowiązkowe.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) dokonując wdrożenia, wdrażał w celu zapewnienia stopnia bezpieczeństwa wskazanego w przepisie te z wymienionych niżej środków technicznych i organizacyjnych, które są odpowiednie do stopnia bezpieczeństwa wynikającego z oceny ryzyka. Jednocześnie zastosowanie żadnego ze wskazanych środków nie jest poza tym obowiązkowe.

– pseudonimizacja i szyfrowanie danych osobowych;
– zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
– zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
– regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Obecność w przepisie pogrubionych słów: ***Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem****, w szczególności wynikające z* jako wstępu do wymienionych dalej w przepisie ryzyk dla przetwarzania danych osobowych, skutkuje po stronie administratora i osób, których dane dotyczą, w sposób wskazany poniżej.

Administrator (podmiot przetwarzający) przy dokonywaniu oceny, czy stopień bezpieczeństwa przetwarzania danych osobowych jest odpowiedni, ma obowiązek uwzględnienia zwłaszcza ryzyka, które wiąże się z przetwarzaniem danych osobowych. Trudno powiedzieć, jakie jeszcze inne ryzyka, niż wiążące się z przetwarzaniem

danych osobowych, administrator miałby brać pod uwagę. Nie można wykluczyć, że inne, hipotetyczne ryzyka, do których w jakimś sensie odnosi się przepis, to ryzyka naruszenia RODO, na przykład przy realizacji uprawnień osób, których dane dotyczą (prawo do bycia zapomnianym itd.) Tak czy inaczej, nie ma wątpliwości, że ryzyka wiążące się z przetwarzaniem danych osobowych, administrator (podmiot przetwarzający) ma obowiązek wziąć pod uwagę.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) przy dokonywaniu oceny, czy stopień bezpieczeństwa przetwarzania danych osobowych jest odpowiedni, uwzględnił zwłaszcza ryzyka, które wiąże się z przetwarzaniem danych osobowych.

Obecność w przepisie pogrubionych słów: ***Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko*** *wiążące się z przetwarzaniem,* ***w szczególności wynikające z*** jako wstępu do wymienionych dalej w przepisie ryzyk dla przetwarzania danych osobowych, skutkuje po stronie administratora i osób, których dane dotyczą, w sposób wskazany poniżej.

Administrator (podmiot przetwarzający) przy dokonywaniu oceny, czy stopień bezpieczeństwa przetwarzania danych osobowych jest odpowiedni, ma obowiązek uwzględnienia zwłaszcza ryzyka wynikającego z okoliczności wskazanych dalej w przepisie.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) przy dokonywaniu oceny, czy stopień bezpieczeństwa przetwarzania danych osobowych jest odpowiedni, uwzględnił zwłaszcza ryzyka, wynikające z okoliczności wskazanych dalej w przepisie. Podkreślić należy, że uwzględnienie tych okoliczności (ryzyk) przez administratora jest tyleż obowiązkiem administratora (podmiotu przetwarzającego) co uprawnieniem (prawem) osoby, której dane dotyczą.

Administrator (podmiot przetwarzający) ma obowiązek przy ocenianiu ryzyka uwzględnić wszystkie okoliczności zdarzenia mającego charakter ryzyka, wymienione w przepisie, a mianowicie:

– przypadkowość,
– niezgodność z prawem,
– przypadkowość i niezgodność z prawem zachodzące jednocześnie.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) przy ocenianiu ryzyka uwzględnił wszystkie okoliczności zdarzenia mającego charakter ryzyka, wymienione w przepisie, a mianowicie:
– przypadkowość,
– niezgodność z prawem,
– przypadkowość i niezgodność z prawem zachodzące jednocześnie.

Administrator (podmiot przetwarzający) ma obowiązek przy ocenianiu ryzyka uwzględnić wszystkie rodzaje zdarzenia dotyczącego danych osobowych, mającego charakter ryzyka, wymienione w przepisie, a mianowicie:
– zniszczenie,
– utratę,
– modyfikację,
– nieuprawnione ujawnienie,
– nieuprawniony dostęp.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) przy ocenianiu ryzyka uwzględnił wszystkie rodzaje zdarzenia mającego charakter ryzyka, wymienione w przepisie, a mianowicie:
– zniszczenie,
– utratę,
– modyfikację,
– nieuprawnione ujawnienie,
– nieuprawniony dostęp.

Administrator (podmiot przetwarzający) ma obowiązek przy ocenianiu ryzyka uwzględnić wszystkie kategorie czynności na danych osobowych wymienione w przepisie. Są to:
– przesyłanie,
– przechowywanie,
– przetwarzanie w inny sposób niż przez przesyłanie lub przechowanie.

Osoba, której dane dotyczą, ma prawo, by administrator (podmiot przetwarzający) przy ocenianiu ryzyka uwzględnił wszystkie kategorie czynności na danych osobowych wymienione w przepisie. Są to:
– przesyłanie,
– przechowywanie,
– przetwarzanie w inny sposób niż przez przesyłanie lub przechowanie.

5. Art. 32 ust. 1 i 2 i 3 Konkretyzacja zasad

Art. 32 RODO konkretyzuje wymienione poniżej zasady.
Przy omawianiu konkretyzacji zasad korzystam z ustaleń, które poczyniłem dla potrzeb książki *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*[237].

Zasada zgodności z prawem

Przetwarzanie zgodne z zasadą zgodności z prawem to przetwarzanie zgodne z art. 6 RODO i ewentualnie z art. 9 RODO i z art. 10 RODO. Z art. 32 ust. 1 RODO wynika, że administrator ma obowiązek uwzględnić wskazane w przepisie ryzyko, tak by móc uwzględnić *stopień bezpieczeństwa odpowiadający temu ryzyku*. Działanie administratora zgodne z analizowanym przepisem powinno zapobiec przetwarzaniu w sposób nieprzewidziany przez administratora, czyli tym samym nieobjęty niezgodny z art. 6 RODO (i ewentualnie z art. 9 RODO i z art. 10 RODO). Taki właśnie związek art. 32 z zasadą zgodności z prawem, dostrzegam.

Zasada rzetelności

Zasada ta jest realizowana przez realizację obowiązków wynikających odpowiednio z art. 13 RODO i z art. 14 RODO, w zakresie informowania o fakcie przetwarzania i o tym, kto jest administratorem.

Zasada przejrzystości

Zasada ta jest realizowana przez realizację obowiązków wynikających odpowiednio z art. 13 RODO i z art. 14 RODO, w zakresie informowania o szczegółach przetwarzania.

Podobnie jak w odniesieniu do poprzedniej zasady, wykonanie oceny ryzyka powinno zapobiec przetwarzaniu np. przez innego administratora niż administrator przedmiotowy (rzetelność) i w sposób inny niż administrator przedmiotowy (przejrzystość) administrator, który w danej sytuacji zadbał o realizację zasady rzetelności.

Artykuł 32 RODO sprzyja również realizacji zasady rzetelności i zasady przejrzystości. Trzeba przyznać, że wskazany związek zasad

---

[237] J. Rzymowski, *RODO – GDPR. Zasady dotyczące*... Nie zamieszczam przypisu do każdej z zasad we wskazanej książce, bo przypisy te wskazywałyby nieustannie prawie na te same miejsca, co nie ma sensu.

z art. 32 RODO jest pozornie nikły, jednak w istocie, jeśli ocena zostanie wykonana niewłaściwie, jeśli środki techniczne i organizacyjne zostaną wskutek tego niewłaściwie dobrane, to może to łatwo doprowadzić do przetwarzania niezgodnego z każdą z zasad.

Zasada ograniczenia celu

Przetwarzanie danych osobowych zgodne z zasadą ograniczenia celu, to przetwarzanie w taki sposób, że administrator przetwarza dane w celach określonych odpowiednio w rejestrze czynności przetwarzania danych osobowych, oraz na gruncie art. 13 RODO lub 14 RODO lub 15 RODO.

Zasada ograniczenia przechowywania

Przetwarzanie danych osobowych zgodne z zasadą ograniczenia przechowywania oznacza przetwarzanie *danych osobowych przez ograniczony czas*.

Wykonanie oceny ryzyka i dostosowanie środków ochrony danych sprzyja realizacji wskazanych zasad.

Zasada prawidłowości

Zasada prawidłowości danych oznacza również obowiązek podjęcia wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

Związek tej zasady z art. 32 RODO jest dostrzegalny. Czynności walidacji danych, mające na celu realizację zasady prawidłowości, są czynnościami na danych. Jako czynności na danych, czynności te powinny znaleźć się w RCPD. Znalezienie się czynności w RCPD skutkuje koniecznością wykonania wobec niej oceny ryzyka – to właśnie świadczy o związku zasady z art. 32 RODO.

Artykuł 24 RODO sprzyja również realizacji zasady prawidłowości.

Świadczą o tym słowa przepisu: *[...] aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem [...]* Przetwarzanie zgodne z RODO to m. in. przetwarzanie zgodne z zasadą prawidłowości. Przetwarzanie danych osobowych zgodne z zasadą prawidłowości oznacza przetwarzanie *danych osobowych w taki sposób, by były one prawidłowe i w razie potrzeby uaktualniane.*

Zasada minimalizacji danych

Przetwarzanie danych osobowych zgodne z zasadą minimalizacji danych oznacza obowiązek przetwarzania danych osobowych w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane.

Zasada integralności

Przetwarzanie danych osobowych zgodne z zasadą integralności oznacza przetwarzanie *danych osobowych w taki sposób, by modyfikacja danych, w tym zniszczenie lub uszkodzenie, zachodziły jedynie w sposób autoryzowany przez administratora.*

Zasada poufności

Przetwarzanie danych osobowych zgodne z zasadą poufności oznacza przetwarzanie *danych osobowych w taki sposób, by były one ujawniane jedynie uprawnionym podmiotom lub osobom*.

Wymienione trzy zasady zdają się szczególnie być konkretyzowane przez art. 32 RODO. Wykonanie oceny ryzyka i dostosowanie środków technicznych i organizacyjnych jest wręcz przykładową konkretyzacją wskazanych zasad.

Zasada odpowiedzialności administratora danych (osobowych)

Zasada odpowiedzialności administratora oznacza, że administrator ma obowiązek przestrzegać zasad z art. 5 ust. 1 RODO.

Wykonanie oceny ryzyka sprzyja realizacji kolejnych zasad z art. 5 RODO. W mniejszym lub większym stopniu, odpowiednio, ale sprzyja. Skoro wykonanie oceny ryzyka sprzyja realizacji zasad z art. 5 ust. 1 RODO, to tym samym sprzyja realizacji zasady odpowiedzialności administratora, która odnosi się do tych zasad.

Zasada rozliczalności

Zasada rozliczalności oznacza, że administrator ma obowiązek **wykazania przestrzegania zasad wynikających z art. 5 ust. 1 RODO**. Zasady z art. 5 ust. 1 RODO są realizowane przez przepisy szczegółowe RODO, czyli obowiązek wykazania przestrzegania zasada oznacza obowiązek wykazania przestrzegania przepisów szczegółowych RODO.

Wykonanie oceny ryzyka i udokumentowanie wykonania tej oceny sprzyja realizacji zasady rozliczalności w takim zakresie, w ja-

kim wykonanie oceny ryzyka sprzyja realizacji pozostałych zasad z art. 5 ust. 1 RODO.

6. Art. 32 ust. 1 i 2 i 3 Postulaty *de lege ferenda*

6.1. Art. 32 ust. 1 i 2 i 3 Postulat 1

Uproszczenie przepisu

W wersji anglojęzycznej i w wersji czeskojęzycznej prawdopodobieństwo i waga są przymiotami (cechami) ryzyka naruszenia praw i wolności osób fizycznych. W wersji polskojęzycznej prawdopodobieństwo jest przymiotem (cechą) wystąpienia tego ryzyka.

W związku z powyższym postuluję nowelizację art. 32 ust. 1 RODO we wskazany poniżej sposób.

Postuluję, by fragment przepisu, o którym tu mowa, miał postać: „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie ~~wystąpienia~~ i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku". (Czcionką przekreśloną zaznaczam element usunięty z przepisu.)

6.2. Art. 32 ust. 1 i 2 i 3 Postulat 2

Uczytelnienie przepisu

Wyżej w (*1.1. Art. 32 ust. 1. Analiza*) wskazuję, że wartości graniczne pojęć środki techniczne i środki organizacyjne leżą daleko od siebie, jednak *każde z tych pojęć zawiera znaczenia, które należą również do drugiego z pojęć*. Innymi słowy, trudno czasem odróżnić jedne środki od drugich. W związku z powyższym, ponieważ nie lubię przepisów niejasnych, postuluję nowelizację art. 32 ust. 1 RODO we wskazany poniżej sposób.

Postuluję usunięcie z art. 32 ust. 1 RODO słów „techniczne i organizacyjne".

Postuluję, by fragment przepisu, o którym tu mowa, miał postać: „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia

praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki ~~techniczne i organizacyjne~~, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:" (Czcionką przekreśloną zaznaczam element usunięty z przepisu.)

7. Art. 32 ust. 1 i 2 i 3 Rozważania historyczne

Rację ma R. Kania, który zwraca uwagę na fakt, że o ile pod rządami UODO 97 *najważniejsze było* m.in. *[...] uwzględnienie ścisłych wymagań technicznych, wyznaczonych przez ustawodawcę [...]* o tyle zastąpione to zostało przez *ryzyko i czas*[238]. Jest to pewien chwyt stylistyczny autora, jednak w swoim artykule, do którego odnoszę się również wyżej w uwadze (*3.5 Art. 32 ust. 1 i 2 i 3 Uwaga 5. Prawa i wolności*) omawia on właśnie kwestie związane z oceną ryzyka.

[238] R. Kania, op. cit., s. 34–36.

Rozdział 3
Naruszenie ochrony danych osobowych i jego zgłaszanie na gruncie art. 33 RODO i art. 34 RODO

Artykuł 33 RODO
Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

Artykuł 33 ust. 1 RODO

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

1. Art. 33 ust. 1 Analiza

Ze słów pogrubionych w cytacie: ***W przypadku naruszenia ochrony danych osobowych****, […] administrator […] zgłasza je organowi nadzorczemu […]* wnioskujemy, że prawodawca uzależnia wykonanie opisanych dalej w przepisie czynności od naruszenia ochrony danych osobowych. Naruszenie ochrony danych osobowych zdefiniowane jest w art. 4 pkt 12 RODO.

Na fakt, że naruszenie ochrony danych osobowych zdefiniowano w art. 4 pkt 12 RODO zwraca uwagę P. Fajgielski. Autor ten zbyt jednak wąsko rozumie zakres naruszenia. Paweł Fajgielski trafnie zwraca uwagę, że naruszeniem z art. 4 pkt 12 RODO są zdarzenia wymienione poniżej, a to:

1) przypadkowe lub niezgodne z prawem zniszczenie danych,
2) przypadkowa lub niezgodna z prawem utrata danych,
3) przypadkowe lub niezgodne z prawem zmodyfikowanie danych,
4) nieuprawnione ujawnienie danych,
5) nieuprawniony dostęp do danych[239].

Cytowany autor zapomina jednak lub pomija, że naruszeniem są też zdarzenia, które jedynie zagrażają zdarzeniami, które wskazał. Stanowisko P. Fajgielskiego jest zbieżne z dawnym stanowiskiem

[239] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679…,* Kom. do art. 33.

PUODO, stanowiskiem, z którego urząd się wycofał. Szeroko opisuję to w publikacji *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*[240], a później jeszcze w publikacji *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*.[241] Odsyłam zwłaszcza do drugiej ze wskazanych książek, wskazuję tam bowiem, jak – prawdopodobnie – pod wpływem doktryny zmieniło się stanowisko PUODO i to zmieniło się w kierunku bardziej restrykcyjnym. W skrócie wyglądało to tak, że zrazu PUODO niewłaściwie definiowało naruszenie ochrony danych osobowych, następnie, niezależnie od siebie, w komentarzu autorstwa P. Litwińskiego, P. Barty i M. Kaweckiego oraz w mojej książce, poświęconej dokumentacji, wskazane zostało właściwe rozumienie przepisu, do którego PUODO się dostosowało.

Dla podsumowania wywodu zwracam uwagę na fakt, że naruszeniami są zdarzenia wskazane przez P. Fajgielskiego oraz stany, w których zachodzi zagrożenie tymi zdarzeniami.

Z uwagi na fakt, że książka niniejsza skierowana jest między innymi do praktyków, dalej, w uwadze (*3.10. Art. 33 ust. 1 Uwaga 10. Naruszenie ochrony danych – zestawienie*) wymieniam zdarzenia, które – jeżeli mają miejsce – to należy je zakwalifikować jako naruszenie ochrony danych osobowych.

Ze słów pogrubionych w cytacie: *W przypadku naruszenia ochrony danych osobowych,* ***administrator*** *[…] zgłasza je […]* wnioskujemy, że obowiązki wynikające z przepisu spoczywają na administratorze. Przez administratora rozumiemy podmiot zdefiniowany w art. 4 pkt 7 RODO.

Ze słów pogrubionych w cytacie: *[…] administrator* ***bez zbędnej zwłoki*** *[…]* wnioskujemy, że obowiązki wynikające z przepisu należy realizować bez zbędnej zwłoki. Prawodawca nie określił, co rozumie przez zwrot *bez zbędnej zwłoki*. Co ciekawe, zwłoka w zgłoszeniu jest dopuszczalna, o ile tylko nie jest to zbędna zwłoka. Dopuszczalna jest zatem zwłoka niezbędna.

Ze słów pogrubionych w cytacie: *[…] administrator* ***bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia*** *– zgłasza je […]* wnioskujemy, że

[240] J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja…*, s. 353–354.

[241] J. Rzymowski, *RODO – GDPR. Przedmiot i cele…*, s. 520–526.

prawodawca określił znaczenie zwrotu *bez zbędnej zwłoki*. W rozumieniu przyjętym przez prawodawcę *bez zbędnej zwłoki* oznacza *w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia*. Prawodawca nie precyzuje, co należy rozumieć przez „stwierdzenie naruszenia", wydaje się jednak, że z uwagi na powszechnie przyjęte rozumienie słowa „stwierdzenie", przez stwierdzenie naruszenia rozumiemy moment dowiedzenia się przez administratora o fakcie zaistnienia naruszenia.

Bliższa analiza słów o stwierdzeniu naruszenia wskazuje, co może wydać się dziwne, że nie do końca wiadomo, w jaki sposób wskazane 72 godziny należy liczyć. Czytamy o stwierdzeniu naruszenia, ale nie do końca wiemy przez kogo owo naruszenie ma być stwierdzone, by uznać, że było stwierdzone. Z przepisu wynika, jak się wydaje, że przez administratora, bo na niego nałożono obowiązek zgłoszenia naruszenia, sprawa jednak wcale nie jest jasna. Kiedy administratora wyobrażamy sobie naiwnie jako osobę fizyczną, to obliczenie 72 godzin jest proste. Administrator dowiaduje się o naruszeniu i następnie od tego momentu zaczyna biec 72-godzinny termin. Jest to jednak podejście naiwne i intencjonalnie upraszczające stan faktyczny. Kiedy administratora wyobrażamy sobie na przykład jako spółkę, to obliczenie 72 godzin nie jest już takie proste.

Wyobraźmy sobie zdarzenie, które ma cechy naruszenia z art. 4 pkt 12 RODO. Zdarzenie ma miejsce, o zdarzeniu wie pracownik, który do niego doprowadził czy też pracownik, który je wykrył. Czy od tego momentu należy liczyć 72 godziny? Przecież na dobrą sprawę, patrząc z punktu widzenia przedmiotowego administratora, administrator ten nie wie jeszcze, czy naruszenie miało miejsce. Zaszło zdarzenie, *naruszenie bezpieczeństwa prowadzące do…* (art. 4 pkt 12 RODO), pracownicy administratora nie ustalili jednak jeszcze, czy zdarzenie to ma charakter naruszenia z art. 4 pkt 12 RODO. Istotne zatem pozostaje pytanie, czy termin 72-godzinny w opisanym stanie faktycznym już biegnie czy jeszcze nie – 72 godziny wydają się być terminem przeznaczonym na ocenę skutków naruszenia, na ocenę ryzyka naruszenia praw i wolności osób fizycznych przez pryzmat art. 33 RODO i art. 34 RODO, żeby jednak dokonywać tych czynności, trzeba mieć pewność, że zdarzenie, które zaszło miało charakter naruszenia z art. 4 pkt 12 RODO, a ustalenie tego – zwłaszcza w dużej strukturze administratora – może zająć wręcz kilka dni. Wydaje się, że

tak długie ustalanie, czy zdarzenie było naruszeniem świadczy o pewnej niekompetencji odpowiednich służb administratora, należy jednak mieć świadomość, że trudno oczekiwać, by administrator i jego służby posiadali wiedzę pełną i doskonałą. Zdobycie wiedzy o samym zdarzeniu może zająć nieco czasu idącego w dni lub godziny, a dopiero po zdobyciu tej wiedzy można przystąpić do ustalania, czy zdarzenie miało charakter naruszenia, a z kolei po ustaleniu tego faktu można przystąpić do oceniania poziomu ryzyka naruszenia praw i wolności osób fizycznych.

Przeprowadzone tu rozważanie nie zawiera odpowiedzi na pytanie o to, od jakiego momentu liczyć termin 72-godzinny. Mam tego świadomość i mam też świadomość, że problem nad którym się tu zastanawiam, nie znajduje, jak się wydaje, rozwiązania na gruncie RODO. Problemem podstawowym, nad którym się tu zastanawiam, jest ustalenie, który moment w łańcuchu zdarzeń uznać za stwierdzenie naruszenia. Podstawowe rozwiązania są dwa.

– Rozwiązanie najprostsze jednak nieprzychylne dla administratora to uznanie że ze stwierdzeniem naruszenia mamy do czynienia w momencie, kiedy pracownik administratora dowiaduje się o zdarzeniu, które później zostaje zakwalifikowane jako naruszenie z art. 4 pkt 12 RODO.
– Rozwiązanie bardziej przychylne dla administratora to uznanie, że ze stwierdzeniem naruszenia mamy do czynienia w momencie, kiedy uprawniony pracownik administratora podejmuje decyzję, że jakieś zdarzenie ma charakter naruszenia z art. 4 pkt 12 RODO. Przyznam, że to rozwiązanie jest mi bliższe. Daje ono nieco więcej czasu administratorowi, ale też niejako szanuje jego decyzyjność.

Problem z liczeniem 72 godzin dostrzegli P. Barta, M. Kawecki i P. Litwiński. Autorzy ci, powołując się na stanowisko EROD, zwrócili uwagę, że *[...] należy uznać, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym uzyskał wystarczającą dozę pewności co do tego, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do ujawnienia danych osobowych*[242]. Z treścią zawarta w cytacie mam pewien problem. Zgadzam się z ogólną myślą wynikającą z cytatu, którą rozumiem tak, że „stwierdzenie wystąpienia naruszenia" ma charakter subiektywny. Zapewne zresztą nie bez

[242] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 348–349.

powodu cytowani autorzy pogląd ten powołali. Zgadzam się z tą myślą do tego stopnia, że nieco w jej duchu stawiam niżej *postulat „de lege ferenda"* (*6.1. Art. 33. Postulat 1. Jak liczyć termin 72-godzinny*). Mam jednak pewien niepokój spowodowany użyciem słów o „incydencie bezpieczeństwa".

Artykuł 34 ust. 1 RODO stanowi o naruszeniu ochrony danych osobowych, naruszenie to jest zdefiniowane w art. 4 pkt 12 RODO. Nie rozwijam tu wątku, rozwijam go bowiem w uwadze (*3.9. Art. 33 ust. 1 Uwaga 9. Incydent*), jednak i tam, i tu przejawiam niepokój spowodowany stosowaniem pojęcia „incydent bezpieczeństwa". Podobnie w duchu subiektywnej oceny nieuzasadnionej zwłoki wypowiada się[243] C. Burton.

W duchu subiektywnej oceny wypowiadają się też, choć nieco inaczej niż C. Burton, autorzy czeskiego komentarza, którzy zwracają uwagę[244] na fakt, że warunkiem realizacji obowiązku z art. 33 RODO jest, by administrator dowiedział się o naruszeniu. Pozornie rzecz jest oczywista, jednak należy sobie to w pełni uświadomić, że jeżeli naruszenie miało miejsce i jednocześnie administrator nie wie, że to naruszenie miało miejsce, to nie ma on szansy zrealizować obowiązków, które wynikają z art. 33 RODO. Co więcej, jeżeli administrator nie wie, że miało miejsce naruszenie, to nie tylko nie może on dokonać zgłoszenia tego naruszenia do PUODO, ale nie może nawet dokonać oceny poziomu ryzyka naruszenia praw i wolności. Nie może dokonać oceny poziomu ryzyka naruszenia praw i wolności, ponieważ nie wie, że naruszenie ochrony danych osobowych miało miejsce. Należy się tu zastanowić nad tym, czy jeżeli administrator nie zgłosi naruszenia, ponieważ o nim nie wiedział, to czy grozi mu odpowiedzialność za niezgłoszenie naruszenia. Pozornie odpowiedź wydaje się prosta, jednak wcale taką nie jest i z uwagi na doniosłość problemu zajmuję się tym niżej w uwadze (*3.17. Art. 33 Uwaga 17. Skutek niestwierdzenia naruszenia ochrony danych osobowych*).

Ze słów pogrubionych w cytacie: *W przypadku naruszenia ochrony danych osobowych,* ***administrator*** *[...]* ***zgłasza je*** *[...]* wnioskujemy, że z przepisu wynika spoczywający na administratorze obowiązek zgłoszenia naruszenia.

---

[243] C. Burton, op. cit., s. 646.

[244] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit., s. 297.

Ze słów pogrubionych w cytacie: *W przypadku naruszenia ochrony danych osobowych, administrator […]* ***zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55*** *[…]* wnioskujemy, że zgłoszenie naruszenia należy dokonać organowi nadzorczemu. Przez organ nadzorczy rozumiemy PUODO

Ze słów: *[…]* ***chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.*** *[…]* wnioskujemy, że administrator nie ma obowiązku zgłoszenia naruszenia, jeżeli jest mało prawdopodobne, by naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Istotne jest, że obowiązek zgłoszenia uzależniono od tego, czy ryzyko naruszenia praw lub wolności osób fizycznych jest prawdopodobne, czy jest mało prawdopodobne. Jeżeli prawdopodobne jest, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, to naruszenie takie należy zgłosić, w terminie opisanym wyżej w przepisie. Jeżeli mało prawdopodobne jest, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, to naruszenie takiego nie należy zgłaszać. Uzależnienie zgłoszenia naruszenia od tego, czy ryzyko […] jest prawdopodobne czy mało prawdopodobne, oznacza, że administrator (danych osobowych) powinien ocenić ryzyko, zanim podejmie decyzję o zgłoszeniu lub o niezgłoszeniu naruszenia. Decyzja ta, jak również związane z nią rozważania powinny przybrać postać pisma, by można wykazać, że decyzje te podejmowano.

Należy zwrócić uwagę na jeden jeszcze niezwykle istotny szczegół. Otóż przepis uzależnia obowiązek zgłoszenia naruszenia ochrony danych osobowych do PUODO od prawdopodobieństwa *naruszenia praw lub wolności osób fizycznych*. Szczególną uwagę zwracam na słowa: „osób fizycznych". Jeżeli zatem naruszenie bezpieczeństwa skutkuje ryzykiem naruszenia praw lub wolności osoby fizycznej, nie osób fizycznych, to takiego naruszenie nie podlega zgłoszeniu. Piszę o tym szerzej w uwadze (*3.8. Art. 33 ust. 1 Uwaga 8. Naruszenie praw lub wolności jednej osoby fizycznej*).

Należy zwrócić uwagę na jeden jeszcze element. Otóż naruszenie nie podlega zgłoszeniu, jeżeli jest mało prawdopodobne, by naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Należy się zatem poważnie zastanowić, kiedy naruszenie podlega zgłoszeniu.

Jeżeli jest **mało prawdopodobne**, by naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, to naruszenie nie podlega zgłoszeniu.

Jeżeli jest **prawdopodobne**, że naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, to naruszenie podlega zgłoszeniu.

Wnioski dotyczące tego, co czynić należy, wskazane wyżej wynikają z prostej językowej analizy słów przepisu. Skoro coś może być mało prawdopodobne, a o tym, że może, wiemy ze słów przepisu, to zapewne to samo zjawisko może również być prawdopodobne.

Należy jednak zwrócić uwagę na kolejny element wywodu. Otóż przepis mówi o prawdopodobieństwie naruszenia praw lub wolności osób fizycznych. Może się jednak zdarzyć, że wskutek naruszenia ochrony danych osobowych zaistnieje nie ryzyko naruszenia praw i wolności o tym czy innym prawdopodobieństwie, ale że zajdzie naruszenie praw i wolności. Dopasowując zatem do przyjętej wyżej konwencji, należy stwierdzić jak w następnym zdaniu.

Jeżeli naruszenie ochrony danych **skutkowało naruszeniem** praw lub wolności osób fizycznych, to naruszenie podlega zgłoszeniu.

Dla porządku warto zwrócić uwagę na kolejny element, otóż między *jest **prawdopodobne**, że naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych* a „naruszenie ochrony danych **skutkowało naruszeniem** praw lub wolności osób fizycznych", znajduje się jeszcze naruszenie ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przy czym „poziom" ten zaczerpnięty został z art. 34 ust. 1 RODO, dotyczącego informowania osób, których dane dotyczą o naruszeniu. Szerzej analizowane jest to w (*3.8. Art. 34 ust. 1 Uwaga 8. Zawiadamianie osób, zgłaszanie PUODO. Uwagi porządkujące*).

Nad zjawiskiem niezgłaszania naruszenia pochylił się P. Fajgielski, trafnie zwracając uwagę, że *Przykładem sytuacji, w której naruszenie ochrony danych wiąże się z małym prawdopodobieństwem naruszenia praw osób, których dane dotyczą, może być przypadek*

utraty danych osobowych wskutek awarii sprzętu komputerowego, w sytuacji, gdy dane udało się odzyskać z kopii zapasowej[245].

Ten sam autor wskazuje, że *omawiany przepis może być powodem wątpliwości interpretacyjnych i niejednolitej praktyki* i zwraca przy tym uwagę na swoją wcześniejszą publikację w tej samej sprawie, co może wskazywać na fakt, że problem ten leży P. Fajgielskiemu na sercu. Jest to zrozumiałe, powiem więcej, mam własne obserwacje, niepoparte co prawda badaniami ilościowymi, ale jednak, które wskazują, że administratorzy mają problemy z podjęciem decyzji o poinformowaniu lub niepoinformowaniu PUODO.

Pierwszym źródłem problemu bywa nieumiejętność ustalenia, czy dane zdarzenie jest w ogóle zgłaszalne.

Drugim źródłem problemu bywa kłopot z ustaleniem poziomu ryzyka naruszenia praw i wolności, czyli problem jest tam, gdzie go dostrzega P. Fajgielski.

Dostrzegam też trzecie źródło problemu, a mianowicie w przypadku naruszeń ochrony danych osobowych, które skutkują naruszeniem praw i wolności, administratorzy miast pogodzić się z faktem, że prawa i wolności naruszono i poinformować o tym PUODO i osoby, których dane dotyczą, przystępują do oceny poziomu ryzyka naruszenia praw i wolności, co może doprowadzić ich do błędnej decyzji o niepoinformowaniu PUODO.

Należy sobie postawić pytanie o to, czy można tu postawić jakiś racjonalny wniosek. Wydaje się, że wątpliwości interpretacyjne są naturalnym problemem prawniczym i od tego się nie uwolnimy. Mając to na uwadze, uważam, że może dobrze by było, gdyby prawodawca w sposób nieco bardziej precyzyjny wskazał, kiedy organ informować należy, a kiedy nie. Nie stawiam tu konkretnego postulatu *de lege ferenda*, mam bowiem wątpliwość, jak przepis, w ewentualnej zmienionej wersji wyglądać powinien. Jednocześnie uważam, że art. 33 ust. 1 RODO i art. 34 ust. 1 RODO (i ewentualnie kolejne ustępy wskazanych artykułów) mogą być napisane jaśniej. Piszę o tym w postulatach (*6. Art. 34 ust. 1. Postulaty „de lege ferenda”*).

---

[245] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679…,* Kom. do art. 33. Przypis P. Fajgielskiego: P. Fajgielski, *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych* [w:] *Aktualne problemy prawnej ochrony danych osobowych 2016*, red. G. Sibiga, M. Praw. 2016/20, s. 45, dodatek specjalny.

Kolejnym problemem, nad jakim trzeba się pochylić przy omawianiu wskazanego fragmentu, jest problem, jakie prawa i wolności należy brać pod uwagę. Naruszenie jakich praw i wolności należy oceniać pod kątem podjęcia decyzji o informowaniu o naruszeniu organu ochrony danych. Piszę o tym w uwagach: (*3.2. Art. 33 ust. 1 Uwaga 2. Prawa i wolności przy ocenie skutków naruszenia*), (*3.3. Art. 33 ust. 1 Uwaga 3. Prawa i wolności w RODO. Zarys zagadnień*), (*3.5. Art. 33 ust. 1 Uwaga 5. Prawa i wolności. Źródła inne niż RODO*), (*3.6. Art. 33 ust. 1 Uwaga 6. Prawa i wolności w EKPC*), (*3.7. Art. 33 ust. 1 Uwaga 7. Prawa i wolności w KPP UE*).

Ze słów pogrubionych w cytacie: ***Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin*** *dołącza się wyjaśnienie przyczyn opóźnienia* wnioskujemy, że realizację warunku zawartego w niewytłuszczonej części cytatu, czyli obowiązek dołączenia do zgłoszenia wyjaśnienia przyczyn opóźnienia uzależniono od faktu przekazania zgłoszenia organowi nadzorczemu po upływie 72 godzin. Z wcześniejszej części przepisu wynika, że 72-godziny należy liczyć od momentu stwierdzenia naruszenia.

Ze słów pogrubionych w cytacie: ***Do zgłoszenia*** *przekazanego organowi nadzorczemu po upływie 72 godzin* ***dołącza się wyjaśnienie przyczyn opóźnienia*** wnioskujemy, że do zgłoszenia, które następuje po upływie 72 godzin od momentu stwierdzenia naruszenia, należy dołączyć wyjaśnienie przyczyny opóźnienia.

2. Art. 33 ust. 1. Komentarz

Z przepisu wnioskujemy, że prawodawca uzależnia wykonanie opisanych w przepisie czynności od zaistnienia naruszenia ochrony danych osobowych.

Naruszenie ochrony danych osobowych zdefiniowane jest w art. 4 pkt 12 RODO[246].

Obowiązki wynikające z przepisu spoczywają na administratorze lub na jednym ze współadministratorów – odpowiednio do ustaleń między nimi[247]. Szerzej w uwadze *(3.16. Art. 33 Uwaga 16. Naruszenie ochrony danych osobowych w realiach współadministrowania*).

---

[246] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit., s. 296.

[247] Por. P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 349.

Obowiązki wynikające z przepisu należy realizować bez zbędnej zwłoki. Prawodawca określił znaczenie zwrotu „bez zbędnej zwłoki". W rozumieniu przyjętym przez prawodawcę, zwrot „bez zbędnej zwłoki" oznacza „*nie później niż w terminie 72 godzin po stwierdzeniu naruszenia*".

Prawodawca nie precyzuje, co należy rozumieć przez „stwierdzenie naruszenia", wydaje się jednak, że z uwagi na powszechnie przyjęte rozumienie słowa „stwierdzenie", przez stwierdzenie naruszenia rozumiemy moment dowiedzenia się przez administratora o fakcie zaistnienia naruszenia.

Z przepisu wynika spoczywający na administratorze (danych osobowych) obowiązek zgłoszenia naruszenia. Zgłoszenia naruszenia należy dokonać organowi nadzorczemu. Przez organ nadzorczy w Polsce należy rozumieć Prezesa Urzędu Ochrony Danych Osobowych.

Administrator nie ma obowiązku zgłoszenia naruszenia, jeżeli jest mało prawdopodobne, by naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Istotne jest, że obowiązek zgłoszenia uzależniono od tego, czy ryzyko naruszenia praw lub wolności osób fizycznych jest prawdopodobne, czy jest mało prawdopodobne.

Jeżeli prawdopodobne jest, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, to naruszenie takie należy zgłosić, w terminie opisanym wyżej w przepisie.

Jeżeli mało prawdopodobne jest, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, to naruszenie takiego nie należy zgłaszać.

Uzależnienie zgłoszenia naruszenia od tego, czy ryzyko naruszenia praw lub wolności osób fizycznych jest prawdopodobne czy mało prawdopodobne, oznacza, że administrator (danych osobowych) powinien ocenić ryzyko, zanim podejmie decyzję o zgłoszeniu lub o niezgłoszeniu naruszenia. Decyzja ta, jak również związane z nią rozważania, powinny przybrać postać pisma, tak by w poszanowaniu zasady rozliczalności można wykazać, że decyzje te podejmowano.

Do zgłoszenia, które następuje po upływie 72 godzin od momentu stwierdzenia naruszenia, należy dołączyć wyjaśnienie przyczyny opóźnienia. Czas ten – 72 godziny należy liczyć od momentu stwierdzenia naruszenia.

3. Art. 33 ust. 1 Uwagi

3.1. Art. 33 ust. 1 Uwaga 1

Ocena ryzyka naruszenia praw i wolności

Ocena ryzyka naruszenia praw i wolności jest, być może, największym wyzwaniem w interpretacji art. 33 RODO. Jest tak ponieważ związane są z tym dwa problemy.

– po pierwsze – jakie prawa i wolności należy brać pod uwagę przy ocenie skutków naruszenia,
– po drugie – jak tej oceny dokonywać.

Ponadto problem ten nakłada się na problem, na który uwagę zwróciła K. Gałęzowska, a mianowicie kiedy zachodzi naruszenie ochrony danych osobowych, kiedy należy odstąpić od informowania organu ochrony danych[248] i kiedy należy jednak organ ten o naruszeniu poinformować. Jak uporać się ze wskazanymi problemami piszę niżej w kolejnych uwagach, jednak nawet sam tylko fakt, że omówienie spraw z pozoru prostych wymaga tylu stron rozważań, dowodzi, że sprawy te, nawet jeśli proste są (bo tak uważam), to uregulowane są w RODO w sposób cokolwiek niejasny.

3.2. Art. 33 ust. 1 Uwaga 2

Prawa i wolności przy ocenie skutków naruszenia

Artykuł 33 ust. 1 RODO uzależnia obowiązek informowania organu ochrony danych od poziomu ryzyka naruszenia praw i wolności, jaki zaistniał w wyniku naruszenia.

Artykuł 34 ust. 1 RODO uzależnia zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych od poziomu ryzyka naruszenia praw i wolności osób fizycznych.

Kwestię ustalenia, jakie prawa i wolności brać pod uwagę, omawiam raz, oczywiste bowiem jest, że zarówno dla potrzeb oceny na gruncie art. 33 ust. 1 RODO, jak i dla potrzeb oceny na gruncie art. 34

[248] K. Gałęzowska, *Zgłaszanie naruszeń – omówienie nowych wytycznych EROD i problemów praktycznych*, [w:] *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych. Aktualne problemy ochrony danych osobowych 2021*. Pod red. G. Sibigi. Dodatek specjalny do „Monitora Prawniczego" 2020, nr 23, s. 52.

ust. 1 RODO należy brać pod uwagę te same prawa i wolności. Wynika to przede wszystkim z zakazu wykładni homonimicznej, znanego też pod nazwą zasady konsekwencji terminologicznej[249]. W najprostszy sposób wyjaśnić można go tak, że jeżeli prawodawca w dwóch różnych miejscach tego samego aktu prawnego używa tego samego słowa, to należy to słowo w obydwu miejscach rozumieć tak samo. Oczywiście miejsc może być więcej niż dwa, a słowo nie musi być jedno, może być to zwrot.

Dla podsumowania tej części wywodu należy stwierdzić, że w niniejszej książce zajmuję się art. 24 RODO, art. 32 RODO, art. 33 RODO i art. 34 RODO; w każdym ze wskazanych przepisów zapisany jest obowiązek dokonywania oceny ryzyka naruszenia praw i wolności. Dla podkreślenia, odpowiednie części przepisów są wytłuszczone, a części nieistotne dla rozważania są usunięte.

W art. 24 ust. 1 czytamy: *Uwzględniając […]* ***ryzyko naruszenia praw lub wolności osób fizycznych*** *o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne […]*

W art. 32 ust. 1 czytamy: *Uwzględniając […]* ***ryzyko naruszenia praw lub wolności osób fizycznych*** *o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne […]*

W art. 33 ust. 1 czytamy: *W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki […] zgłasza je organowi nadzorczemu […] chyba że jest mało prawdopodobne, by naruszenie to* ***skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych***.

W art. 34 ust. 1 czytamy: *Jeżeli naruszenie ochrony danych osobowych* ***może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych****, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą […]*

W czterech wskazanych przepisach uzależniono wykonanie pewnych czynności od poziomu ryzyka naruszenia praw i wolności osób fizycznych, w związku z różnymi zdarzeniami. Artykuł 24 ust. 1 RODO i art. 32 ust. 1 RODO odnoszą się do oceny ryzyka na etapie wykonywania tejże na początku działalności administratora (ewen-

[249] L. Morawski, op. cit., s. 104–105.

tualnie przy pierwszym wdrożeniu RODO u administratora) i potem powtarzalnie w miarę potrzeb. Zdarzeniem kluczowym jest tu ocena ryzyka. Art. 33 ust. 1 RODO i art. 34 ust. 1 RODO odnoszą się do oceny skutków naruszenia ochrony danych osobowych. Mirosław Gumularz i T. Izydorczyk pięknie opisują to zjawisko w cytowany niżej sposób.

Określanie przyczyny wystąpienia ryzyka naruszenia praw lub wolności, na uwagi na to, kiedy jest wykonywane, dzieli się na dwa podstawowe sposoby:

1) określanie przyczyn (źródeł) ryzyk potencjalnych – czyli takich, które się jeszcze nie wydarzyły;

2) określanie przyczyn (źródeł) ryzyk zaistniałych – czyli takich, które się zmaterializowały[250].

Wypowiedź wskazanych autorów jest dla mnie o tyle cenna, że wynika z niej, że na etapie oceny ryzyka, na gruncie art. 24/32 RODO (bo tak rozumiem punkt 1 cytatu) administrator ocenia coś, co się jeszcze nie wydarzyło, ale co się zdarzyć może. Jeśli chodzi o punkt drugi cytatu, to autorzy odnoszą się zapewne do art. 33/34 RODO. Rzeczywiście oceniamy tam ryzyko zaistniałe, czyli zdarzenie, które miało miejsce, ale jeśli mamy oceniać ryzyko zaistniałe, to oceniamy raczej skutki takiego zdarzenia. Jeśli zdarzeniem jest np. ujawnienie danych osobowych, które zaszło w warunkach naruszenia ochrony danych osobowych, to oceniane skutki to poziom ryzyka naruszenia praw i wolności. Jeżeli przyjmiemy, że zdarzeniem tym jest naruszenie praw i wolności, to skutkiem będzie dalsze działanie administratora, czyli informowanie lub nieinformowanie odpowiednio osób, których dane dotyczą i organu ochrony danych osobowych. Słowa o ryzykach potencjalnych zwracają też – moim zdaniem – uwagę na to, że administrator nie tyle ma przewidywać przyszłość, co jest trudne, o ile nie niemożliwe, ile ma on oceniać, jakie ryzyko zachodzi w momencie dokonywania oceny – to jest właśnie ryzyko potencjalne. Administrator nie wie, czy owo ryzyko się zrealizuje, czy nie, bo wiedzieć tego nie może; wie jednak, czy w odniesieniu do danej czynności ryzyko to zachodzi czy nie.

Z uwagi na powtarzalność zjawiska i wskazaną wyżej konieczność brania pod uwagę tych samych praw i wolności, kwestię oceny

[250] M. Gumularz, T. Izydorczyk, op. cit., s. 46.

ryzyka naruszenia praw i wolności omawiam w tym miejscu zarówno dla potrzeb interpretacji art. 33 RODO, jak i dla potrzeb interpretacji art. 34 RODO.

Zwracam jednocześnie uwagę na fakt, że kwestię praw, obowiązków i wolności w RODO omawiam w książce *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*[251], oraz w niniejszej książce w uwagach: (*3.1. Art. 24 Uwaga 1.Prawa i wolności*), (3.2. Art. 24 Uwaga 2. *Przykładowe prawa i wolności zasadnicze*), (*3.3. Art. 24 Uwaga 3. Przykładowe prawa i wolności szczegółowe*), (*3.4. Art. 24 Uwaga 4. Inne prawa i wolności*); uwagi te tyczą się art. 24 RODO. Zajmuję się tym też w niniejszej książce w uwagach (*3.4 Art. 32 ust. 1 i 2 i 3 Uwaga 4. Błędy w ocenie ryzyka*) i (*3.5 Art. 32 ust. 1 i 2 i 3 Uwaga 5. Prawa i wolności*), poczynionych przy okazji analizy art. 32 RODO.

Znacznie bogatsze zestawienie znajdziemy w tekście G. Sibigi i współautorów, którzy zestawili[252] bodaj wszystkie przepisy RODO, dla stosowania których ryzyko jest istotne. Podkreślenia wymaga jedynie, że w każdej sytuacji jest to ryzyko naruszenia praw i wolności.

Wyżej wyjaśniam, że kiedy w RODO mowa jest o prawach i wolnościach, to zawsze o tych samych. Pytaniem pozostaje jednak, o jakie to prawa i wolności chodzi w RODO. Myślę, że z problemem tym zmagał się W. Chomiczewski, który w komentarzu do art. 33 RODO wskazał, że prawa i wolności należy rozumieć podobnie, jak na gruncie przepisu art. 6 ust. 1 lit. f RODO i dodatkowo przypisem odesłał do konkretnej uwagi własnej poczynionej jako element komentarza do art. 6 ust. 1 lit. f RODO[253]. Skoro W. Chomiczewski odesłał, to nie pozostało nic innego, jak iść drogą jego odesłania. Poszedłem zatem, przyznam jednak, że doznałem pewnego rozczarowania. Wskazany autor pisze zrazu, że: *Kategorią obiektywną są natomiast podstawowe prawa i wolności podmiotu danych*[254]. (Z tym można się zgodzić, po-

---

[251] J. Rzymowski, *RODO – GDPR. Przedmiot i cele...*

[252] G. Sibiga, I. Małobęcka-Szwast, D. Nowak, K. Syska, [w:] D. Lubasz red. n. *Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych*, Warszawa 2022, s. 64–65.

[253] W. Chomiczewski, [w:] *RODO Ogólne rozporządzenie o ochronie danych. Komentarz.* Red. n. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka. Warszawa 2018, s. 711.

[254] Ibidem, s. 395.

jęcie kategorii obiektywnej jest co prawda nieco mętnawe, jednak w konkretnym miejscu, w którym użył go W. Chomiczewski jest ono czytelne jako przeciwieństwo interesu, o którym mowa w art. 6 ust. 1 lit. f RODO.) Nadal jednak nie wiem, o jakie prawa i wolności chodzi. Wskazany autor pisze, że: *Należy ich poszukiwać zarówno w przepisach europejskich, jak i krajowych. Na gruncie tych pierwszych będzie chodziło w szczególności o prawa podstawowe i wolności wskazane w Karcie Praw Podstawowych Unii Europejskiej, a także Europejskiej Konwencji Praw Człowieka. Dodatkowo podstawowe prawa i wolności mogą wynikać z prawa krajowego poszczególnych państw członkowskich, a zwłaszcza z ich konstytucji*[255].

Zasadnicza deklaracja W. Chomiczewskiego wygląda dobrze, autor wskazuje doniosłe akty prawne. Niestety, pojawia się tu pewien problem, otóż zarówno w Karcie Praw Podstawowych Unii Europejskiej (dalej: KPP UE), jak i w Europejskiej Konwencji Praw Człowieka (dalej: EKPC) niewiele jest do znalezienia na temat ochrony danych osobowych czy nawet prywatności.

Jeśli chodzi o KPP UE to analizy tego aktu prawnego pod kątem ustalenia, jakie prawa są na jego gruncie chronione, dokonałem przy okazji pisania książki *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*[256]. Ustaliłem wtedy, że w KPP UE zapisanych jest około 152 praw człowieka. Używam określenia „około", mimo precyzyjnego wskazania liczby, ponieważ możliwe jest nieco inne wyróżnienie niektórych praw. Prawa te wymieniam we wskazanej książce, nie widzę więc sensu, by wymieniać je tutaj. Dla ułatwienia lektury wymieniam niżej jedynie te prawa, które, moim zdaniem związane są z ochroną danych osobowych i prywatnością. Jest ich kilka. Dalej w uwadze (*3.7. Art. 33 ust. 1 Uwaga 7. Prawa i wolności w KPP UE*) wskazuję dziesięć tych praw.

Jeśli chodzi o EKPC, to dla podjęcia uczciwej polemiki z W. Chomiczewskim, przyjrzałem się temu aktowi przy pisaniu niniejszych słów. Dla porządku wypisałem z EKPC wszystkie prawa. Jest ich około 19. Z dziewiętnastu praw można pod kątem ochrony danych osobowych, ochrony prywatności wybrać może dwa. Wszystkie prawa z EKPC wymieniam niżej w uwadze (*3.6. Art. 33 ust. 1 Uwaga*

[255] Ibidem, s. 395–396.

[256] J. Rzymowski, *RODO – GDPR. Przedmiot i cele...*

6. Prawa i wolności w EKPC), zwracam tam też uwagę na wspomniane dwa.

Nie podejmuję trudu wypisania wszystkich praw z Konstytucji, jedynie dla potrzeb polemiki z W. Chomiczewskim. W Konstytucji – co nie jest tajemnicą ni odkryciem – zapisano prawo do ochrony danych osobowych. Jest ono zapisane w art. 51 Konstytucji, który brzmi:

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa. osobowych.

Podsumowując powyższe ustalenia, należy stwierdzić, że w KPP UE praw, związanych z ochroną danych osobowych, jest dziesięć, w EKPC są dwa, w Konstytucji jest jedno. Nie jest to wiele, ale współgra to z uwagą W. Chomiczewskiego, który pisze, że: *Na gruncie przepisu art. 6 ust. 1 lit. f nie chodzi o każdy* ***interes, podstawowe prawo i wolność****, lecz tylko o takie,* ***które wymagają ochrony danych osobowych****. Oceny spełnienia tego warunku trzeba dokonywać już na gruncie konkretnego stanu faktycznego*[257]. O ile z pierwszą z zawartych w cytacie myśli się zgadzam, a nawet więcej, wymieniam poniżej tylko te prawa, które związane są z ochroną danych osobowych, o tyle co do drugiej ze wskazanych myśli mam poważną wątpliwość.

Uważam otóż, że błędem niebezpiecznym dla administratora jest wybieranie tych czy innych praw i wolności, zależnie od konkretnego naruszenia. Pozornie wydaje się to nieuzasadniona wątpliwość. Pozornie wydaje się, że wskazane jest, kiedy administrator dostosowuje swoje postępowanie do zdarzenia. Więcej nawet, mógłby ktoś rzec, że wybierając odpowiednie prawa i wolności zależnie od zdarze-

[257] W. Chomiczewski, op. cit., s. 396.

nia, administrator dokonuje po prostu poprawnej subsumpcji. Pozornie wydaje się to wszystko prawdą.

Pozornie. Należy sobie bowiem zadać pytanie o to, co się stanie, kiedy administrator niewłaściwie wybierze prawa do oceny ryzyka ich naruszenia. Powody mogą być różne. Administrator może być po prostu niekompetentny i wybrać nie te prawa, które powinien. Administrator może też wykonać inny manewr i wybrać te prawa, które nie zostały przez dane naruszenie ochrony danych osobowych naruszone ani nawet zagrożone.

Piszę wyżej, że jest to niebezpieczne dla administratora. Uważam tak dlatego, że jeżeli administrator nie wybierze właściwych praw i nie oceni naruszenia ochrony danych przez pryzmat ryzyka naruszenia tych praw, to może się zdarzyć, że administrator nie zgłosi naruszenia do PUODO ani nie poinformuje o naruszeniu osób, których dane dotyczą, mimo że naruszenie wymagało czy to tylko zgłoszenia do PUODO, czy to zgłoszenia do PUODO i poinformowania osób. Należy sobie uświadomić, co się dzieje, kiedy administrator bierze pod uwagę niewłaściwe prawa, a zwłaszcza prawa, które nie zostały naruszone zdarzeniem. Spójrzmy po kolei.

– Ma miejsce zdarzenie.
– Administrator ustala, że zdarzenie to jest naruszeniem ochrony danych osobowych z art. 4 pkt 12 RODO.
– Administrator dokumentuje ustalenia.
– Administrator wybiera niewłaściwe prawa, wybiera te prawa, które nie zostały naruszone naruszeniem ochrony danych osobowych.
– Administrator ocenia poziom ryzyka naruszenia wybranych (niewłaściwych) praw.
– Administrator dokumentuje ustalenia.
– Z oceny ryzyka naruszenia praw wynika, że nie należy zgłaszać naruszenia PUODO ani informować o nim osób, których dane dotyczą.
– Administrator nie zgłasza naruszenia do PUODO.

Przerwijmy w tym miejscu wyliczankę i zastanówmy się, co się stało. Administrator nie zgłosił naruszenia ani nie poinformował osób. Administrator postąpił tak, ponieważ ustalił, że ryzyko naruszenia praw i wolności osób fizycznych było niskie. Tylko że w tym miejscu administrator popełnił pewien błąd. Otóż administrator wybrał niewłaściwe prawa i wolności. Ryzyko naruszenia tych praw i wolności,

które administrator wybrał, rzeczywiście było niskie, ale ryzyko naruszenia innych praw i wolności, których administrator nie brał pod uwagę przy ocenie, było podstawowe lub wysokie. Jak zatem widać, naruszenie skutkuje takim poziomem ryzyka naruszenia praw i wolności, który skutkuje obowiązkiem zgłoszenia do PUODO, jednak administrator nie dokonuje zgłoszenia do PUODO, ponieważ nie wie, że naruszenie ochrony danych skutkuje wyższym – niż mu się wydaje – poziomem ryzyka naruszenia praw i wolności. Administrator nie wie, ponieważ wybrał niewłaściwe prawa i wolności. Nieważne, czy uczynił to z przebiegłości czy z nieuctwa. Skutek może być ten sam – kara administracyjna za naruszenie i kara administracyjna za niezgłoszenie naruszenia.

Z powyższych rozważań przebija jeden wniosek, kluczowe jest ustalenie katalogu praw (i wolności), które należy brać pod uwagę przy ocenianiu poziomu ryzyka naruszenia praw i wolności. Równie ważne jest, by po ustaleniu tego katalogu trzymać się go i nie go nie zawężać. Można, stosownie do okoliczności, brać pod uwagę te czy inne prawa, ze źródeł wskazanych przez W. Chomiczewskiego czy jakichkolwiek innych, jednak praw, które należą do – nazwijmy to – katalogu minimalnego, pomijać nie wolno. Nie wolno, bo prędzej czy później skończy się to karą. Katalog tych praw pokrywa się z katalogiem zasad z art. 5 RODO. Zestawiam je w niżej w części książki zatytułowanej *Tabele pomocnicze, zestawienia*.

Witold Chomiczewski wskazał kilka źródeł praw. Odnoszę się do tego wyżej, prawa wskazane w tych źródłach wskazuję niżej, jednak wskazany autor zapomniał o jednym jeszcze źródle. Źródle najważniejszym, z punktu widzenia podejmowanych tu rozważań. Źródłem tym jest… RODO!

Rozważania dotyczące tego, jakie prawa i wolności należy brać pod uwagę przy stosowaniu RODO, nawiązują do analogicznych rozważań prowadzonych w niniejszej publikacji, na gruncie art. 24 RODO w uwagach (*3.1. Art. 24 Uwaga 1.Prawa i wolności*), (*3.2. Art. 24 Uwaga 2. Przykładowe prawa i wolności zasadnicze*), (*3.4. Art. 24 Uwaga 4. Inne prawa i wolności*), (*3.2. Art. 24 Uwaga 2. Przykładowe prawa i wolności szczegółowe*) oraz na gruncie analizy art. 32 RODO w uwadze (*3.5 Art. 32 ust. 1 i 2 i 3 Uwaga 5. Prawa i wolności*). Zagadnieniami tym zajmuję się również w pozostałych książkach z niniejszego cyklu, a to w *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wol-*

ności, definicje. (str. 78-143), *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*. (s. 143–159). Rozważań tych nie chcę powtarzać, jedynie dla porządku sygnalizuję poniżej główne ich wątki.

Należy pamiętać, że ustalenie poziomu ryzyka naruszenia praw i wolności osób fizycznych jest zagadnieniem niezwykle istotnym już choćby z tego powodu, że zależnie od tego poziomu ryzyka, na administratorze spoczywa obowiązek poinformowania PUODO o naruszeniu lub (odpowiednio) obowiązek ten na administratorze nie spoczywa. W związku z tym, nie sposób zgodzić się z pewną myślą P. Barty, M. Kaweckiego i P. Litwińskiego, wyrażoną w komentarzu[258]. Czytamy tam, że: *Ustawodawca unijny wskazał, że nie każde naruszenie ochrony danych osobowych związane jest z naruszeniem praw osób, których dane dotyczą. Nie wydaje się, aby powyższe było jednak zamiarem ustawodawcy unijnego*. Nie mogę zgodzić się z cytowanym tu poglądem wskazanych autorów. Uważam, że sytuacja kształtuje się wręcz odwrotnie, niż wskazani autorzy przedkładają. W związku z tym trawestuję niżej cytat, tak by oddawał moje rozumienie zagadnienia, a następnie go uzupełniam. Uważam więc, że (początek trawestacji) ustawodawca unijny wskazał, że nie każde naruszenie danych osobowych związane jest z naruszeniem praw osób, których dane dotyczą, ponieważ to właśnie było zamiarem ustawodawcy unijnego. (Koniec trawestacji.) Należy pamiętać że naruszenie ochrony danych osobowych jest zdefiniowane w art 4 pkt 12 RODO. Naruszenie takie może mieć charakter pewnego zdarzenia i wtedy rzeczywiście można się zgodzić że naruszenie takie jest związane z naruszeniem praw osób, których dane dotyczą, jednak naruszenie takie może również mieć charakter zagrożenia takim zdarzeniem i wtedy, zależnie od tego, z jakim zdarzeniem mamy do czynienia, i zależnie od poziomu zagrożenia mamy raczej do czynienia nie tyle z naruszeniem praw osób, których dane dotyczą, a jedynie z zagrożeniem naruszeniem tych praw. Dla uniknięcia redundancji wywodu odsyłam do uwagi (*3.10. Art. 33 ust. 1 Uwaga 10. Naruszenie ochrony danych – zestawienie*).

Paweł Barta, M. Kawecki i P. Litwiński piszą dalej, że: *W ustawodawstwie UE oraz rzecznictwo TS nie dokonano bowiem dotychczas podziału naruszeń praw podstawowych, do jakich na podstawie*

[258] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 350.

art. 7 i 8 KPP należy ochrona danych osobowych, na naruszenia ingerujące w prawa i wolności osób, których dane dotyczą, i nie stanowiące takiej ingerencji. Uznaje się bowiem, że każde naruszenie praw podstawowych stanowi taką ingerencję[259]. Przede wszystkim oczywiste jest, że naruszenie praw podstawowych, o jakim piszą wskazani autorzy, stanowi naruszenie praw i wolności. Prawa podstawowe wymienione w KPP UE są po prostu prawami (i wolnościami, czy też służą ochronie wolności, co funkcjonalnie wychodzi na jedno).

Jeżeli więc prawa podstawowe zostają naruszone, to oczywiste jest, że naruszone zostają prawa i to nie żadne inne, a przecież te właśnie prawa podstawowe. Mam świadomość, że dopuszczam się tu swojego rodzaju „chodzenia w kółko" czy też, do pewnego stopnia, błędu samoodniesienia. Czynię to jednak świadomie, aby zwrócić uwagę, że naruszenie praw opatrzonych jakimś przymiotnikiem, w jakiś sposób doprecyzowanych, tu: praw podstawowych, skutkuje niczym innym jak właśnie naruszeniem tych praw. Nic dziwnego, że nie dokonano podziału naruszeń praw podstawowych na te, które naruszają prawa i wolności osób, których dane dotyczą i na te, które nie naruszają praw i wolności osób, których dane dotyczą. Podział taki byłby absurdalny, jeżeli prawa zostają naruszone, to zostają naruszone – piszę o tym w dwóch zdaniach powyżej.

Wskazany błąd samoodniesienia nie wynika jednak z treści RODO, przypominam bowiem, że na gruncie artykułu 33 RODO mamy najpierw do czynienia z naruszeniem ochrony danych osobowych, które zostało zdefiniowane w artykule 4 pkt 12 RODO i następnie musimy zastanowić się – już w konkretnej sytuacji – w konkretnym stanie faktycznym, czy to właśnie naruszenie ochrony danych osobowych skutkuje zagrożeniem dla praw i wolności osób, których dane osobowe dotyczą lub naruszeniem praw i wolności osób, których dane dotyczą. Jeżeli prawa i wolności zapisane w KPP UE zostają naruszone (a przynajmniej prawa i wolności zapisane art 7 i 8 KPP), to prawa i wolności zapisane w art 5 ust 1 RODO również zostaną naruszone. Szerzej piszę o tym w uwadze (*3.4. Art. 33 ust. 1 Uwaga 4. Prawa i wolności w RODO. Naruszenie łącznie z naruszeniem innych praw i wolności*), Należy jednak pamiętać, że owszem, jeżeli zostają naruszone prawa podstawowe (odpowiednie, dotyczące ochrony danych

[259] Ibidem.

osobowych), to zostają naruszone prawa (te właśnie) oraz niektóre prawa z art. 5 ust. 1 RODO. Możliwa jest jednak sytuacja i o takiej właśnie sytuacji stanowi art. 33 RODO, w której nastąpi naruszenie z art. 4 pkt 12 RODO, jednak naruszenie jakichkolwiek praw nastąpiło lub nie nastąpiło i to właśnie, czy ono nastąpiło, należy ocenić. Tego właśnie dotyczy art. 33 RODO. Ocenić i stosownie do wyniku tej oceny poinformować PUODO lub nie.

3.3. Art. 33 ust. 1 Uwaga 3

Prawa i wolności w RODO

Zarys zagadnień

Podstawowe zagadnienia dotyczące praw i wolności w RODO, sygnalizuję poniżej w punktach. Nie zamieszczam szczegółowych uzasadnień, wyżej wskazuję, gdzie uzasadnienia te się znajdują, w których miejscach książek mojego autorstwa.

– W kilku przepisach RODO mowa jest o prawach i wolnościach.
– O prawach i wolnościach mowa jest w art. 24 ust. 1 RODO, w art. 32 ust. 1 RODO w art. 33 ust. 1 RODO i w art 34 ust. 1 RODO oraz w innych przepisach.
– Ilekroć w RODO jest mowa o prawach i wolnościach, tylekroć mowa jest o tych samych prawach i wolnościach.
– Ilekroć w RODO jest mowa o prawach i wolnościach, tylekroć RODO odsyła do praw i wolności, o których jest mowa w samym RODO.
– W RODO występują, czy też zdefiniowane są prawa i wolności dwóch kategorii, a to prawa i wolności zasadnicze oraz prawa i wolności szczegółowe.
– Prawa i wolności zasadnicze zdefiniowane są w art 5 RODO.
– Prawa i wolności szczegółowe zdefiniowane są w przepisach szczegółowych RODO, czyli w przepisach od artykułu 6 RODO wzwyż, łącznie z artykułem 6 RODO.
– W art. 5 RODO zapisane są zasady dotyczące przetwarzania danych osobowych, należy jednak zwrócić uwagę na fakt, że przepis ten zaczyna się od słów: *Dane osobowe muszą być*. Wynika z tego, że zasady z art. 5 RODO są to obowiązki administratora i jednocześnie prawa osób, których dane dotyczą i jednocześnie są to wolności chronione przez system wskazanych praw i obowiązków.

3.4. Art. 33 ust. 1 Uwaga 4

Prawa i wolności w RODO

Naruszenie łącznie z naruszeniem innych praw i wolności

Jeśli chodzi o prawa i wolności z RODO, a zwłaszcza o prawa i wolności zasadnicze, zapisane w art. 5 ust. 1 RODO, to należy zwrócić na pewne doniosłe, ale i ciekawe zjawisko. Zjawisko to ma dwie odmiany.

– **Odmiana pierwsza** zachodzi, jeżeli ma miejsce naruszenie zdefiniowane w art. 4 pkt 12 RODO i jeżeli to naruszenie ma charakter wynikającego z przepisu zdarzenia (nie zaś zagrożenia takim zdarzeniem), to prawdopodobnie zawsze zostają naruszone niektóre prawa i wolności zapisane w art. 5 ust. 1 RODO. Nie jedynie zagrożone naruszeniem, ale właśnie naruszone.
– **Odmiana druga** zachodzi, jeżeli ma miejsce naruszenie zdefiniowane w art. 4 pkt 12 RODO i jeżeli to naruszenie ma charakter zagrożenia wynikającym z przepisu zdarzeniem (nie zaś samego właściwego już zdarzenia), to prawdopodobnie zawsze zostają zagrożone niektóre prawa i wolności zapisane w art. 5 ust. 1 RODO. Nie naruszone, ale zagrożone naruszeniem.

Obserwuję jeszcze jedno ciekawe zjawisko, analogiczne do opisanego. Otóż, jeżeli ma miejsce naruszenie zdefiniowane w art. 4 pkt 12 RODO i jednocześnie naruszenie to skutkuje naruszeniem praw i wolności z KPP UE lub z Konstytucji RP lub z EKPC, to prawdopodobnie zawsze naruszone zostają niektóre prawa i wolności z art. 5 ust. 1 RODO. Piszę o niektórych prawach i wolnościach, to które bowiem zostają naruszone, zależne jest od naruszenia z art. 4 pkt 12 RODO. Do zjawiska tego odnoszę się na końcu książki w tabeli: *Ryzyko naruszenia praw i wolności związane z zaistnieniem naruszenia ochrony danych osobowych*, umieszczonej w części: *Tabele pomocnicze. Zestawienia*.

Z uwagi na zjawiska opisane w niniejszym podrozdziale uważam, że art. 33 ust. 1 RODO powinien zostać tak znowelizowany, by nie było wątpliwości, jakie prawa i wolności należy brać pod uwagę przy dokonywaniu oceny ryzyka naruszenia tychże.

3.5. Art. 33 ust. 1 Uwaga 5

Prawa i wolności. Źródła inne niż RODO

Jak zatem widać, w RODO jest wskazane, jakie prawa i wolności administrator powinien brać pod uwagę za każdym razem, jak tylko RODO odsyła do „praw i wolności". Nic nie stoi na przeszkodzie, by administrator brał pod uwagę także inne prawa (i wolności). Wskazuję niżej, z jakich źródeł mogą one wynikać.

– z KPP UE,
– z EKPC,
– z Konstytucji RP.

Katalogi praw zamieszczam na końcu książki w części zatytułowanej *Tabele pomocnicze, zestawienia*. Analogiczne zestawienia znajdują się we wcześniejszych książkach, tu jednak ujmuję je w tabelach, w sposób uporządkowany. Ujęcie takie powinno ułatwić dokonywanie odpowiednich ocen przez tych administratorów, którzy zdecydowaliby się wiedzę na ten temat czerpać z niniejszej publikacji.

3.6. Art. 33 ust. 1 Uwaga 6

Prawa i wolności w EKPC

Wyżej w uwadze (*3.2. Art. 33 ust. 1 Uwaga 2. Prawa i wolności przy ocenie skutków naruszenia*) prowadzę dyskurs z W. Chomiczewskim. Wywodzę tam, że: *w KPP UE praw, związanych z ochroną danych osobowych, jest dziesięć, w EKPC są dwa, w Konstytucji jest jedno*. Poniżej, na następnej stronie, wymieniam prawa, które wynikają z EKPC i wskazuję poprzez pogrubienie czcionki te prawa, które uważam za związane z ochroną danych osobowych na tyle, że należy je brać pod uwagę tam, gdzie w RODO prawodawca nakazuje brać pod uwagę prawa i wolności, a administrator czuje niedosyt, korzystając jedynie z RODO.

1. Prawo do przestrzegania praw człowieka (Art. 1 EKPC).
2. Prawo człowieka do życia (Art. 2 EKPC).
3. Prawo człowieka do niebycia poddanym torturom ani nieludzkiemu lub poniżającemu traktowaniu albo karaniu (Art. 3 EKPC).
4. Prawo człowieka do niebycia trzymany w niewoli lub w poddaństwie (Art. 4 EKPC).

5. Prawo człowieka do niebycia zmuszonym do świadczenia pracy przymusowej lub
6. Prawo człowieka do wolności i bezpieczeństwa osobistego (Art. 5 EKPC).
7. Prawo człowieka do rzetelnego procesu sądowego (Art. 6 EKPC).
8. Prawo człowieka do niebycia karanym bez podstawy prawnej (Art. 7 EKPC).
9. **Prawo człowieka do poszanowania życia prywatnego i rodzinnego (Art. 8 EKPC).**
10. Prawo człowieka do wolności myśli, sumienia i wyznania (Art. 9 EKPC).
11. Prawo człowieka do wolności wyrażania opinii (Art. 10 EKPC).
12. Prawo człowieka do wolności zgromadzania się i stowarzyszania się (Art. 11 EKPC).
13. Prawo człowieka do zawarcia małżeństwa (Art. 12 EKPC).
14. Prawo człowieka do skutecznego środka odwoławczego. (Art. 13 EKPC).
15. **Prawo człowieka do niebycia dyskryminowanym (Art. 14 EKPC).**
16. Prawo człowieka do uchylania stosowania zobowiązań w stanie niebezpieczeństwa publicznego (Art. 15 EKPC).
17. Prawo człowieka będącego cudzoziemcem, by jego działalność polityczna nie była ograniczana (Art. 16 EKPC).
18. Prawo człowieka do tego. by żadne z postanowień EKPC nie było interpretowane jako przyznanie jakiemukolwiek państwu, grupie lub osobie prawa do podjęcia działań lub dokonania aktu zmierzającego do zniweczenia praw i wolności wymienionych w EKPC konwencji albo ich ograniczenia w większym stopniu, niż to przewiduje EKPC (Art. 17 EKPC).
19. Prawo człowieka to tego, by ograniczenia praw i wolności, na które zezwala EKPC konwencja, nie były stosowane w innych celach niż te, dla których je wprowadzono (Art. 18 EKPC).

3.7. Art. 33 ust. 1 Uwaga 7

Prawa i wolności w KPP UE

Wyżej w uwadze (*3.2. Art. 33 ust. 1 Uwaga 2. Prawa i wolności przy ocenie skutków naruszenia*) wspominam o prawach i wolnościach, które zapisane są w KPP UE. Jako konsekwencję tamtej wzmianki, poniżej zamieszczam dziesięć praw z KPP UE, które w jakiś sposób związane są z ochroną danych osobowych, z ochroną prywatności. Wspomniany akt prawny „zawiera" około 152 praw człowieka. Nie wymieniam ich wszystkich w wywodzie głównym ani w zestawieniach na końcu książki, uważam, bowiem, że jest to niecelowe. Prawa te, na podstawie przepisów KPP UE, sformułowałem i wymieniłem prawdopodobnie wszystkie w książce *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje.* (s. 126–143).

1. Prawo człowieka do poszanowania życia prywatnego i rodzinnego (Art. 7 KPP UE).
2. Prawo człowieka do poszanowania domu (Art. 7 KPP UE).
3. Prawo człowieka do poszanowania komunikowania się (Art. 7 KPP UE).
4. Prawo człowieka do ochrony danych osobowych które go dotyczą (Art. 8 ust. 1 KPP UE).
5. Prawo człowieka do przetwarzania danych osobowych w sposób rzetelny (Art. 8 ust. 2 KPP UE).
6. Prawo człowieka do przetwarzania danych osobowych w określonych celach (Art. 8 ust. 2 KPP UE).
7. Prawo człowieka do przetwarzania danych osobowych za zgodą osoby, której dane dotyczą (Art. 8 ust. 2 KPP UE).
8. Prawo człowieka do przetwarzania danych osobowych oparte na innej niż zgoda uzasadniona podstawę prawną przewidzianą ustawą (Art. 8 ust. 2 KPP UE).
9. Prawo człowieka do dostępu do zebranych danych osobowych, które go dotyczą (Art. 8 ust. 2 KPP UE).
10. Prawo człowieka do dokonania sprostowania danych osobowych, które go dotyczą (Art. 8 ust. 2 KPP UE).

3.8. Art. 33 ust. 1 Uwaga 8

Naruszenie praw lub wolności jednej osoby fizycznej

Analiza art. 33 ust. 1 RODO wskazuje, że należy zgłaszać naruszenie, o ile jest prawdopodobne, że skutkowało ono naruszeniem praw lub wolności osób fizycznych. Zwracam uwagę na zwrot: „osób fizycznych", zwrot ten odnosi się do osób, czyli do liczby mnogiej rzeczownika „osoba". Jedna osoba, to nie są osoby, jedna osoba jest jedna. Skoro prawodawca stanowi o osobach, to znaczy, że o co najmniej dwóch osobach. Przepisy prawa nie mają charakteru metaforycznego. Znaczą to, co znaczą i jeżeli prawodawca pisze w przepisie o więcej niż jednej osobie, ponieważ pisze o osobach, to rozumieć to, co prawodawca pisze, należy zgodnie z tym, co on pisze, że w przepisie nie jest mowa o osobie, a o osobach co najmniej dwóch. Jeżeli zatem naruszenie dotyczy praw lub wolności osoby fizycznej, to naruszenie takie nie podlega zgłoszeniu. Nie wiemy oczywiście, jak zareagowałby PUODO, oficjalnych wypowiedzi przedstawicieli organu w tej sprawie próżno szukać. Analiza „kazusu Morele" wskazuje, że samodenuncjacja skutkować może ukaraniem i to ogromną karą[260]. Nie mogę nie zwrócić uwagi, że ukaranie drakońską karą podmiotu, który był ofiarą ataku, po czym praworządnie zgłosił naruszenie do PUODO jest dewastujące dla stosowania RODO. Jeżeli takich zdarzeń będzie więcej, to ogół administratorów danych osobowych będzie wiedział, że lepiej jest ukryć naruszenie, licząc, że pozostanie ono ukryte i złamać w ten sposób prawo, niż być prawu posłusznym i zgłosić naruszenie, po czym płacić gigantyczną karę i płakać gorzko nad swą praworządnością.

Nie namawiam bynajmniej do łamania prawa i niezgłaszania naruszeń, które zgłaszać należy, zwracam jednak uwagę, że art. 33 ust. 1 RODO każe zgłaszać naruszenia praw lub wolności co najmniej dwóch osób fizycznych. Daje to zatem administratorowi pretekst do niezgłaszania naruszenia, jeżeli owo dotyczy praw i wolności jednej tylko osoby fizycznej.

Podmioty publiczne nie powinny zgłaszać naruszeń praw lub wolności jednej osoby, zgłoszenie samo w sobie nie jest niczym złym, co najwyżej niepotrzebnym, naraża jednak na kontrole i ukaranie karą administracyjną, a te w Polsce są wysokie.

---

[260] Por. P. Fajgielski, *Prawo ochrony danych osobowych*…, s. 16.

Podmiotom publicznym nie wolno jest zgłaszać naruszeń praw lub wolności jednej osoby, zgłoszenie takie jest naruszeniem Konstytucji. Podmiot publiczny, który zgłasza naruszenie praw i wolności jednej osoby, narusza nakaz działania na podstawie i w granicach prawa, jak się wydaje zwłaszcza w zakresie nakazu działania na podstawie prawa.

Administrator powinien mieć na uwadze powyższe ustalenia, ponieważ pozwalają mu one podjąć decyzję. Jeżeli przyjmiemy, że zaszło zdarzenie, które podlegałoby zgłoszeniu, gdyby naruszone były prawa i wolności więcej niż jednej osoby fizycznej, jednak dotyczy ono jednej osoby fizycznej, to administrator powinien rozważyć wymienione poniżej możliwości.

– Administrator nie zgłasza naruszenia, zakładając, że PUODO się o naruszeniu nie dowie i że osoba, której dane dotyczą, się nie dowie. Jest to podejście nieco beztroskie, administrator ryzykuje karę administracyjną za niezgłoszenie naruszenia, ale jednocześnie nikt o owym naruszeniu nie wie. PUODO może powziąć wiedzę o naruszeniu przy okazji kontroli, kiedy zapozna się z dokumentacją, którą administrator sporządził na podstawie art. 33 ust. 5 RODO.
– Administrator nie zgłasza naruszenia, dokonuje przy tym ustaleń, że dotyczyło ono praw i wolności jednej osoby fizycznej, odnotowuje to i odnotowuje, że nie zgłosił naruszenia właśnie dlatego, że dotyczyło ono praw i wolności jednej osoby, podczas gdy zgłasza się naruszenia dotyczące praw i wolności więcej niż jednej osoby, więc zgłoszenie tego naruszenia byłoby naruszeniem RODO, być może nawet nadającym się do ukarania. Wydaje się to dziwaczne, ale należy pamiętać, że obowiązek zgłoszenia jest lub go nie ma – zależnie od stanu faktycznego i zależnie od przyjętej interpretacji stanu prawnego. Jeżeli obowiązku nie ma i jednocześnie administrator zgłasza naruszenie, to tym samym administrator narusza RODO. Jest to rozumowanie odważne, jednak uważam, że w pełni uzasadnione. Może okazać się ryzykowne, jeżeli PUODO i sąd go nie podzielą, ale to już nieco inna sprawa.
– Administrator zgłasza naruszenie, wie, że nie powinien, ponieważ dotyczy ono praw i wolności jednej tylko osoby. Administrator uważa, że bezpieczniej jest zgłosić naruszenie, niż tego nie uczynić. Rozumowanie to wydaje się poprawne, z jednym jednak

zastrzeżeniem. Otóż kiedy administrator zgłasza naruszenie, to PUODO się tym samym o tym naruszeniu dowiaduje, co może skutkować nałożeniem kary lub kontrolą, która z kolei może doprowadzić do wykrycia innych naruszeń i nałożeniem kary.

Nie lubię pozostawiać rozważań **bez podsumowania**, mam jednak świadomość, że poczynione tu podsumowanie może zostać potraktowane przez czytelników jak sugestia działania. Z tego względu, w tym miejscu wyjątkowo powstrzymam się od podsumowywania. Możliwe drogi postępowania zaprezentowałem, decyzję musi podjąć administrator.

Pomimo powyższego podsumowania, czynię niżej jeszcze pewne uzupełniające uwagi.

Jestem w stanie wyobrazić sobie zarzut, zgodnie z którym słowa *praw lub wolności osób fizycznych* mają charakter zwrotu frazeologicznego, którego prawodawca użył, mimo iż intencją prawodawcy było odniesienie się zarówno do praw i wolności „osób" fizycznych, jak i do praw i wolności „osoby" fizycznej. Jestem w stanie sobie zarzut taki wyobrazić, mogę jednak na niego bardzo łatwo odpowiedzieć. Otóż w RODO prawodawca nieraz wypowiada się na temat nie „osób fizycznych", ale „osoby fizycznej" i czyni to – co podkreślam – nie tylko w polskiej wersji językowej. W tekście RODO mowa jest o „osobie fizycznej" co najmniej nieco ponad 50 razy. Obliczenie to daje podobny wynik na gruncie wersji anglojęzycznej i czeskojęzycznej. Wyniki są tu przybliżone, ponieważ wskutek niekompetencji tłumacza czasem osoba fizyczna jest odpowiednikiem „a natural person", czasem jednak też niestety jest odpowiednikiem „a data subject". Mimo pewnych niekonsekwencji translatorskich, mowa jest w RODO o „osobie fizycznej" kilkadziesiąt razy i bez względu na wersję językową. Jak więc widać, prawodawca zapewne intencjonalnie posługuje się liczbą pojedynczą i liczbą mnogą słowa „osoba", nie widzę zatem powodu, by uznać, że jedynie w art. 33 i w art. 34 RODO prawodawca użył słów o osobach (liczba mnoga) fizycznych, w sposób przypadkowy i niedbały.

Na marginesie prowadzonych rozważań pragnę zwrócić uwagę, że również Preambuła RODO zawiera elementy, z których – jak uważam – wynika, że art. 33 RODO (a uprzedzając, powiedzmy, że i art. 34 RODO) dotyczy naruszenia praw i wolności więcej niż jednej osoby fizycznej. Podstawowe rozumowanie, które wynika z art. 33

RODO, znajduje się wyżej. Analogiczne rozumowanie może być poprowadzone w odniesieniu do art. 34 RODO. W związku z tym, poniżej jedynie wskazuję argumenty przemawiające za poglądem o braku obowiązku zgłaszania naruszeń, które dotyczą danych osobowych jednej osoby fizycznej. Zwracam jednocześnie uwagę, że wskazane poniżej fragmenty wskazują – jak uważam – na fakt, że prawodawca posługuje się w RODO liczbą mnogą i liczbą pojedynczą słowa „osoba" w sposób świadomy.

W motywie 85 Preambuły RODO czytamy m.in.: *Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować* ***ryzyko naruszenia praw lub wolności osób fizycznych***. Czyli administrator zgłasza naruszenie organowi, jeżeli naruszenie *mogło powodować* ***ryzyko naruszenia praw lub wolności osób fizycznych***[261]. Jak widzimy, obecna jest tu liczba mnoga. Idźmy jednak dalej.

W motywie 86 Preambuły RODO czytamy m.in.: *Administrator powinien bez zbędnej zwłoki* ***poinformować osobę****, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować* ***wysokie ryzyko*** *naruszenia praw lub wolności tej osoby, tak aby umożliwić* ***tej osobie*** *podjęcie niezbędnych działań zapobiegawczych*. Jak zatem widać, w sytuacji wysokiego ryzyka administrator informuje „osobę".

Podsumowując należy stwierdzić, że lektura wskazanych przepisów preambuły nasuwa wniosek, że jeżeli ryzyko naruszenia praw i wolności jest wysokie, to administrator informuje nawet jedną osobę, której dane dotyczą, więc naruszenie może dotyczyć danych jednej osoby fizycznej, by obowiązek informowania tej osoby istniał. Jeżeli jednak ryzyko naruszenia jest średnie i dotyczy praw i wolności jednej tylko osoby, to administrator o takim ryzyku nie informuje PUODO. Rozumowania nie prowadzę dalej, wnioski znajdują się wyżej, pod rozumowaniem głównym, to jest poboczne.

---

[261] Pogrubienia: J. Rzymowski.

Ślad rozważań tego problemu znajduję u W. Chomiczewskiego. Autor ten zrazu pisze: *Pomimo zaistnienia naruszenia ochrony danych osobowych, administrator* ***nie musi*** *dokonywać zgłoszenia,* ***jeżeli jest mało prawdopodobne, by skutkowało ono ryzykiem naruszenia praw lub wolności osób fizycznych***[262]. I dalej, co niezwykle ciekawe, wspomniany autor pisze, że: *Oceny, czy występuje ryzyko naruszenia praw lub wolności człowieka, musi dokonać administrator**[263]. Prawdopodobnie przeskok z „osób fizycznych" na „człowieka" nie jest przypadkowy i sprawia wrażenie pewnego uniku. Może jednak się mylę, dalej bowiem czytamy, że: *W toku dokonywania oceny, czy występują ryzyka ich naruszenia , administrator powinien brać pod uwagę wszelkie możliwe szkody, jak i krzywdy, które mogą wyniknąć z danego zdarzenia dla osób fizycznych**[264].

Zacytowane zdania W. Chomiczewskiego wymagają pewnego komentarza. Otóż niepokoi nieco zwrot *administrator* ***nie musi*** *dokonywać zgłoszenia*, sugeruje on bowiem (takie mam przynajmniej wrażenie), że o ile administrator nie musi zgłoszenia dokonywać, to może to uczynić. Zwracam uwagę, że zgłoszenie takie jest bezprzedmiotowe. O ile podmiot prywatny rzeczywiście może zgłoszenia dokonać, nie ma bowiem przepisu zakazującego takiego działania, o tyle podmiotowi publicznemu nie wolno.

Kontrowersyjny, ale warty odnotowania pogląd dostrzegam u M. Gumularza i T. Izydorczyka. Otóż piszą oni, że: *Oprócz praw lub wolności osób, których dane dotyczą, RODO posługuje się także pojęciem praw lub wolności innych. Przykładowo zgodnie z art. 15 ust. 4 RODO, prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych*[265]. Faktem jest, że w art. 15 ust. 4 RODO znajdujemy słowa, do których odnoszą się wskazani autorzy. Ja z cytowanych słów wnoszę, że mowa jest w

---

[262] W. Chomiczewski, op. cit., s. 711 (wytłuszczenia W. Chomiczewskiego).

[263] Ibidem. Gwiazdką (*) oznaczam miejsce przypisu umieszczonego u W. Chomiczewskiego: „J.M.Grages, [w:] *Kommentar zur BDSG und zur DSGVO*…, red. K.U. Plath, 2016, s.1153".

[264] Ibidem, s. 712. Gwiazdką (*) oznaczam miejsce przypisu umieszczonego u W. Chomiczewskiego: „S.Jandt, [w:] *DS.–GVO*..., red. J. Kühling, B. Buchner, s. 617; Reif, [w:] *DS.–GVO*..., red. P. Gola, s. 496".

[265] M. Gumularz, T. Izydorczyk, op. cit., s. 50–51.

przepisie o prawach i wolnościach osób innych niż osoba, której dane dotyczą, czyli, zważywszy na kontekst sformułowania, mowa jest tam o prawa i wolnościach osób, których dane dotyczą, które to osoby są inne od osoby, która realizuje swoje prawa na gruncie art. 15 RODO.

Przekładając rzecz na przykład, jeżeli osoba, której dane dotyczą. żąda udostępnienia kopii danych, które jej dotyczą, to w związku z tym udostępnianiem nie mogą zostać jej udostępnione kopie danych innych osób, których dane osobowe przetwarza dany administrator. Tak właśnie rozumiem przepis, do którego odnosi się cytat. Oczywiście nie musi tu chodzić tylko o ujawnienie danych dotyczących innych osób, ale również o ich zniszczenie i o inne niepożądane zdarzenia. Powiedzmy, że do tego miejsca to, co uważam zgadza się z tym, co piszą M. Gumularz i T. Izydorczyk. Dalej jednak nabieram wątpliwości. Zrazu wskazaniu autorzy piszą: *Użycie pojęcia innych wskazuje, że chodzi o podmioty inne niż osoba, której dane dotyczą (której dane są przetwarzane)*[266]. Tu mój niepokój nie jest wielki, ale jednak niepokoi mnie, że autorzy po pierwsze, piszą o innych podmiotach, po drugie, że nie zwracają uwagi na fakt, że przepis odnosi się (jak ja go rozumiem) do innych osób, których dane są przetwarzane. Ostatnie zdanie wywodu cytowanych autorów pogłębia niestety mój niepokój. Piszą oni: *Nie muszą to być wyłącznie osoby fizyczne, o czym świadczy motyw 63 RODO*[267].

Lektura motywu 63 Preambuły RODO absolutnie nie świadczy o tym, o czym miałaby zdaniem wskazanych autorów świadczyć. Nie chcę tu analizować tego motywu, jednak wniosek z jego lektury przedstawiłem. Niestety, jest coś jeszcze do powiedzenia na temat słowa „innych" w art. 15 ust. 4 RODO. Otóż w polskiej wersji językowej rzeczywiście widnieje „innych", jednak w wersji angielskiej widzimy: „laws and freedom of others". Nie chcę tu prowadzić dyskusji słownikowej, bo może ona wieść na manowce, odnotujmy tylko brzmienie wersji angielskiej. W wersji niemieckiej widzimy: „die Rechte und Freiheiten anderer Personen". W tej wersji językowej widzimy już osoby (*Personen*). Osoby prawne to byłoby raczej „juristiche Personen". W wersji czeskiej widnieje: „práva a svobody jiných osob", czego tłumaczyć nie trzeba. Z kolei w wersji słowackiej czytamy:

[266] Ibidem, s. 51.

[267] Ibidem.

„práva a slobody iných" i w wersji chorwackiej czytamy: „prava i slobode drugih". Jak widać, wersje językowe i tu nie są spójne. Czytając przedstawione wersje językowe RODO, mam poczucie, że w art. 15 ust. 4 RODO mowa jest o prawach i wolnościach osób fizycznych. Stanowisko M. Gumularza i T. Izydorczyka rozumiem, jednak – jak piszę wyżej – niepokoi mnie ono i co tu dodaję, zdecydowanie go nie podzielam. Nie podzielam też stanowiska, jakoby z motywu 63 RODO wynikało poparcie dla tezy, jakoby w art. 15 ust. 4 RODO była mowa nie tylko o osobach fizycznych. Mając na uwadze powyższe, zwracam uwagę, że o ile można się spierać, czy w art. 15 ust. 4 RODO prawodawca odnosi się do praw i wolności tylko osób fizycznych czy również osób prawnych (choć uważam taki spór za niepotrzebny), ale podkreślenia wymaga (i tu już nie widzę miejsca na spory), że RODO chroni przede wszystkim prawa i wolności osób, których dane dotyczą.

3.9. Art. 33 ust. 1 Uwaga 9

Incydent

Bywa, że czytając o RODO, napotykamy na pojęcie incydentu. Podkreślenia wymaga, że incydent jest pojęciem spoza RODO, które – jak wynika z mojej praktyki (nie mam tu konkretnych badań) – bywa wykorzystywane do pozornego łagodzenia rygorów wynikających z art. 33 RODO i z art. 34 RODO. Bywa, że administratorzy stwierdzają, że zaszło zdarzenie opisane w art. 4 pkt. 12 RODO, czyli naruszenie ochrony danych osobowych, jednak nazywają je incydentem, a następnie bądź to nie kwalifikują owego incydentu jako naruszenia – więc nie muszą oceniać ryzyka naruszenia praw i wolności, bądź to tak oceniają ryzyko naruszenia praw i wolności, by uzyskać wynik, który w ich mniemaniu jest korzystny, czyli wynik, który nie zmusza np. do zgłoszenia naruszenia do PUODO. Oczywiste jest, że ocenę ryzyka naruszenia praw i wolności administrator zawsze może wykonać niewłaściwie, niezależnie od tego, czy robi tak z niewiedzy czy z niewłaściwie rozumianej przebiegłości.

Przykładem opowieści o incydencie są rozważania zawarte w artykule M. Mazura[268]. Autor ten pisze, że: *Każde naruszenie ochrony danych osobowych jest incydentem, ale nie każdy incydent stanowi naruszenie przepisów o ochronie danych osobowych*. Wcześniej ten sam autor pisze, że: *Naruszenie stanowi zatem rodzaj zdarzenia zagrażającego bezpieczeństwu, przy czym nie każde takie zdarzenie stanowi naruszenie ochrony danych osobowych*. Jeszcze wcześniej, w tym samym artykule autor definiuje naruszenie ochrony danych osobowych. Mamy zatem naruszenie ochrony danych osobowych – jest ono zdefiniowane w art. 4 pkt 12 ROODO. Naruszenie to rodzaj zdarzenia zagrażającego bezpieczeństwu. (Nie wiemy, jakie naruszenie, bo autor pozbawił je części nazwy, ale prawdopodobnie chodzi nadal o naruszenie z art. 4 pkt 12 RODO.) Następnie dowiadujemy się, że to naruszenie, które jest zdarzeniem zagrażającym bezpieczeństwu, nie zawsze jest naruszeniem ochrony danych osobowych (dokładnie: nie każde takie naruszenie stanowi naruszenie ochrony danych osobowych). Dalej autor wplata zacytowaną wyżej myśl o incydencie. Odnosząc się ekstremalnie przychylnie, można tak zinterpretować słowa M. Mazura, że mają one sens, ale mówiąc szczerze, przejrzyste owe słowa nie są.

Należy stwierdzić jednoznacznie, że sprawy opisane przez M. Mazura mają się tak, jak opisuję poniżej.

– Zachodzi zdarzenie.
– Administrator ustala, czy zdarzenie realizuje warunki naruszenia ochrony danych osobowych z art. 4 pkt 12 RODO.
– Jeżeli zdarzenie nie realizuje warunków naruszenia ochrony danych osobowych z art. 4 pkt 12 RODO, to administrator na tym kończy ocenianie zdarzenia.
– Jeżeli zdarzenie realizuje warunki naruszenia ochrony danych osobowych z art. 4 pkt 12 RODO, to administrator przystępuje do oceny ryzyka naruszenia praw i wolności osób fizycznych.
– Jeżeli jest *mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych* (art. 33 ust. 1 RODO), to administrator nie informuje nikogo.

[268] M. Mazur, *Zgłaszanie naruszeń ochrony danych*. „ABI Expert" 2018, 3(8), s. 22–23.

– Jeżeli jest *prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych* (art. 33 ust. 1 RODO), to administrator informuje PUODO.
– Jeżeli naruszenie *może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych* (art. 33 ust. 1 RODO), to *administrator […] zawiadamia osobę, której dane dotyczą […]* i administrator informuje PUODO.
– Jeżeli naruszenie ochrony danych osobowych skutkuje naruszeniem praw i wolności osób fizycznych, to administrator zawiadamia osobę, której dane dotyczą i administrator informuje PUODO.

Jak widać, pojęcie incydentu nie jest potrzebne do dokonania analizy zdarzenia na gruncie art. 33 RODO i na gruncie art. 34 RODO, przy świadomości treści art. 4 pkt. 12 RODO.

Lektura wspomnianego wyżej artykułu M. Mazura dostarcza wielu atrakcji. Wyżej opisałem pierwszą z nich, związaną z pojęciem incydentu. Niestety, dalej autor rozwija swoje imaginacyjne opowieści. Jak opisałem w poprzedniej uwadze, od poziomu ryzyka naruszenia praw i wolności osób fizycznych zależy, czy naruszenie to zostanie tajemnicą administratora, czy zostanie o nim poinformowane PUODO, czy osoby, których dane dotyczą i PUODO. Administrator musi zatem wiedzieć, jakie prawa i wolności brać pod uwagę przy ocenie naruszenia.

Michał Mazur pisze[269] o tym następująco: *Ryzyko naruszenia praw i wolności istnieje, gdy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono*. Zdanie tu przytoczone nieco niepokoi, połowa bowiem zdania traktuje o prawach i wolnościach, a druga połowa o szkodach, ale czytajmy dalej: *Przykładem takich szkód jest dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, naruszenie dobrego imienia czy strata finansowa […]* Dalej M. Mazur powołuje się na stanowisko Grupy Roboczej art. 29. Tu niepokój przekształca się w pewność, że cytowany autor nie do końca wie, o czym pisze. Wskazane przezeń zdarzenia, czyli szkody, dyskryminacja itd., to nie są prawa i wolności. To są możliwe konsekwencje naruszenia ochrony danych osobowych, o których czytamy w art. 33 ust. 3 lit. c RODO.

[269] Ibidem.

Podkreślenia wymaga, że w przypadku zaistnienia zdarzenia z art. 4 pkt 12 RODO należy oceniać ryzyko naruszenia praw i wolności, a nie ryzyko tego, czy zdarzenie będzie miało niekorzystne skutki dla osoby, której dane dotyczą. Odnoszę się tak szeroko do imaginacji M. Mazura, ponieważ jest on przedstawiony pod artykułem jako p.o. zastępcy dyrektora Zespołu Współpracy z Administratorami Danych w Urzędzie Ochrony Danych Osobowych. Artykuł pochodzi z roku 2018, nie wiem, kim dziś (koniec 2021 roku) jest jego autor, jednak należy podkreślić, że jego tok rozumowania jest mylny, niezależnie od faktu pracy w UODO.

O incydencie (bezpieczeństwa) wspomniano też w oficjalnym dokumencie Grupy Roboczej art. 29. Autorzy dokumentu poprawnie, choć nieco mętnie, wywodzą na temat naruszenia (sic!) naruszenia ochrony danych osobowych, incydentu. Niestety w wywodach tych znajduje się zdanie: *[...] choć wszystkie przypadki naruszenia ochrony danych osobowych są incydentami bezpieczeństwa, nie wszystkie incydenty bezpieczeństwa muszą wiązać się z naruszeniem ochrony danych osobowych [...]*[270]. Zdanie to jest trafne, jeżeli jednak przeczyta je ktoś, kto nie do końca rozumie, czym jest naruszenie ochrony danych osobowych, to może go to doprowadzić do popełnienia wskazanych w niniejszym podrozdziale błędów interpretacyjnych.

Na temat incydentu wypowiadają się w komentarzu do art. 32 RODO P. Barta, M. Kawecki i P. Litwiński[271]. Przede wszystkim określają oni incydent mianem *incydentu fizycznego lub technicznego*. Dalej piszą, że RODO takowych incydentów nie definiuje, z czym się zgadzam. Wskazani autorzy definiują zatem *incydent fizyczny lub techniczny* jako *naruszenie fizycznej lub technicznej ochrony danych (jako efektu zastosowanych odpowiednio środków organizacyjnych i technicznych, o których mowa w komentowanym przepisie), ich integralności i/lub poufności – środki techniczne i organizacyjne zapewniały zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich*. Cenię autorów definiujących pojęcia, sam staram się też czasem to czynić. Pojęcie zdefiniowane, zdefiniowane ostrożnie,

[270] Grupa Robocza art. 29, *Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679*. Przyjęte w dniu 3 października 2017 r. Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r. 18/PL WP250 rev.01, s. 8.

[271] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 345.

zdefiniowane trafnie to pojęcie zrozumiane. Wskazani autorzy podjęli ryzyko zdefiniowania incydentu i chyba czegoś nie zauważyli. Po pierwsze, piszą o środkach technicznych i organizacyjnych, uważając je (chyba) za pojęcia jasne, bo pojęć tych po prostu używają. Dla mnie pojęcia te jasne nie są. Piszę o tym wyżej, choćby w (*6.2. Art. 32 ust. 1 i 2 i 3 Postulat 2. Uczytelnienie przepisu*). Dalej, niestety, wskazani autorzy potykają się tak, jak uważam, że (w odniesieniu to środków technicznych i organizacyjnych) potknął się prawodawca, a mianowicie piszą oni o *fizycznej lub technicznej* ochronie danych. Jak je odróżnić? Nie wiem. Tym niemniej głos P. Barty, M. Kaweckiego i P. Litwińskiego są ciekawym i doniosłym głosem w niepotrzebnej dyskusji nad pojęciem incydentu, w której to dyskusji i ja w niniejszej książce stanowisko zajmuję.

Nad zjawiskiem incydentu pochyla się również C. Burton. Zwraca on uwagę na to, że[272] należy przeprowadzić rozróżnienie między naruszeniami ochrony danych osobowych, które dotyczą danych osobowych i incydentami bezpieczeństwa, które mogą nie dotyczyć danych osobowych.

3.10. Art. 33 ust. 1 Uwaga 10

Naruszenie ochrony danych osobowych – zestawienie

Pojęcie naruszenia ochrony danych jest kluczowe dla rozważanych tu zagadnień związanych ze zgłoszeniem tegoż naruszenia do PUODO. Niżej wymieniam zdarzenia, które mają charakter naruszenia. Szczegółowa analiza tych zdarzeń, a właściwie rozważania, które doprowadziły do sformułowania ich nazw, prowadzę w książce *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*. Łódź. 2020[273], do której odsyłam. Zwracam przy tym uwagę, że we wskazanej książce wymieniłem 45 takich zdarzeń. W istocie zdarzeń takich jest 90, należy bowiem brać pod uwagę zdarzenie i zagrożenie tymże.

Z uwagi na fakt, że niniejsza książka skierowana jest między innymi do praktyków, niżej wymieniam zdarzenia, które – jeżeli mają miejsce – to należy je zakwalifikować jako naruszenie. Administrator,

---

[272] C. Burton, op. cit., s. 659.

[273] J. Rzymowski, *RODO – GDPR. Przedmiot i cele...*

który zastanawia się, czy zdarzenie jest naruszeniem z art. 4 pkt 12 RODO, może po prostu przeczytać zamieszczoną poniżej listę i sprawdzić, czy zdarzenie które miało miejsce, jest tożsame z którymkolwiek ze zdarzeń z listy zamieszczonej poniżej. Jeżeli jest tożsame, to zdarzenie takie jest naruszeniem na gruncie art. 4 pkt 12 RODO i należy następnie przystąpić do dokonywania oceny ryzyka naruszenia praw i wolności na gruncie art. 33 RODO i art. 34 RODO.

Możliwa jest też inna metoda, oparta na zadawaniu kolejnych pytań, prezentuję ją niżej, w uwadze (*3.10. Art. 33 ust. 1 Uwaga 10. Naruszenie ochrony danych osobowych – metoda ustalenia*).

Zdarzenia, których zaistnienie oznacza,
że miało miejsce naruszenie ochrony danych osobowych

1. Przypadkowe zniszczenie danych osobowych przesyłanych. (Raczej przesyłanych przez administratora lub podmiot przetwarzający, nie do administratora lub podmiotu przetwarzającego, nie jest to jednak pewne.)
2. Zagrożenie przypadkowym zniszczeniem danych osobowych przesyłanych. (Raczej przesyłanych przez administratora lub podmiot przetwarzający, nie do administratora lub podmiotu przetwarzającego, nie jest to jednak pewne.)
3. Przypadkowe zniszczenie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
4. Zagrożenie przypadkowym zniszczeniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
5. Przypadkowe zniszczenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
6. Zagrożenie przypadkowym zniszczeniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
7. Przypadkowe utracenie danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
8. Zagrożenie przypadkowym utraceniem danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
9. Przypadkowe utracenie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.

10. Zagrożenie przypadkowym utraceniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
11. Przypadkowe utracenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
12. Zagrożenie przypadkowym utraceniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
13. Przypadkowe zmodyfikowanie danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
14. Zagrożenie przypadkowym zmodyfikowaniem danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
15. Przypadkowe zmodyfikowanie danych osobowych, które są przechowywane przez administratora lub podmiot przetwarzający.
16. Zagrożenie. przypadkowym zmodyfikowaniem danych osobowych przechowywanych przez administratora lub podmiot przetwarzający.
17. Przypadkowe zmodyfikowanie danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający, w sposób inny niż przesyłanie lub przechowywanie.
18. Zagrożenie przypadkowym zmodyfikowaniem danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
19. Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych. Przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
20. Zagrożenie przypadkowym i nieuprawnionym ujawnieniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
21. Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
22. Zagrożenie przypadkowym i nieuprawnionym ujawnieniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
23. Przypadkowe i nieuprawnione ujawnienie danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający, w sposób inny niż przez przesyłanie lub przechowywanie.

24. Zagrożenie przypadkowym i nieuprawnionym ujawnieniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający, w sposób inny niż przez przesyłanie lub przechowywanie.
25. Przypadkowy i nieuprawniony dostęp do danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
26. Zagrożenie przypadkowym i nieuprawnionym dostępem do danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
27. Przypadkowy i nieuprawniony dostęp do danych osobowych danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
28. Zagrożenie przypadkowym i nieuprawnionym dostępem do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
29. Przypadkowy i nieuprawniony dostęp do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie, czyli które są w jakikolwiek sposób (z uwzględnieniem zawartego w przepisie wyłączenia) przetwarzane.
30. Zagrożenie przypadkowym i nieuprawnionym dostępem do danych osobowych przetwarzanych w sposób inny niż przez przesyłanie lub przechowywanie przez administratora lub przez podmiot przetwarzający
31. Niezgodne z prawem zniszczenie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający. Naruszenie może mieć miejsce zwłaszcza podczas samego transferu danych osobowych między administratorem (podmiotem przetwarzającym) – nadawcą a adresatem.
32. Zagrożenie niezgodnym z prawem zniszczeniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
33. Niezgodne z prawem zniszczenie danych osobowych, przechowywanych przez administratora lub przez podmiot przetwarzający.

34. Zagrożenie niezgodnym z prawem zniszczeniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
35. Niezgodne z prawem zniszczenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
36. Zagrożenie niezgodnym z prawem zniszczeniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
37. Niezgodne z prawem utracenie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający. Utracenie należy utożsamiać z zagubieniem, wydaje się, że z zagubieniem podczas transferu, transportu, przesyłania.
38. Zagrożenie niezgodnym z prawem utraceniem danych osobowych przesyłanych do administratora od administratora przez administratora do podmiotu przetwarzającego od podmiotu przetwarzającego przez podmiot przetwarzający.
39. Niezgodne z prawem utracenie danych osobowych przechowywanych przez administratora, czyli ich zagubienie przez administratora lub przez podmiot przetwarzający podczas ich przechowywania.
40. Zagrożenie niezgodnym z prawem utraceniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający, czyli ich zagubieniem podczas ich przechowywania.
41. Niezgodne z prawem utracenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie, czyli ich zagubienie podczas wykonywania czynności innych niż przesyłanie lub przechowywanie.
42. Zagrożenie niezgodnym z prawem utraceniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie, czyli ich zagubienie podczas wykonywania czynności innych niż przesyłanie lub przechowywanie.
43. Niezgodne z prawem zmodyfikowanie danych osobowych przesyłanych. Przesyłanych od administratora, przesyłanych do administratora, przesyłanych przez administratora, przesyłanych od

podmiotu przetwarzającego, przesyłanych do podmiotu przetwarzającego, przesyłanych przez podmiot przetwarzający.

44. Zagrożenie niezgodnym z prawem zmodyfikowaniem danych osobowych przesyłanych. Przesyłanych od administratora, przesyłanych do administratora, przesyłanych przez administratora, przesyłanych od podmiotu przetwarzającego, przesyłanych do podmiotu przetwarzającego, przesyłanych przez podmiot przetwarzający.
45. Niezgodne z prawem zmodyfikowanie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający. Zmodyfikowanie bez upoważnienia lub polecenia, czyli ze złamaniem zasady integralności.
46. Zagrożenie niezgodnym z prawem zmodyfikowaniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający. Zmodyfikowaniem bez upoważnienia lub polecenia, czyli ze złamaniem zasady integralności.
47. Niezgodne z prawem zmodyfikowanie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
48. Zagrożenie niezgodnym z prawem zmodyfikowaniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
49. Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych. Przesyłanych od administratora, przesyłanych do administratora, przesyłanych przez administratora, przesyłanych od podmiotu przetwarzającego, przesyłanych do podmiotu przetwarzającego, przesyłanych przez podmiot przetwarzający.
50. Zagrożenie niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przesyłanych. Przesyłanych od administratora, przesyłanych do administratora, przesyłanych przez administratora, przesyłanych od podmiotu przetwarzającego, przesyłanych do podmiotu przetwarzającego, przesyłanych przez podmiot przetwarzający.
51. Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający. Jest to ujawnienie z naruszeniem zasady zgodności z prawem i zasady poufności, ujawnienie, nad którym nie sprawuje kontroli administrator ani podmiot przetwarzający.

52. Zagrożenie niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
53. Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
54. Zagrożenie niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
55. Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
56. Zagrożenie niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
57. Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
58. Zagrożenie niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
59. Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
60. Zagrożenie niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
61. Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
62. Zagrożenie przypadkowym i niezgodnym z prawem zniszczeniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.

63. Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
64. Zagrożenie przypadkowym i niezgodnym z prawem zniszczeniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
65. Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
66. Zagrożenie przypadkowym i niezgodnym z prawem zniszczeniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
67. Przypadkowe i niezgodne z prawem utracenie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
68. Zagrożenie przypadkowym i niezgodnym z prawem utraceniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
69. Przypadkowe i niezgodne z prawem utracenie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
70. Zagrożenie przypadkowym i niezgodnym z prawem utraceniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
71. Przypadkowe i niezgodne z prawem utracenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
72. Zagrożenie przypadkowym i niezgodnym z prawem utraceniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
73. Przypadkowe lub niezgodne z prawem zmodyfikowanie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.

74. Zagrożenie przypadkowym lub niezgodnym z prawem zmodyfikowaniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
75. Przypadkowe lub niezgodne z prawem zmodyfikowanie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
76. Zagrożenie przypadkowym lub niezgodnym z prawem zmodyfikowaniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
77. Przypadkowe i niezgodne z prawem zmodyfikowanie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
78. Zagrożenie przypadkowym i niezgodnym z prawem zmodyfikowaniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
79. Przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
80. Zagrożenie przypadkowym lub niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
81. Przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
82. Zagrożenie przypadkowym lub niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
83. Przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
84. Zagrożenie przypadkowym lub niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przetwarzanych przez

administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.

85. Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.
86. Zagrożenie i niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
87. Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
88. Zagrożenie przypadkowym i niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
89. Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przesyłanie lub przechowywanie.
90. Zagrożenie przypadkowym i niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przesyłanie lub przechowywanie.

Należy zwrócić uwagę na fakt, że naruszenie ochrony danych osobowych, które zachodzi, naruszenie które zaszło, naruszenie, z którym administrator danych osobowych ma do czynienia w konkretnym przypadku, może niejako składać się z kilku wymienionych powyżej typów zdarzeń[274].

3.11. Art. 33 Uwaga 11

Naruszenie ochrony danych osobowych

Metoda ustalenia

W niniejszym podrozdziale wskazuję metodę pozwalającą na ustalenie, czy dane zdarzenie jest naruszeniem ochrony danych osobowych. Metoda ta polega na zadaniu szeregu pytań. Trudno powie-

[274] Podobnie: Grupa Robocza art. 29, *Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679*. Przyjęte w dniu 3 października 2017 r. Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r. 18/PL WP250 rev.01, s. 8.

dzieć, czy jest to metoda lepsza niż metoda proponowana w uwadze poprzedniej (*3.10. Art. 33 ust. 1 Uwaga 10. Naruszenie ochrony danych osobowych – zestawienie*). Wydaje się, że jest to metoda szybsza. Nic nie stoi na przeszkodzie, by w konkretnym stanie faktycznym zastosować obydwie metody. Wynik powinien być taki sam. Jeżeli wynik jest inny, to w żadnym wypadku nie należy go uśredniać (choć sam nie wiem, co miałoby to tu oznaczać", należy za to ustalić, gdzie podczas dokonywania oceny popełniono błąd.

Definicja naruszenia ochrony danych osobowych zawarta jest w art. 4 pkt 12 RODO. Stanowi on:
naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Jak widać, definicja składa się z trzech grup zjawisk. Zdarzenie jest naruszeniem ochrony danych osobowych, jeżeli posiada cechy należące do każdej ze wskazanych grup zjawisk. Możliwa jest też sytuacja, że zdarzenie posiada kilka cech należących do danej grupy.

Żeby zatem ustalić, czy zdarzenie jest naruszeniem ochrony danych osobowych, zdefiniowanym w art. 4 pkt 12 RODO, należy zadać trzy pytania. Wskazuję je poniżej.

Pytanie pierwsze
Czy zdarzenie miało charakter
– przypadkowy lub
– niezgodny z prawem?
Jeżeli zdarzenie miało charakter przypadkowy lub niezgodny z prawem, to należy zadać pytanie kolejne. Jeżeli zdarzenie nie miało takiego charakteru, to zdarzenie nie było naruszeniem ochrony danych osobowych, więc zadawanie pytań kolejnych jest bezcelowe.

Pytanie drugie
Czy zdarzenie polegało na:
– zniszczeniu danych osobowych lub
– utraceniu danych osobowych, lub
– zmodyfikowaniu danych osobowych, lub
– nieuprawnionym ujawnieniu danych osobowych, lub

– nieuprawnionym dostępie do danych osobowych?
Czy zdarzenie zagrażało (prowadziło do):
– zniszczeniem danych osobowych lub
– utraceniem danych osobowych, lub
– zmodyfikowaniem danych osobowych, lub
– nieuprawnionym ujawnieniem danych osobowych, lub
– nieuprawnionym dostępem do danych osobowych?
Jeżeli zdarzenie polegało na jednym z wymienionych w tym zestawieniu zjawisk (w tym zjawisk o charakterze zagrożenia), to należy zadać pytanie kolejne. Jeżeli zdarzenie nie polegało na żadnym z tych zjawisk, to zdarzenie nie było naruszeniem ochrony danych osobowych, więc zadawanie pytań pozostałych jest bezcelowe.

Pytanie trzecie
Czy zdarzenie dotyczyło danych osobowych:
– przesyłanych lub
– przechowywanych, lub
– przetwarzanych inaczej niż przez przesyłanie lub przechowywanie?

Jeżeli zdarzenie dotyczyło danych przetwarzanych na jeden z opisanych w tym zestawieniu sposobów, to należy zadać pytanie kolejne. Jeżeli zdarzenie nie dotyczyło danych osobowych przetwarzanych na żaden z opisanych w zestawieniu sposobów, to zdarzenie nie było naruszeniem ochrony danych osobowych, więc zadawanie pytań pozostałych jest bezcelowe.

Jeżeli uzyskano co najmniej po jednej odpowiedzi twierdzącej z każdej grupy pytań, to zdarzenie, wobec którego zadawano pytania, **jest** naruszeniem ochrony danych osobowych, zdefiniowanym w art. 4 pkt 12 RODO. Jeżeli zdarzenie **jest** naruszeniem ochrony danych osobowych, zdefiniowanym w art. 4 pkt 12 RODO, to administrator ma obowiązek przystąpić do oceny ryzyka naruszenia praw i wolności osób fizycznych. Kiedy administrator ustali poziom ryzyka naruszenia praw i wolności osób fizycznych, wtedy będzie wiedział, czy zdarzenie należy zgłosić organowi nadzorczemu, czy należy o nim poinformować osoby, których dane dotyczą, czy nie.

Jeżeli odpowiedź na pytanie z co najmniej jednej grupy była przecząca, to zdarzenie, wobec którego zadawano pytania, **nie jest** naruszeniem ochrony danych osobowych, zdefiniowanym w art. 4 pkt

12 RODO. Jeżeli zdarzenie **nie jest** naruszeniem ochrony danych osobowych, zdefiniowanym w art. 4 pkt 12 RODO, to przystępowanie przez administratora do oceny ryzyka naruszenia praw i wolności osób fizycznych jest bezcelowe. Bezcelowe, ponieważ takie zdarzenie, zdarzenie, które nie jest naruszeniem na gruncie art. 4 pkt 12 RODO, nie podlega ocenie ani na gruncie art. 33 RODO, ani na gruncie art. 34 RODO.

Tytułem uzupełnienia warto zwrócić uwagę na jedno jeszcze zjawisko, otóż piszę wyżej, że jeżeli odpowiedź na pytania z danej grupy jest negatywna, to należy zaniechać dalszego badania, ponieważ zdarzenie nie jest naruszeniem ochrony danych osobowych. Potwierdzam to jednak, jestem świadom, że osoba dokonująca oceny może się pomylić. Z tego względu warto wykonać całe badanie, nawet jeżeli odpowiedź na pytania na przykład z pierwszej grupy brzmi negatywnie. Warto wykonać całe badanie i w sytuacji, kiedy na przykład odpowiedzi na pytania z dwóch grup są pozytywne, przemyśleć, czy negatywna odpowiedź nie jest odpowiedzią błędną.

Podobna myśl prawnicza stoi chyba za zestawieniem naruszeń przedstawionym przez G. Sibigę i współautorów. Opisują oni i podają przykłady trzech rodzajów naruszeń, a to:
– naruszenia dotyczącego poufności danych osobowych,
– naruszenia dotyczącego integralności danych osobowych,
– naruszenia dotyczącego dostępności danych osobowych[275].

Wskazani autorzy nie stosują metody opartej na pytaniach, ale metodę opisową, wzbogaconą o przykłady, jednak z racji tematyki, odnotowuję tu ich wystąpienie.

Nieco niepokoi mnie stanowisko wyrażone w artykule K. Gałęzowskiej. Autorka ta pisze, że: *Użycie terminu „prowadzące do" sugeruje, że, aby zakwalifikować jakieś zdarzenie jako naruszenie ochrony danych osobowych, musi nastąpić określony skutek*[276]. Jeżeli na przykład rozpatrzymy niezgodne z prawem zniszczenie danych osobowych… Czy konieczne jest zniszczenie, by uznać, że nastąpiło naruszenie z art. 4 pkt 12 RODO? Słowa wskazanej autorki mogą sugerować, że ma ona taki właśnie pogląd. Muszę podkreślić, że jeśli taki

[275] G. Sibiga, I. Małobęcka-Szwast, D. Nowak, K. Syska, op. cit., s. 77.

[276] K. Gałęzowska, op. cit., s. 52.

właśnie jest pogląd K. Gałęzowskiej, to uważam ten pogląd za błędny. Widać to – jak się wydaje – w dwóch płaszczyznach.

W płaszczyźnie językowej „prowadzące do" nie oznacza wcale, że dany skutek musiał mieć miejsce. Gdyby intencją prawodawcy było przesądzenie, że dla zaistnienia naruszenia konieczne jest, by zaszło zniszczenie lub utracenie, lub zmodyfikowanie, lub nieuprawnione ujawnienie, lub nieuprawniony dostęp do danych osobowych, że nie wystarczy samo zagrożenie takimi zdarzeniami, to zapewne prawodawca użyłby określenia, które by na to wskazywało. Wersja anglojęzyczna jest tu zgodna z wersją polskojęzyczną, zawiera bowiem słowa: *a breach of security leading to*. Wydaje się, że gdyby interpretacja przepisu miała być taka jak proponuje K. Gałęzowska, to naruszenie ochrony danych osobowych byłoby definiowane jako „naruszenie bezpieczeństwa mające postać przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych, lub w inny sposób przetwarzanych".

Podobnie widzę rzecz w płaszczyźnie znaczeniowej. Pozostańmy przy zniszczeniu danych osobowych jako przykładzie. Gdyby naruszeniem ochrony danych miało być zniszczenie, ale zagrożenie zniszczeniem już nie, to trudno byłoby mówić o różnym ryzyku naruszenia praw i wolności osób fizycznych. Przecież zniszczenie (w warunkach z art. 4 pkt 12 RODO) automatycznie skutkuje naruszeniem kilku co najmniej praw. Prawa do przetwarzania w sposób zgodny z prawem, prawa do przetwarzania w sposób ograniczony co do zakresu, prawa w sposób ograniczony co do czasu, prawa do przetwarzania w sposób integralny. W wypadku zniszczenia danych, oczywiste staje się nie zagrożenie naruszeniem wskazanych praw, ale naruszenie tych praw, więc stopniowanie ryzyka naruszenia praw i wolności nie byłoby możliwe. A przecież jest. Skoro zatem racjonalny prawodawca uzależnił, czy i gdzie należy zgłaszać naruszenie ochrony danych osobowych od poziomu ryzyka naruszenia praw i wolności, to zróżnicowanie tego poziomu musi być możliwe. W takim więc razie interpretacja, zgodnie z którą jedynie (w tym przykładzie) zniszczenie byłoby naruszeniem ochrony danych, a zagrożenie zniszczeniem, by naruszeniem nie było – jest błędna. Być może ja po prostu niewłaściwie zrozumiałem stanowisko K. Gałęzowskiej, ale rzecz jest na tyle istotna, że nie sposób być tu nadmiernie ostrożnym.

Za interpretacją, zgodnie z którą naruszeniem ochrony danych osobowych może być samo zagrożenie zdarzeniami z art. 4 pkt. 12 RODO, przemawia – jak sądzę – interpretacja PUODO. Co ciekawe, nie zawsze tak było, organ ochrony danych zrazu miał nieco inne stanowisko, zbliżone do domniemanego stanowiska K. Gałęzowskiej, o czym piszę w książce wydajnej w 2020 roku[277]. Opisuję tam szczegółowo zmagania organu z zakresem znaczeniowym pojęcia naruszenia ochrony danych osobowych.

Fakt, że prosty przepis może być niewłaściwie rozumiany, o czym piszę też niżej w uwadze (*3.13. Art. 33 Uwaga 13. Naruszenie zdaniem EROD. Polemika*), każe postawić postulat nowelizacyjny (*6.3. Art. 33. Postulat 3 Uczytelnienie przepisu*).

3.12. Art. 33 Uwaga 12

Naruszenie zdaniem EROD. Wątpliwości

Europejska Rada Ochrony Danych zajęła się zjawiskiem naruszeń i zgłaszaniem tychże. W wytycznych z 2021 roku EROD wyróżnia trzy rodzaje naruszeń. Są to:
– *confidentiality breach*,
– *integrity breach*,
– *availability breach*.

Na język polski tłumaczymy to następująco:
– naruszenie poufności,
– naruszenie integralności,
– naruszenie dostępności.

Problem polega na tym, że jeśli chodzi o „naruszenie dostępności", o którym mowa w wytycznych EROD z 2021 roku, to nie współgra ono z treścią art. 4 pkt 12 RODO. We wcześniejszym oficjalnym dokumencie, a mianowicie wytycznych z 2018 r.[278] czytamy, że: *Jeżeli chodzi o pojęcie „utraty" danych osobowych, należy interpretować je jako odnoszące się do sytuacji, w której dane mogą nadal*

[277] J. Rzymowski, *RODO – GDPR. Przedmiot i cele…*, s. 520–526.

[278] Grupa Robocza art. 29, *Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679*. Przyjęte w dniu 3 października 2017 r. Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r. 18/PL WP250 rev.01, s. 7.

istnieć, ale administrator utracił nad nimi kontrolę, nie posiada już do nich dostępu lub nie znajduje się już w ich posiadaniu. W wersji anglojęzycznej posłużono się słowem: „loss", co dawałoby pewną nadzieję, jednak w wersji anglojęzycznej czytamy: *In terms of "loss" of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession*[279]. Widać zatem tu pewne uzasadnienie dla zaliczenia „naruszenia dostępności" do „naruszeń ochrony danych osobowych", ale przyznam, że cytowany dokument mnie nie przekonuje. W cytowanych słowach dokumentu widzę uzasadnienie dla stanowiska zgodnie z którym „naruszenie dostępności" stanowi naruszenie ochrony danych osobowych, jednak nie widzę uzasadnienia dla cytowanych słów dokumentu. Patrząc na rzecz inaczej, uważam, że należy „naruszenie dostępności" traktować jako naruszenie ochrony danych osobowych, ponieważ tak wynika z oficjalnych dokumentów organów UE, jednak w samym RODO z wielkim trudem dostrzegam uzasadnienie dla takiego stanowiska. Z ostrożności należy jednak, zwłaszcza w praktyce, zgadzać się ze stanowiskiem organów.

3.13. Art. 33 Uwaga 13

Naruszenie zdaniem EROD. Polemika

Niestety, opisane wyżej wątpliwości to niejedyne wątpliwości, jakie mam w związku ze stanowiskiem EROD w wytycznych[280] z 2021 roku (dalej używam określenia: „Wytyczne").

W Wytycznych czytamy, że: *A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymization, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or*

[279] Article 29 Data Protection Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679*. Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018. 18/EN. WP250. rev.01, s. 7.

[280] European Data Protection Board. Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021. Version 1.0.

social disadvantage to those individuals. One of the most important obligation of the data controller is to evaluate these risks to the rights and freedoms of data subjects and to implement appropriate technical and organizational measures to address them.

Na język polski tłumaczymy to na: „Naruszenie może potencjalnie mieć szereg istotnych niekorzystnych efektów ubocznych dla osób fizycznych, co może skutkować fizyczną, materialna lub niematerialną szkodą. RODO wyjaśnia, że może to obejmować utratę kontroli nad ich danymi osobowymi, ograniczenie ich praw, dyskryminację, kradzież tożsamości lub oszustwo, stratę finansową, nieuprawnione odwrócenie pseudonimizacji, uszczerbek na reputacji i utratę poufności danych osobowych chronionych tajemnicą zawodową. Może również obejmować wszelkie inne znaczące ekonomiczne lub socjalne niedogodności dla osób fizycznych. Jednym z najważniejszych obowiązków administratora danych jest ocena tych zagrożeń dla praw i wolności osób, których dane dotyczą i wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapobieżenia im". Jak widać, autorzy Wytycznych odnoszą się tu do zagrożeń dla interesów osób, których dane dotyczą i wskazują, że zagrożenia te są zagrożeniami dla praw i wolności. Z tym można się zgodzić, w duchu zasady ekonomiki myślenia można zapomnieć o interesach osób, których dane dotyczą i uznać, że wskazane tu zagrożenia stanowią zagrożenia dla praw i wolności. Nieco niepokoi, że autorzy Wytycznych nie wskazują, dla jakich dokładnie praw i wolności widzą tu zagrożenia, ale to niestety nie jest jedyny problem.

Dalej czytamy: *The breach should be notified when the controller is of the opinion that it is likely to result in a risk to the rights and freedoms of the data subject.* Na język polski tłumaczymy to na: „Naruszenie powinno zostać zgłoszone, gdy administrator uzna, [że prawdopodobne jest,] że może ono skutkować ryzykiem dla praw i wolności podmiotu danych". Pomijając pewną lekkość w podejściu do tego, kiedy zachodzi obowiązek, nie można mieć tu poważniejszych zastrzeżeń. Niestety, dalej czeka nas wiele zaskoczeń. Zrazu Wytyczne wskazują, że administratorzy powinni mieć odpowiednie procedury w przewidywaniu naruszeń – i tu nie można mieć zastrzeżeń, dalej jednak Wytyczne rozpadają się na osiemnaście kazusów wraz z ich omówieniami. I tu zaczyna się prawdziwy problem.

Co do większości kazusów nie mam zastrzeżeń, acz razi mnie poważnie, że autorzy Wytycznych nie wskazują, jakie prawa i wolności zostały w konkretnych stanach faktycznych naruszone. Mam jednak świadomość, że to nie ja jestem autorem tego dokumentu, jego zaś autorzy napisali go po prostu nieco inaczej, niż ja bym to uczynił. Tu problemu nie ma, są jednak w Wytycznych kazusy, z rozwiązaniem których zgodzić się nie mogę. Problemu nie ma pozornie, ponieważ nie wskazując konkretnych praw, autorzy Wytycznych zastawili na siebie pułapkę.

Zgadzam się z wnioskiem sformułowanym w odniesieniu do **kazusu 14**. Stan faktyczny jest tam taki, że urząd zajmujący się bezrobotnym wysłał do bezrobotnych wiadomości poczty elektronicznej i do każdego z adresatów wysłał załącznik zawierając dane ponad sześciu tysięcy poszukujących pracy (imię [zapewne z nazwiskiem J.Rz.], adres poczty elektronicznej, adres pocztowy, numer ubezpieczenia społecznego). Dodałbym, że w opisanym stanie faktycznym naruszono wskazane niżej prawa.

– Prawo do przetwarzania w sposób zgodny z prawem, zapisane w zasadzie zgodności z prawem.
– Prawo do przetwarzania w sposób ograniczony co do celu, zapisane w zasadzie ograniczenia celowego.
– Prawo do przetwarzania w sposób ograniczony do tego, co niezbędne adekwatne i stosowne, zapisane w zasadzie minimalizacji.
– Prawo do przetwarzania danych osobowych w sposób poufny, zapisane w zasadzie poufności.

Zwracam uwagę, że wskazane powyżej prawa naruszono, a nie tylko stworzono ryzyko ich naruszenia.

Kazus 15. Lista uczestników kursu językowego została wysłana do piętnastu uczestników poprzedniej edycji kursu, zamiast do hotelu. Lista zawierała dane osobowe [imiona zapewne z nazwiskami – J.Rz.], adresy poczty elektronicznej, preferencje jedzeniowe. Dalej autorzy Wytycznych wywodzą, że szkody dla osób zainteresowanych nie są prawdopodobne – z tym się mogę zgodzić, ale zwracam uwagę, że administrator nie powinien oceniać potencjalnych szkód dla osób, których dane były przedmiotem naruszenia, ale że administrator powinien oceniać ryzyko naruszenia ich praw i wolności. Dalej wskazano, że ilość danych jest niewielka, co jest prawdą, jednak znów przypomi-

nam, że administrator nie powinien zgodnie z RODO oceniać skali naruszenia, ale powinien oceniać ryzyko naruszenia praw i wolności osób, których dane dotyczą. Pomijam fragment dotyczący mitygacji ewentualnych skutków. W końcu czytamy (tłumaczę na jęz. polski), że „[…] jest mało prawdopodobne, że naruszenie skutkowało ryzykiem naruszenia praw i wolności". I dalej nie zaleca się zgłoszenia organowi ani poinformowania osób.

I tu właśnie jestem zaskoczony. W opisywanym stanie faktycznym naruszono wiele praw, wskazuję je poniżej.

– Prawo do przetwarzania w sposób zgodny z prawem i wolność od przetwarzania w sposób niezgodny z prawem, zapisane w zasadzie zgodności z prawem. Prawo to naruszono, ponieważ nie sposób znaleźć w art. 6 RODO warunku zgodności z prawem przetwarzania danych osobowych, który legalizowałby wysłanie danych w sposób opisane w kazusie.
– Prawo do przetwarzania w sposób ograniczony co do celu i wolność od przetwarzania w sposób nieograniczony co do celu, zapisane w zasadzie ograniczenia celowego. Ponieważ celem przetwarzania danych osobowych przez administratora na pewno nie jest informowanie uczestników poprzedniego kursu językowego o danych następnego kursu językowego.
– Prawo do przetwarzania w sposób ograniczony do tego, co niezbędne adekwatne i stosowne, i wolność od przetwarzania w sposób ograniczony do tego, co niezbędne adekwatne i stosowne, zapisane w zasadzie minimalizacji. Ponieważ wysłanie danych uczestnikom poprzedniego kursu nie jest niezbędne, adekwatne ani stosowne do celu przetwarzania, czyli do poinformowania hotelu o preferencjach jedzeniowych uczestników kursu.
– Prawo do przetwarzania danych osobowych w sposób poufny i wolność od przetwarzania w sposób niepoufny, zapisane w zasadzie poufności. Ponieważ uczestnicy poprzedniego kursu nie są uprawnieni do przetwarzania danych uczestników kolejnego kursu.

Zwracam uwagę, że wskazane powyżej prawa naruszono, a nie tylko stworzono ryzyko ich naruszenia. Skoro należy poinformować osoby przy wysokim ryzyku, to przy naruszeniu tym bardziej, co wynika z zasady *a fortiori*. Jednocześnie jedynie niski poziom ryzyka zwalnia z poinformowania organu ochrony danych, więc i organ należy poinformować.

Ponadto w opisywanym stanie faktycznym stworzono ryzyko dla wskazanych poniżej praw.

– Prawo do przetwarzania danych osobowych w sposób prawidłowy i wolność od przetwarzania w sposób nieprawidłowy zapisane w zasadzie prawidłowości. Dostrzegam tu wysokie ryzyko, ponieważ nie należy się spodziewać, że jeżeli dane zostają komuś przypadkiem ujawnione, to będzie on dbał o ich prawidłowe przetwarzanie.
– Prawo do przetwarzania w sposób ograniczony co do czasu i wolność od przetwarzania w sposób nieograniczony co do czasu zapisane w zasadzie ograniczenia przechowywana. Dostrzegam również wysokie ryzyko, ponieważ nie należy się spodziewać, że jeżeli dane zostają komuś przypadkiem ujawnione, to będzie on dbał o ich przetwarzanie przez czas właściwy dla pierwotnego administratora.

Wskazuję powyżej, że naruszono cztery konkretne prawa i wolności i stworzono wysokie ryzyko dla dwóch praw i wolności. Wskazuję konkretne prawa i wolności. Czynię to, by wskazać, że zalecenia zawarte w Wytycznych są błędne. W opisanym stanie faktycznym naruszenie należy zgłosić do organu i należy o nim poinformować osoby, których dane dotyczą. Właśnie przy wskazanym kazusie autorzy Wytycznych wpadli w przypadkiem zastawioną przez siebie pułapkę – nie ocenili ryzyka dla konkretnych praw i wolności i jednocześnie brak ryzyka wyimaginowali, ponieważ uznali, że szkody dla ludzi, których dane dotyczą, będą niewielkie.

Nie jest moim celem analizowanie wskazanych Wytycznych, tym bardziej że z większością zaleceń się zgadzam, zwracam jednak uwagę na fakt, że autorzy Wytycznych mylą skutki dla osób, których dane dotyczą, skutki o charakterze różnorakich szkód, z ryzykiem naruszenia praw i wolności. Te dwa zjawiska trzeba rozgraniczać. Poza tym należy brać pod uwagę konkretne prawa i wolności po to, by następnie móc ocenić ryzyko ich naruszenia.

Karolina Gałęzowska napisała, że: *Przy wątpliwościach dotyczących definicji naruszenia nie jest jasne, czym jest ryzyko naruszenia praw i wolności osób, których dane dotyczą*[281]. Nie uważam, by definicja naruszenia ochrony danych osobowych powinna być źródłem wątpliwości.

[281] K. Gałęzowska, op. cit.

Odnoszę się do niej wyżej w uwadze (*3.11. Art. 33 Uwaga 11. Naruszenie ochrony danych osobowych – metoda ustalenia*), a wcześniej jeszcze omawiam w drugiej książce z niniejszego cyklu. Faktem jest jednak, że – jak widać – nawet poważne organy mają wątpliwości. Trudno powiedzieć, czy świadczy to o kondycji tychże organów, czy o jakości prawa. Niezależnie od źródła zmagań, dobrze by było, gdyby przepis był czytelniejszy, należy zatem postawić postulat nowelizacyjny, co czynię niżej (*6.3. Art. 33. Postulat 3 Uczytelnienie przepisu*).

3.14. Art. 33 Uwaga 14

Naruszenie ochrony danych osobowych

Kolejność działań

W podrozdziałach niniejszego rozdziału wyjaśniam powyżej:
– czym jest naruszenie ochrony danych osobowych,
– jak odróżnić zdarzenie, które nie jest naruszeniem ochrony danych osobowych od zdarzenia, które jest naruszeniem ochrony danych osobowych,
– jakie prawa i wolności należy brać pod uwagę przy ocenie ryzyka naruszenia praw i wolności,
– kiedy administrator ma obowiązek poinformować osoby, których dane dotyczą o naruszeniu ochrony danych osobowych.

Wcześniej we wstępie sygnalizuję: *Zagadnienia związane z działaniami, jakie powinny zostać podjęte przez administratora w sytuacji zaistnienia zjawisk, które godzą w bezpieczeństwo danych*. Z uwagi na nie jedynie naukowy, ale również – jak mam nadzieję – praktyczny charakter niniejszej publikacji, zamieszczam poniżej zestawienie czynności, jakie powinny być wykonane w związku z naruszeniem ochrony danych osobowych. Czynności te omawiam powyżej, w odpowiednich, poświęconych im podrozdziałach, do których poniżej odsyłam. Należy jednocześnie pamiętać, że każda ze wskazanych poniżej czynności powinna być udokumentowana. Powiedzmy to nawet ostrzej. Administrator ma obowiązek dokumentować przeprowadzenie tych czynności i dokumentację tę przechowywać. Obowiązek ten wynika z zasady rozliczalności.

Niżej prezentuję zestawienie czynności związanych z naruszeniem ochrony danych osobowych. Zestawienie to ma pewien walor

porządkujący. Nie uzasadniam poniżej kolejnych działań, za to wskazuję miejsca w niniejszej książce, gdzie stosowne ujawnienia i wyjaśnienia się znajdują.

1. Ma miejsce zdarzenie. Zdarzenie, co do którego administrator, czyli zwykle stosowne jego służby, czasem personel zarządzający, czasem inspektor ochrony danych, czasem pracownik zajmujący się bezpieczeństwem informatycznym, czasem pracownicy merytoryczni, mają podejrzenie, że zdarzenie to może być naruszeniem ochrony danych osobowych. Naruszenie ochrony danych osobowych zdefiniowane jest w art. 4 pkt 12 RODO. Omawiam je jako definicję, w innej książce[282] z cyklu. W niniejszej książce omawiam je raczej przez pryzmat funkcjonalny, wyżej w uwagach (*3.10. Art. 33 ust. 1 Uwaga 10. Naruszenie ochrony danych – zestawienie*) i (*3.11. Art. 33 Uwaga 11. Naruszenie ochrony danych osobowych – metoda ustalenia*).

1.1. Kiedy ma miejsce zdarzenie, które może być naruszeniem ochrony danych osobowych, to administrator musi być świadom pewnego zagrożenia, o charakterze czegoś na kształt definicyjnej pułapki. Otóż na swojego rodzaju suburbiach wiedzy z szeroko pojętej ochrony danych funkcjonuje pojęcie incydentu. Funkcjonuje ono nawet bardziej w sferze praktyki niż w sferze doktryny, przez co jego użycie jest trudniej uchwytne, ale i w sferze doktryny jest ono dostrzegalne. Zajmuję się zjawiskiem incydentu wyżej w uwadze (*3.9. Art. 33 ust. 1 Uwaga 9. Incydent*). I właśnie tu kryje się wspomniana pułapka. Kiedy ma miejsce zdarzenie, może ono mylnie być potraktowane, jak ów „incydent" (czasem wzbogacany o atrakcyjne dodatki – incydent bezpieczeństwa, incydent ochrony danych itd.). Zdarzenie takie odnotowane zostaje w rejestrze takowych incydentów i na tym kończy się zainteresowanie administratora zdarzeniem. Zagrożenia są tu liczne.

1.1.1. **Po pierwsze,** zdarzenie takie często powinno być zakwalifikowane jako naruszenie i dalej oceniane.

1.1.2. Wynika z tego **drugie** zagrożenie, a mianowicie jeżeli zdarzenie nie jest dalej oceniane, to administrator naraża się na odpowiedzialność z racji niezgłoszenia naruszenia do PUODO;

[282] J. Rzymowski, op. cit., s. 501.

nie wie on przy tym, czy zgłoszenie takie powinno zostać zrealizowane, ponieważ tego nie ocenił.

1.1.3. Analogiczne jest **trzecie** zagrożenie, a mianowicie administrator naraża się na odpowiedzialność z racji niepoinformowania o naruszeniu osób, których dane dotyczą; nie wie on przy tym, czy poinformowanie takie powinno zostać zrealizowane, ponieważ również tego nie ocenił.

1.1.4. Podsumowaniem może być zagrożenie **czwarte**, a mianowicie może się zdarzyć, że administrator odnotuje zdarzenie w dokumentacji, którą ma obowiązek prowadzić na podstawie art. 33 ust. 5 RODO. W dokumentacji takiej administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, a tym samym w jakiś sposób przyznaje, że owszem, że naruszenie miało miejsce, ale że uznał je za incydent i nie poddał dalszym ocenom. Dalej sytuacja administratora jest analogiczna do tej opisanej wyżej przy zagrożeniu trzecim i zagrożeniu czwartym. Możliwa jest odpowiedzialność, administrator nie wie, czy zgłaszać i informować, jednak posiada dowody, które mogą, zależnie od zdarzenia świadczyć w jego interesie lub przeciw niemu.

1.1.5. Odmianą jest zagrożenie **piąte**, a mianowicie kiedy administrator odnotowuje zdarzenie w osobnym rejestrze, w rejestrze takich właśnie zdarzeń – incydentów, zbiera tam informacje, z których wynika, że zdarzenie jest naruszeniem, ale nie podejmuje dalszych kroków. Administrator posiada wtedy dowód, że naruszył RODO, że nie dokonał ocen. Faktem jest, że dowód ten nie znajduje się w dokumentacji powstałej na podstawie art. 33 ust. 5 RODO, ale w dokumentacji, rzekłbym, autorskiej, to jednak nie ma tu szczególnego znaczenia.

I tu sytuacja administratora jest analogiczna do tej opisanej wyżej przy zagrożeniu trzecim i zagrożeniu czwartym. I tu możliwa jest odpowiedzialność, administrator nie wie, czy zgłaszać i informować, jednak posiada dowody, które mogą – zależnie od zdarzenia – świadczyć w jego interesie lub przeciw niemu.

2.a. Administrator uznaje, że zdarzenie **nie jest** naruszeniem ochrony danych osobowych (art. 4 pkt 12 RODO). Uzyskanie takiego wy-

niku oceny, że zdarzenie **nie jest** naruszeniem ochrony danych osobowych, w zasadzie kończy obowiązki administratora związane z danym zdarzeniem (art. 33 ust. 1 RODO w zw. z art. 4 pkt 12 RODO i art. 34 ust. 1 RODO w zw. z art. 4 pkt 12 RODO). Jeżeli spojrzymy na stan faktyczny przez pryzmat zasady rozliczalności (art. 5 ust. 2 RODO), to okazuje się, że administrator powinien zachować dowody na to, że zdarzenie miało miejsce i że dokonywał oceny dla ustalenia, czy jest ono naruszeniem ochrony danych osobowych czy nie.

2.b. Administrator uznaje, że zdarzenie **jest** naruszeniem ochrony danych osobowych[283] (Art. 4 pkt 12 RODO). Uzyskanie takiego wyniku oceny, że zdarzenie **jest** naruszeniem ochrony danych osobowych, skutkuje tym, że po stronie administratora pojawiają się kolejne obowiązki związane z danym zdarzeniem.

3.b. Administrator ustala poziom ryzyka naruszenia praw i wolności osób fizycznych, których dane dotyczą i następnie podejmuje działania odpowiednio do tego poziomu (art. 33 ust. 1 RODO i art. 34 ust. 1 RODO). Wskazane poniżej poziomy wynikają z art. 33 RODO i art. 34 RODO. Rozumowanie, które doprowadziło do ich ustalenia, nazwania i zestawienia znajduje się wyżej w uwadze (*3.14. Art. 24. Uwaga 14. Poziomy ryzyka*). Wstępne zestawienie poziomów ryzyka naruszenia praw i wolności osób fizycznych znajduje się wyżej, w uwadze (*3.15. Art. 24. Uwaga 15. Zestawienie poziomów ryzyka naruszenia praw i wolności osób fizycznych*).

3.b.1. Jeżeli zachodzi

brak ryzyka naruszenia praw i wolności osób fizycznych,
to administrator

3.b.1.1. nie zgłasza naruszenia ochrony danych osobowych do PUODO (art. 33 ust. 1 RODO),

i

3.b.1.2. nie informuje o naruszeniu ochrony danych osobowych osób, których dane dotyczą (art. 34 ust. 1 RODO).

3.b.2. Jeżeli zachodzi

[283] Podobnie: K. Wygoda, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie...,* s. 366.

ryzyko o małym prawdopodobieństwie naruszenia praw i wolności osób fizycznych, o którym to ryzyku wnioskujemy ze słów art. 33 ust. 1 RODO: […] *chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych*. (art. 33 ust. 1 RODO),
to administrator

3.b.2.1. nie zgłasza naruszenia ochrony danych osobowych do PUODO (art. 33 ust. 1 RODO)
i

3.b.2.2. nie informuje o naruszeniu ochrony danych osobowych osób, których dane dotyczą (art. 34 ust. 1 RODO).

3.b.3. Jeżeli zachodzi
ryzyko o średnim poziomie (ryzyko), o którym wnioskujemy z art. 33 ust. 1 RODO i z motywu 76 Preambuły RODO,
to administrator

3.b.3.1. zgłasza naruszenie ochrony danych osobowych do PUODO (art. 33 ust. 1 RODO)
i

3.b.3.2. nie informuje o naruszeniu ochrony danych osobowych osób, których dane dotyczą (art. 34 ust. 1 RODO).

3.b.4. Jeżeli zachodzi lub może zajść
wysokie ryzyko naruszenia praw i wolności osób fizycznych, o którym wnioskujemy ze słów art. 34 ust. 1 RODO: […] *wysokie ryzyko naruszenia praw lub wolności osób fizycznych*,
to administrator

3.b.4.1. zgłasza naruszenie ochrony danych osobowych do PUODO (art. 33 ust. 1 RODO)
i

3.b.4.2. informuje o naruszeniu ochrony danych osobowych osoby, których dane dotyczą (art. 34 ust. 1 RODO).

3.b.5. Jeżeli zachodzi
naruszenie praw i wolności osób fizycznych,
to administrator

3.b.5.1. zgłasza naruszenie ochrony danych osobowych do PUODO (art. 33 ust. 1 RODO)
i

3.b.5.2. informuje o naruszeniu ochrony danych osobowych osoby, których dane dotyczą (art. 34 ust. 1 RODO).

4. Administrator dokumentuje naruszenia ochrony danych osobowych, niezależnie od poziomu ryzyka naruszenia praw i wolności osób fizycznych, niezależnie od tego, czy administrator zgłasza naruszenie do PUDOO, niezależnie od tego, czy administrator informuje osoby, których dane dotyczą o naruszeniu ochrony danych osobowych. Administrator dokumentuje okoliczności naruszenia, skutki naruszenia, działania zaradcze jakie podjął (art. 34 ust. 5 RODO).

Na marginesie prezentowanych tu ustaleń, zwracam niepolemicznie uwagę, że w przypadku naruszenia praw i wolności: o średnim poziomie i o wysokim poziomie P. Barta, M. Kawecki i P. Litwiński, posługują się określeniem *ryzyko […] większe niż małe*[284].

Podobne do zastosowanego powyżej, rozbite na etapy, ujęcie zastosował K. Wygoda[285]. Wydaje się, że dla zrozumienia, zobrazowania, a zwłaszcza wyjaśnienia kolejności czynności, swojego rodzaju porządku ich następstwa, ujęcie etapowe jest tu najlepsze.

3.15. Art. 33 Uwaga 15

Naruszenie dostępności

Wyżej odnoszę się do zjawiska naruszenia ochrony danych osobowych, które jest zdefiniowane w art. 4 pkt 12 RODO. Drobiazgowa analiza, której powyżej dokonuję, czy to w uwadze (*3.10. Art. 33 ust. 1 Uwaga 10. Naruszenie ochrony danych osobowych – zestawienie*), czy to w uwadze (*3.11. Art. 33 Uwaga 11. Naruszenie ochrony danych osobowych – metoda ustalenia*) nie wskazuje, by w zakresie pojęcia naruszenia ochrony danych osobowych mieściła się utrata dostępu do danych, czy utrata dostępności do danych. W oficjalnym dokumencie Grupy Artykułu 29 o zjawiskach tego rodzaju się wspomina. Trzeba być tego świadomym, jednak wywody Grupy Roboczej są nieprzekonujące do tego stopnia, że Grupa powołuje się na swoje własne wcześniejsze ustalenia, które cytuję poniżej.

---

[284] Por. P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 352.

[285] K. Wygoda, K. Wygoda, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie…,* s. 367–369.

W swojej opinii 03/2014 na temat powiadamiania o przypadkach naruszenia Grupa Robocza Art. 29 wyjaśniła, że zgodnie z trzema powszechnie uznawanymi zasadami bezpieczeństwa14 naruszenia można podzielić na następujące kategorie:

– *„naruszenie dotyczące poufności danych" – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych;*
– *„naruszenie dotyczące integralności danych" – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych;*
– *„naruszenie dotyczące dostępności danych" – naruszenie, w rezultacie którego dochodzi do przypadkowego lub nieuprawnionego dostępu do danych osobowych lub zniszczenia danych osobowych*[286].

Wskazany podział jest trafny, jednak im dalej czytam dokument, tym bardziej się niepokoję.

O naruszeniu czytam dalej, że: *Naruszenie zostanie każdorazowo uznane za naruszenie dotyczące dostępności danych, jeżeli doprowadziło ono do trwałej utraty lub zniszczenia danych osobowych*[287]. Z tym twierdzeniem się zgadzam, jednak zwracam uwagę, że we wskazanej sytuacji zachodzi naruszenie ochrony danych osobowych nie dlatego, że zdarzenie (naruszenie?) miało związek z dostępnością, ale dlatego że *doprowadziło ono do trwałej utraty lub zniszczenia danych osobowych*.

Niepokoję się, kiedy czytam, że: *W tym kontekście warto zastanowić się nad tym, czy tymczasowa utrata dostępności danych osobowych powinna zostać uznana za sytuację, w której doszło do wystąpienia naruszenia, a jeżeli tak – czy naruszenie to należy zgłosić*[288]. Przecież skoro nie zaszło zniszczenie ani ujawnienie, ani zdarzenia im pokrewne, to tymczasowa utrata dostępności nie mieści się w definicji naruszenia ochrony danych osobowych. Skoro się nie mieści, to nie jest naruszeniem ochrony danych, więc rozważania, czy zgłaszać orga-

---

[286] Grupa Robocza art. 29, *Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679*. Przyjęte w dniu 3 października 2017 r. Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r. 18/PL WP250 rev.01, s. 8. Nieco sformatowałem graficznie treść, tak by nie raziła zaimportowanym układem graficznym.

[287] Ibidem, s. 8–9.

[288] Ibidem, s. 9.

nowi nadzorczemu (PUODO) takie, nie będące naruszeniem zdarzenie, nie powinny być prowadzone.

Dalej czytamy, że: *W art. 32 RODO zatytułowanym „Bezpieczeństwo przetwarzania" wyjaśniono, że przy wdrażaniu środków technicznych i organizacyjnych pozwalających zapewnić stopień bezpieczeństwa odpowiadający ryzyku, należy wziąć pod uwagę m.in. „zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania" oraz „zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego"*[289]. Wszystko jest prawdą, tylko nie rozumiem, dlaczego autorzy używają zacytowanych fragmentów art. 32 RODO dla udowodnienia swojej tezy.

I w końcu dochodzimy w lekturze do zdania podsumowującego tok rozważań, brzmi ono: *Dlatego też incydent bezpieczeństwa skutkujący utratą dostępu do danych osobowych przez określony czas również stanowi rodzaj naruszenia, ponieważ brak dostępu do danych może wywrzeć istotny wpływ na prawa i wolności osób fizycznych*. Z zapisaną tu tezą nie sposób się zgodzić. Jej autor dokonał tu niejako fuzji dwóch przepisów, dwóch instytucji. Pierwsza z nich to naruszenie zdefiniowane w art. 4 pkt. 12 RODO. Naruszenie ochrony danych jest tam zdefiniowane: *incydent bezpieczeństwa skutkujący utratą dostępu do danych osobowych przez określony czas* w zakresie tej definicji się nie mieści. Skoro się nie mieści, to nie podlega ocenie na gruncie art. 33 RODO i art. 34 RODO. Autor rozumowanie odwrócił, wskazując, że zdarzenie takie jest naruszeniem (nie użyto pełnej nazwy), *ponieważ brak dostępu do danych może wywrzeć istotny wpływ na prawa i wolności osób fizycznych*. Jak widać, dokonano tu swojego rodzaju przeskoku między art. 4 pkt 12 RODO a art. 33 RODO i art. 34 RODO, jest to jednak przeskok nieuprawniony. Podkreślenia wymaga, że o ile art. 33 RODO i art. 34 RODO korzystają z art 4 pkt 12 RODO, o tyle art. 4 pkt 12 RODO jest przepisem autonomicznym i albo konkretne zdarzenie mieści się w jego zakresie, albo nie.

Dalej czytamy: *Gwoli wyjaśnienia, jeżeli dane osobowe są niedostępne z uwagi na fakt, że system jest poddawany wcześniej zaplanowanym pracom konserwacyjnym, taka sytuacja nie stanowi przypadku „naruszenia bezpieczeństwa", o którym mowa w definicji usta-*

[289] Ibidem.

nowionej w art. 4 pkt 12[290]. I znowu rzecz trzeba wyjaśniać. Opisana sytuacja nie stanowi „naruszenia ochrony danych osobowych" jednak raczej dlatego, że nie realizuje warunków zapisanych w definicji, nie zaś dlatego że nie stanowi „naruszenia bezpieczeństwa", ponieważ prawodawca nie wyjaśnił, czym owo „naruszenie bezpieczeństwa" jest. Zapewne opisane zdarzenie nie stanowi „naruszenia bezpieczeństwa", tego jednak nie wiemy, bo prawodawca nie wskazuje, czym jest naruszenie bezpieczeństwa. Prawodawca wskazuje, czym jest naruszenie ochrony danych osobowych i wiemy, że wskazane zdarzenie nim nie jest.

W końcu czytamy, że: *Naruszenie skutkujące tymczasową utratą dostępności danych powinno zostać udokumentowane zgodnie z art. 33 ust. 5, podobnie jak naruszenie skutkujące trwałą utratą lub zniszczeniem danych osobowych (lub dowolny inny rodzaj naruszenia). Ułatwi to administratorowi wykazanie rozliczalności przed organem nadzorczym, który może zwrócić się o udostępnienie mu rejestrów do wglądu*[291]. Ze wskazaną wypowiedzią znów wypada się zgodzić. Uważam, że: *Naruszenie skutkujące tymczasową utratą dostępności danych powinno zostać udokumentowane*, ale właśnie dlatego że nie jest naruszeniem z art. 4 pkt 12 RODO i z punktu widzenia bezpieczeństwa prawnego administratora, dobrze, by mógł on wykazać, że zdarzenie (bo nie „naruszenie") naruszeniem ochrony danych osobowych nie jest.

Niestety, podobne, choć po spartańsku przejawione, poglądy znajdziemy też w komentarzu oxfordzkim[292]. Widać jednak, że C. Burton intensywnie czerpie z cytowanego wyżej dokumentu Grupy Artykułu 29. Oznacza to rzetelnie przypisami, jednak brak mi jest tam własnego stanowiska autora.

[290] Ibidem.

[291] Ibidem.

[292] C. Burton, op. cit., s. 645.

3.16. Art. 33 Uwaga 16

Naruszenie ochrony danych osobowych w realiach współadministrowania

Wyżej w (*1. Art. 33 ust. 1. Analiza*) piszę, że: *Obowiązki wynikające z przepisu spoczywają na administratorze lub na jednym ze współadministratorów – odpowiednio do ustaleń między nimi.*
Kontynuując ten wątek, zwracam uwagę, że jeżeli jeden ze współadministratorów, zgodnie z ustaleniami między tymi współadministratorami, zgłosi (zgłaszalne) naruszenie do PUODO, to dobrze i nie sposób dopatrzeć się tu jakiegokolwiek naruszenia RODO. Należy jednak równocześnie zwrócić uwagę, że jeżeli odpowiedni współadministrator zlekceważy swój obowiązek wynikający z umowy i omawianego przepisu, to trzeba pamiętać, że obowiązek wynikający z art. 34 ust. 1 RODO spoczywa na administratorze, tym samym na każdym z nich niejako z osobna i fakt współadministrowania nie zwalnia z tego obowiązku. W związku z tym można spodziewać się stosownej odpowiedzialności po stronie każdego z administratorów (współadministratorów, nie zaś jedynie tego, który obowiązku nie zrealizował, choć miał to na mocy umowy uczynić niejako w imieniu pozostałych[293].

Innymi słowy, w sytuacji realizacji obowiązku przez jednego ze współadministratorów nie widać zagrożenia odpowiedzialnością, w sytuacji, gdy jeden ze współadministratorów, ten właściwy, umownie wyznaczony, zlekceważy obowiązek, wtedy odpowiedzialność grozi każdemu z administratorów.

3.17. Art. 33 Uwaga 17

Skutek niestwierdzenia naruszenia ochrony danych osobowych

Analiza art. 34 ust. 1 RODO każe przemyśleć pewien poważny problem, który z tego przepisu wynika. Otóż jak wiemy, jeżeli naruszenie ochrony danych osobowych nie skutkuje niskim poziomem ryzyka naruszenia praw i wolności osób fizycznych, to na administratorze spoczywa obowiązek zgłoszenia naruszenia ochrony danych osobowych do PUODO. Obowiązek ten administrator powinien zre-

[293] Por. P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 367–369.

alizować, jak stanowi przepis, *bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia*. I w tym momencie pojawia się problem, może się bowiem zdarzyć, że naruszenie ochrony danych miało miejsce i jednocześnie to naruszenie ochrony danych osobowych nie skutkowało niskim poziomem ryzyka naruszenia praw i wolności osób fizycznych. Jeżeli administrator dowiedziałby się o takim naruszeniu, to powinien je zgłosić do PUODO, w terminie wskazanym wyżej. Jeżeli administrator nie zgłosił naruszenia, które powinien był zgłosić, to grozi mu odpowiedzialność administracyjna na podstawie art. 83 ust. 4 lit. a RODO.

Pozornie rzecz wydaje się prosta. Należy się jednak zastanowić nad tym, co się dzieje, jeżeli administrator nie dowiedział się o naruszeniu ochrony danych osobowych. Prześledźmy.

– Najpierw ma miejsce naruszenie ochrony danych osobowych.
– Następnie administrator dowiaduje się o zaistnieniu (tego) naruszenia ochrony danych osobowych.
– Następnie administrator dokonuje oceny ryzyka naruszenia praw i wolności osób fizycznych.
– Następnie administrator ustala, że poziom ryzyka naruszenia praw i wolności osób fizycznych nie jest niski.

W związku z tym, że poziom ryzyka naruszenia praw i wolności osób fizycznych nie jest niski, to administrator ma obowiązek zgłosić naruszenie do PUODO. Jeżeli Administrator nie zgłosi naruszenia do PUODO, to naraża się na odpowiedzialność administracyjną. Zwracam jednak uwagę na fakt, że obowiązek zgłoszenia naruszenia w terminie określonym jako *bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia* należy zrealizować właśnie we wskazanym terminie. Pozornie. Twierdzenie to stanowi truizm, jednak też jedynie pozornie. Żeby obowiązek wskazany w przepisie rzeczywiście musiał być zrealizowany przez administratora czy też, innymi słowy, żeby na administratorze spoczywał obowiązek wynikający z przepisów, to termin wskazany w przepisie musi zacząć biec.

Zwracam uwagę na fakt, że wskazany w przepisie termin biegnie nie od momentu zaistnienia naruszenia ochrony danych osobowych, ale że biegnie on od momentu stwierdzenia naruszenia ochrony danych osobowych.

Jeżeli zatem naruszenie ochrony danych osobowych ma miejsce i jednocześnie nie zostanie ono stwierdzone przez administratora, to na administratorze tym nie spoczywa obowiązek zgłoszenia naruszenia organowi nadzorczemu. Wniosek ten może wydawać się dziwacznie, jednak wynika on w sposób oczywisty z drobiazgowej analizy przepisów.

Uczciwość wymaga, by wskazać że autorzy czeskiego komentarza twierdzą[294] może nie przeciwnie, ale jednak w sposób nieco niepokojący, z punktu widzenia wyprowadzonej tu tezy. Uważają oni bowiem, że jeżeli administrator nie stwierdzi naruszenia, to nie zwalnia go to z odpowiedzialności za naruszenie RODO, aczkolwiek jednocześnie należy wskazać na fakt, że jako przepisy, których naruszenie może być u źródłem odpowiedzialności, czescy autorzy wskazują art. 24 RODO i art. 32 RODO, czyli – jak się wydaje – źródło odpowiedzialności widzą raczej w niewłaściwej ocenie ryzyka przetwarzania danych osobowych i niewłaściwym zabezpieczeniu tych danych niż w niezgłoszeniu naruszenia ochrony danych osobowych, które powinno zostać zgłoszone organowi ochrony danych.

Być może wypowiedź czeskiej doktryny nie powinna niepokoić. Jeżeli wypowiedź tę przeanalizujemy spokojnie, to okazuje się, że czescy autorzy formułują kilka osobnych myśli.

– Zrazu zwracają uwagę na fakt, że może się zdarzyć, iż administrator nie dowie się o naruszeniu ochrony danych osobowych. Jest to myśl pierwsza.
– Następnie zwracają uwagę na fakt, że tego, iż administrator nie dowie się o naruszeniu ochrony danych osobowych, nie wynika, iż zwalnia go to z odpowiedzialności związanej z naruszeniem RODO. Jest to myśl druga.
– W końcu zwracają uwagę na fakt, że odpowiedzialność może wynikać z naruszenia art. 32 RODO lub art. 24 RODO.

Jeżeli myśl czeskich autorów uporządkujemy we wskazany sposób, to przestaje ona niepokoić i okazuje się że nie stoi ona wcale w sprzeczności, o którą zrazu ją podejrzewałem

Należy zwrócić uwagę na to, że Grupa Robocza art. 29, w istocie prawdopodobnie prezentuje ten sam pogląd. W dokumencie wydanym przez ten podmiot czytamy bowiem: *To, kiedy dokładnie można uznać, że administrator „stwierdził" wystąpienie określonego naru-*

[294] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit., s. 297.

szenia, będzie zależało od okoliczności, w jakich doszło do tego naruszenia. W niektórych przypadkach wystąpienie naruszenia można stosunkowo łatwo stwierdzić już na początku, natomiast w innych ustalenie, czy doszło do ujawnienia danych osobowych, może wymagać czasu. W tym kontekście powinno się jednak położyć nacisk na szybkie zbadanie danego incydentu w celu ustalenia, czy faktycznie doszło do naruszenia ochrony danych osobowych, a jeżeli tak – podjąć działania zaradcze i, w razie konieczności, zgłosić naruszenie[295]. Jak widać, Grupa Robocza prowadzi rozważania, zastanawiając się nad działaniami administratora od momentu, w którym „doszło do tego naruszenia". Grupa Robocza pisze o położeniu nacisku na szybkie zbadanie incydentu, z czym należy się zgodzić, z jednym jednak zastrzeżeniem. Otóż administrator może po prostu nie wiedzieć, że incydent miał miejsce. Administrator nie wie, że incydent miał miejsce, nie może więc zastanowić się, czy incydent naruszeniem był, czy nie był, ponieważ nie ma takiej szansy.

Na marginesie prowadzonych rozważań warto zastanowić się nad jednym jeszcze pokrewnym zagadnieniem. Należy się otóż zastanowić, czy na administratorze spoczywa obowiązek aktywnego działania podejmowane w celu wykrycia naruszeń ochrony danych. Otóż ani z art. 33 RODO, ani z art. 34 RODO obowiązek taki nie wynika, co jednak nie znaczy, że zagadnienie wykrywania naruszeń ochrony danych administrator może bagatelizować. Przede wszystkim niewykrycie naruszenia ochrony danych może być uznane za naruszenie art. 24 RODO. Z przepisu tego wynika, że administrator ma obowiązek wdrożyć *odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z* RODO.

Jeżeli zatem ma miejsce naruszenie i administrator go nie wykryje i nie zgłosi, to:

– administrator raczej nie zostanie ukarany za niezgłoszenie (wyjaśniam to wyżej – termin do zgłoszenia nie zaczął nigdy biec),
– raczej nie zostanie ukarany za samo niewykrycie (bo nie dostrzegam przepisu, który przewidywałby karę za niewykrycie naruszenia),
– ale za niewdrożenie procedury mającej na celu wykrycie naruszenia, administrator może zostać ukarany.

[295] Grupa Robocza art. 29, op. cit., s. 12.

Co więcej, w ostatniej z opisywanych sytuacji, kiedy administrator może zostać ukarany, wykrycie, że naruszenie miało miejsce i go nie zgłoszono, bo go nie wykryto, może jak najbardziej być wskaźnikiem na naruszenie art. 24 RODO przez administratora. Nie zgłoszono, ponieważ nie wykryto, a nie wykryto, ponieważ nie wdrożono odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO. Odpowiedzialność na podstawie art. 24 RODO nie jest tu jednak pewna i wydaje się, że może być podważona. Uważam tak, ponieważ art. 24 RODO nakłada obowiązek wdrożenia środków technicznych i organizacyjnych w pewnym konkretnym celu. Celem tym jest, by dane osobowe były przetwarzane zgodnie z RODO.

Naruszenie ochrony danych jest niewątpliwie przetwarzaniem niezgodnym z RODO, jednak zgłoszenie czy niezgłoszenie nie jest przetwarzaniem danych osobowych. Zgłoszenie naruszenia ochrony danych jest niejako metaobowiązkiem, który nie mieści się w dziedzinie przetwarzania danych osobowych i który należy zrealizować, kiedy zaszło naruszenie w dziedzinie przetwarzania danych. Artykuł 24 RODO dotyczy przetwarzania danych osobowych zgodnie z RODO, nie zaś tego, co należy czynić, kiedy przetwarzanie danych osobowych jest niezgodne z RODO ani tego czy należy niezgodności przetwarzania danych osobowych z RODO się doszukiwać. Problemowi temu jedno zdanie poświęcili[296] autorzy czescy, twierdząc krótko, że art. 33 RODO nie nakłada na administratora obowiązku wykrywania naruszeń, po czym łagodnie kierując do art. 24 RODO i do art. 32 RODO.

3.18. Art. 33 Uwaga 18

Naruszenie ochrony danych osobowych a zjawiska sztucznej inteligencji

Kilka słów warto poświęcić naruszeniu danych osobowych w związku ze zjawiskami sztucznej inteligencji. Dostrzegam tu dwie podstawowe grupy problemów, wymieniam je poniżej.

– Naruszenie ochrony danych osobowych a zjawiska sztucznej inteligencji kontrolowane przez administratora danych osobowych.

[296] M. Nuliček, J. Donát, F. Nonnemann, B. Lichnovský, J. Tomíšek, op. cit.

– Naruszenie ochrony danych osobowych a zjawiska sztucznej inteligencji kontrolowane przez podmioty lub osoby inne niż administrator danych osobowych.

Odnosząc się do pierwszego ze zjawisk, należy zadać pytanie o to, czy jeżeli zjawisko sztucznej inteligencji, czy też system sztucznej inteligencji kontrolowany przez administratora danych osobowych doprowadzi do zdarzenia, które byłoby naruszeniem ochrony danych osobowych, gdyby doprowadził do niego człowiek, pracownik administratora, to czy takie zdarzenie jest naruszeniem ochrony danych osobowych.

Wyobraźmy sobie więc, że system sztucznej inteligencji zniszczy dane osobowe na dyskach administratora. Zrobi to, ponieważ polecono mu uzyskać możliwie dużo przestrzeni dyskowej w zasobach administratora. Polecenie wyszło ze strony administratora danych osobowych, tyle że administrator ten nie miał świadomości, że system potraktuje je dosłownie. System sztucznej inteligencji w związku ze zleconym mu zadaniem skasuje posiadane przez administratora dane osobowe, znajdujące się zarówno w bazach aktualnie używanych, jak i we wszelkich kopiach (pomijam trudność czy niemożność usunięcia z tzw. twardych kopii, ale to tylko przykład).

By ustalić, czy zdarzenie było naruszeniem ochrony danych osobowych, należy zadać pytania, które wynikają z art. 4 pkt 12 RODO.

Pytanie pierwsze

Czy zdarzenie miało charakter przypadkowy lub niezgodny z prawem?

Trudno uznać, że zdarzenie było przypadkowe. Administrator posłużył się sztuczną inteligencją po to, aby uzyskać miejsce na dyskach. Zdarzenie nie miało więc charakteru przypadkowego, miało charakter celowy, tak przynajmniej się wydaje. Co ciekawe, działanie administratora było celowe, ale jego wynik można chyba określić jako przypadkowy, dlatego sygnalizuję, że celowości zdarzenia nie jestem pewien. Na rzecz można spojrzeć inaczej i uznać, że naruszeniem jest skutek, czyli (chyba) przypadkowe usunięcie danych przez sztuczną inteligencję. Piszę to niechętnie, mam bowiem poczucie, że w opisywanej sytuacji usunięcie danych przypadkowe nie było. Co więcej, działanie sztucznej inteligencji też było celowe, celem było usunięcie informacji z dysków.

Zdarzenie miało charakter niezgodny z prawem, tu wątpliwości nie mam. Przede wszystkim usunięcie danych osobowych jest ich przetwarzaniem i jako takie musi mieć podstawę w art. 6 RODO. Zależnie od sytuacji, podstawy można się doszukać w kolejnych, odpowiednich do sytuacji literach artykułu 6 ust. 1 RODO, ale nie w opisywanym stanie faktycznym. W opisywanym stanie faktycznym nie znajdziemy w art. 6 RODO podstawy prawnej do przypadkowego usunięcia danych. Poza tym zdarzenie takie narusza zasadę ograniczenia czasowego, zasadę minimalizacji i zasadę integralności. Zdecydowanie można uznać, że opisywane zdarzenie było niezgodne z prawem.

Pytanie drugie

Czy zdarzenie polegało na zniszczeniu danych osobowych? Pomijam pozostałe możliwości, ponieważ zdarzenie polegało właśnie na zniszczeniu danych osobowych, nie ma więc sensu zadawać kolejnych pytań z tej grupy.

Pytanie trzecie

Czy zdarzenie dotyczyło danych osobowych przechowywanych? I tu pomijam pozostałe możliwości, ponieważ zdarzenie dotyczyło właśnie danych osobowych przechowywanych, nie ma więc sensu zadawać kolejnych pytań z tej grupy.

Ponieważ odpowiedzi na zadane wyżej pytania brzmią twierdząco, to należy uznać, że zdarzenie jest naruszeniem ochrony danych osobowych. Powtórzmy więc wniosek w wersji pełnej. Jeżeli zjawisko sztucznej inteligencji, czy też system sztucznej inteligencji kontrolowany przez administratora danych osobowych doprowadzi do zdarzenia, które byłoby naruszeniem ochrony danych osobowych, gdyby doprowadził do niego człowiek, pracownik administratora, to takie zdarzenie **jest** naruszeniem ochrony danych osobowych.

Odnosząc się do drugiego ze zjawisk, należy zadać sobie pytanie o to, czy jeżeli zjawisko sztucznej inteligencji, czy też system sztucznej inteligencji kontrolowany przez podmiot zewnętrzny wobec administratora danych osobowych, kierowany przez, powiedzmy, naruszyciela, doprowadzi do zdarzenia, które byłoby naruszeniem ochrony danych osobowych, gdyby doprowadził do niego człowiek, to czy takie zdarzenie jest naruszeniem ochrony danych osobowych.

Wyobraźmy sobie więc, że system sztucznej inteligencji zapoznał się z danymi osobowymi. Pokonał zabezpieczenia administratora i skopiował dane osobowe.

By ustalić, czy zdarzenie było naruszeniem ochrony danych osobowych należy zadać pytania, które wynikają z art. 4 pkt 12 RODO.

Pytanie pierwsze

Czy zdarzenie miało charakter przypadkowy lub niezgodny z prawem?

Zdarzenie było skutkiem działania podmiotu innego niż administrator danych osobowych. Z puntu widzenia tego innego podmiotu zdarzenie może nie było przypadkowe. Z punktu widzenia administratora danych osobowych zdarzenie przypadkowe było

Uważam, że zdarzenie takie było również niezgodne z prawem, nie znajduję bowiem dla niego uzasadnienia w art. 6 ust. 1 RODO.

Zdarzenie miało charakter niezgodny z prawem. Przede wszystkim usunięcie danych osobowych jest ich przetwarzaniem i jako takie musi mieć podstawę w art. 6 RODO. Zależnie od sytuacji podstawy można się doszukać w kolejnych, odpowiednich do sytuacji literach artykułu 6 ust. 1 RODO, ale nie w opisywanych stanie faktycznym. W opisywanym stanie faktycznym nie znajdziemy w art. 6 podstawy prawnej do przypadkowego usunięcia danych. Poza tym zdarzenie takie narusza zasadę ograniczenia czasowego, zasadę minimalizacji i zasadę integralności. Zdecydowanie można uznać, że opisywane zdarzenie było niezgodne z prawem.

Pytanie drugie

Czy zdarzenie polegało na nieuprawnionym dostępie do danych osobowych? Wydaje się, że tak właśnie było. Mam tu pewien niepokój związany z tym, czy nieuprawniony dostęp to tylko dostęp uzyskany przez nieuprawnioną osobę, czy również przez inne zjawisko, takie jak w opisywanym przypadku systemu sztucznej inteligencji, czy jakiekolwiek inne zjawisko sztucznej inteligencji. Piszę, że wydaje mi się, że nieuprawniony dostęp zaszedł, zastrzegam jednak, że nie jestem tego pewien. Faktem jest, że trudno jest znaleźć miejsce w art. 6 RODO, by zalegalizować opisywany tu dostęp, ale mówimy wtedy o zjawisku zgodności z prawem. Teraz zastanawiam się, czy zaszedł nieuprawniony dostęp lub (może) nieuprawnione ujawnienie. Raczej

widziałbym tu dostęp, ponieważ ujawnienie wydaje się być czymś, co jest inicjowane raczej przez administratora niż przez naruszyciela, ale nie upierałbym się przy tym, przynajmniej dla potrzeb prowadzonego tu rozważania. Problem widzę gdzie indziej. Łatwo jest orzec, że zaszedł nieuprawniony dostęp lub (ewentualnie) nieuprawnione ujawnienie, ale zastanówmy się nad tym, czy istnieje mechanizm wynikający z przepisów RODO, za pomocą którego można sprawić, że dostęp uzyskany przez zjawisko sztucznej inteligencji z nieuprawnionego staje się uprawnionym. Jeżeli dokładnie przyjrzymy się art. 29 RODO i art. 32 ust. 4 RODO, to na gruncie art. 32 ust. 4 RODO nie sposób nie ujrzeć, że osoba, która jest uprawniana do przetwarzania danych przez administratora danych osobowych to osoba fizyczna. Tak zwane upoważnienie do przetwarzania danych osobowych, niezależnie od tego, jak zjawisko to nazwiemy, jest nadawane osobie fizycznej. Nie ma – a przynajmniej ja jej nie znam – praktyki upoważniania do przetwarzania danych osobowych nadawanych zjawiskom sztucznej inteligencji. Być może jest to coś, o czym należy pomyśleć, o czym powinien pomyśleć prawodawca, ale na razie, przynajmniej na gruncie RODO o tym nie pomyślano. Idąc dalej tym tropem… Nie da się upoważnić zjawiska sztucznej inteligencji do przetwarzania danych osobowych, a skoro tak, to być może kiedy sztuczna inteligencja niekontrolowana przez administratora, „obca" wobec administratora danych osobowych sztuczna inteligencja uzyska dostęp do danych osobowych, to nie stanowi to dostępu nieuprawnionego. Kwestia ta powinna zapewne zostać uregulowana, ale na razie, kiedy patrzę na RODO, to regulacji takowej nie widzę.

Można tu poczynić unik i stwierdzić, że jeżeli obca wobec administratora sztuczna inteligencja uzyska dostęp do danych osobowych, to może ona następnie ujawnić te dane osobie fizycznej czy to osobie, która tę inteligencję kontroluje, czy może wybranej przez siebie osobie fizycznej (dziś wydaje się to fantazją, za kilka lat może nie), więc zdarzenie można zakwalifikować jako zagrożenie nieuprawnionym dostępem do danych osobowych lub zagrożenie nieuprawnionym ujawnieniem danych osobowych. Można poczynić taki unik, ale wiele on nie wyjaśnia, czyniąc bowiem unik, zmieniamy okoliczności zdarzenia – z dostępu uzyskanego przez sztuczną inteligencję przechodzimy na zagrożenie dostępem uzyskanym przez osobę fizyczną. Dotykamy tu też spraw takich, jak ogólna sztuczna inteligencja

(*general* lub *strong*) i wąska sztuczna inteligencja (*narrow* lub *weak*)[297]. Wydaje się przy tym, że dla poruszanych tu zagadnień kluczowe nie byłoby, czy w interakcję z danymi wchodzi ogólna czy wąska sztuczna inteligencja, ale raczej czy byłaby to sztuczna inteligencja autonomiczna[298] czy nie.

Można też poczynić inny unik i w ogóle zmienić okoliczności zdarzenia i uznać, że obca sztuczna inteligencja zniszczyła dane osobowe. Można to uczynić, ale to nie rozwiązuje problemu, nie stanowi bowiem odpowiedzi na pytanie o to, czy sztuczną inteligencję można uprawnić do danych osobowych.

Pytanie trzecie

Czy zdarzenie dotyczyło danych osobowych przechowywanych? I tu pomijam pozostałe możliwości, ponieważ zdarzenie dotyczyło właśnie danych osobowych przechowywanych, nie ma więc sensu zadawać kolejnych pytań z tej grupy. Odpowiedź brzmi twierdząco, jednak oczywiście jedynie odpowiedź na to pytanie.

Prowadzone wyżej rozważania prowadzą do ciekawego **wniosku**. Otóż jeżeli zjawisko sztucznej inteligencji czy też system sztucznej inteligencji obcy wobec administratora uzyska dostęp do danych osobowych, to można mieć wątpliwość, czy zdarzenie takie jest naruszeniem ochrony danych osobowych na gruncie art. 4 pkt 12 RODO. Zdarzenie takie jest zapewne niewłaściwe, niepożądane, ale zdecydowanie nie mogę uczciwie powiedzieć, że zdarzenie takie jest naruszeniem ochrony danych osobowych na gruncie art. 4 pkt 12 RODO.

Tytułem uzupełnienia warto zauważyć, że jeżeli zdarzenie polega na zniszczeniu danych osobowych przez obcą wobec administratora danych osobowych sztuczną inteligencję, to takie zdarzenie jest naruszeniem ochrony danych osobowych.

Prowadzone tu rozważania pozwalają może nie na postawienie wniosków, które idą daleko, ale na pewno na przewidywanie, że przy dłuższych badaniach, wnioski takie są możliwe[299]. Należy zwrócić

---

[297] Podziały z: W. Barfield, U. Pagallo. *Advanced Introduction to Law and Artifficial Intelligence*. Cheltenham i Northampton Massachusetts 2020, s. 5. Tłumaczenie: J.Rz.

[298] W. Barfield, U. Pagallo, op. cit., s. 4. Tłumaczenie: J.Rz.

[299] F. Kasl, *Porušení bezpečnosti osobních údajů w kontextu Internetu věcí*, Masarykova univerzita 2021, s. 22.

uwagę, że jeżeli zjawisko sztucznej inteligencji, system sztucznej inteligencji działa w oderwaniu od człowieka i wykonuje jakieś działania, to zbliżamy się do tego, co bywa nazywane Internetem rzeczy. Wyżej zastanawiam się nad tym, czy jeżeli sztuczna inteligencja obca wobec administratora danych osobowych uzyska dostęp do danych osobowych, to czy zdarzenie takie jest naruszeniem danych osobowych. Mamy więc zderzenie przetwarzania danych osobowych przez administratora z Internetem rzeczy.

Zróbmy jednak jeszcze jeden krok, wyobraźmy sobie, że zbiór danych osobowych jest kontrolowany przez sztuczną inteligencję i że żadnego poza nią administratora zidentyfikować nie sposób. Warto zadać tu dwa pytania.

Prawdopodobnie mniej ważne pytanie jest pytaniem o to, czy gdyby sztuczna inteligencja kontrolowała przetwarzanie danych osobowych i nie dałoby się zidentyfikować administratora i inna sztuczna inteligencja (lub po prostu osoba fizyczna) uzyskałaby dostęp do tych kontrolowanych danych osobowych w sposób nieautoryzowany przez sztuczną inteligencję kontrolującą przetwarzanie danych, to czy takie zdarzenie mogłoby być naruszeniem ochrony danych osobowych.

Prawdopodobnie ważniejszym pytaniem jest: czy gdyby sztuczna inteligencja kontrolowała przetwarzania danych osobowych i nie dałoby się zidentyfikować administratora, to czy taka sztuczna inteligencja byłaby administratorem danych osobowych.

Pojawia się tu pytanie uzupełniające, a mianowicie pytanie o to, kto w takim razie byłby w takiej sytuacji administratorem danych osobowych i czy byłby nim ktokolwiek.

Nie ma co ukrywać, że prowadzone powyżej rozważania prowadzą nas do jednego jeszcze pytania, a mianowicie pytania o to, czy sztuczna inteligencja, zjawisko sztucznej inteligencji, system sztucznej inteligencji może być administratorem danych osobowych.

Pozostaje się tu zgodzić z czeskim autorem, który w zjawisku Internetu rzeczy dostrzega przemianę nie tylko techniczną[300], że zarówno Sztuczna inteligencja przyczynia się do poważnych zmian w prawie, w tym szczególnie w prawie ochrony danych osobowych. Podobną myśl dostrzegam u D. Lubasza, który dopuszcza, że mogą pojawić się głosy o braku *wystarczających gwarancji i ochrony pod-*

[300] Ibidem, s. 123.

miotów danych w związku z przetwarzaniem ich danych z wykorzystaniem mechanizmów sztucznej inteligencji na gruncie obecnej regulacji. Zgadzam się tu ze wskazanym autorem i głos taki właśnie podnoszę. Powyżej zająłem się ważnym, ale jednak tylko wycinkiem zjawisk, które wynikać mogą z zetknięcia ochrony danych osobowych i prawa ochrony danych osobowych ze zjawiskami sztucznej inteligencji, ale już przy takim nawet wyrywkowym spojrzeniu widzę, że brak jest osadzenia zjawisk sztucznej inteligencji w prawie analogicznym do tego, w jaki sposób osadzone są w nim osoby fizyczne.

Widzę tu dwa możliwe rozwiązania. Pierwszym jest ustanowienie w odniesieniu do sztucznej inteligencji instytucji analogicznej wobec osobowości prawnej. Drugim jest powiązanie sztucznej inteligencji z osobami, które się nią posługują, co może się okazać trudne, kiedy pojawią się autonomiczne zjawiska sztucznej inteligencji. Trzecim jest stworzenie przepisów odnoszących się do zjawiska sztucznej inteligencji w obrębie poszczególnych podgałęzi prawa.

4. Art. 33 ust. 1 Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa I

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

Obecność w przepisie pogrubionych słów: ***W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki […] zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55*** skutkuje po stronie administratora i osób, których dane dotyczą, w sposób wskazany poniżej.

Jeżeli ma miejsce naruszenie ochrony danych osobowych, to **administrator ma** je **obowiązek** zgłosić organowi nadzorczemu, czyli w polskich warunkach – PUODO. **Administrator ma obowiązek** dokonać tego zgłoszenia bez zbędnej zwłoki.

Jeżeli ma miejsce naruszenie ochrony danych osobowych, to **osoba, której dane dotyczą, ma prawo** do tego, by administrator zgłosił naruszenie organowi nadzorczemu, czyli w polskich warunkach – PUODO. Osoba, której dane dotyczą, ma prawo, by administrator zgłosił naruszenie bez zbędnej zwłoki.

Obecność w przepisie pogrubionych słów: *[...] administrator* ***bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia*** *– zgłasza je [...]* skutkuje po stronie administratora i osób, których dane dotyczą, w sposób wskazany poniżej.

Administrator ma obowiązek zgłosić naruszenie bez zbędnej zwłoki. Przez obowiązek zgłoszenia naruszenia bez zbędnej zwłoki należy rozumieć obowiązek zgłoszenia rzeczywiście bez wspomnianej zbędnej zwłoki, przy czym o ile to jest możliwe, to nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Należy tu poczynić pewne zastrzeżenie – otóż obowiązek zgłoszenia we wskazanym w przepisie 72 godzinnym terminie, obowiązuje, o ile zgłoszenie w tym terminie jest możliwe. Trudno powiedzieć, co miałoby być powodem niemożliwości zgłoszenia, jeżeli jednak zgłoszenie w terminie wskazanym w przepisie nie jest możliwe, to na administratorze nie spoczywa obowiązek zgłoszenia w tym terminie.

Można postawić tezę, że obowiązek zgłoszenia w terminie 72-godzinnym jest obowiązkiem pod warunkiem rozwiązującym. Obowiązek zachodzi, chyba, że okaże się, że zgłoszenie w terminie 72 godzin jest niemożliwe, wtedy warunek się realizuje i powoduje, że obowiązek przestaje mieć miejsce.

Osoba, której dane dotyczą, ma prawo do tego, by administrator zgłosił naruszenie bez zbędnej zwłoki, o ile to możliwe, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

Można postawić tezę, że prawo do tego, by administrator zgłosił naruszenie w terminie 72-godzinnym jest prawem pod warunkiem rozwiązującym. Prawo przysługuje, chyba że okaże się, że zgłoszenie w terminie 72 godzin jest niemożliwe, wtedy warunek się realizuje i powoduje, że prawo przestaje przysługiwać.

Jeżeli ma miejsce naruszenie ochrony danych osobowych, to **administrator ma** je **obowiązek** zgłosić organowi nadzorczemu, czyli w polskich warunkach – PUODO. **Administrator ma obowiązek** dokonać tego zgłoszenia bez zbędnej zwłoki.

Jeżeli ma miejsce naruszenie ochrony danych osobowych, to **osoba, której dane dotyczą, ma prawo** do tego, by administrator zgłosił naruszenie organowi nadzorczemu, czyli w polskich warunkach –

PUODO. Osoba, której dane dotyczą, ma prawo, by administrator zgłosił naruszenie bez zbędnej zwłoki.

Obecność w przepisie pogrubionych słów: *[...] administrator [...] zgłasza je organowi [...]* ***chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych***. *[...]* skutkuje po stronie administratora i osób, których dane dotyczą, w sposób wskazany poniżej.

Jeżeli jest to mało prawdopodobne, że naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, to **obowiązek** zgłoszenia naruszenia ochrony danych PUODO, **nie spoczywa na administratorze**.

Jeżeli jest to mało prawdopodobne, że naruszenie ochrony danych osobowych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, to **prawo** do tego, by administrator zgłosił naruszenie PUODO, **nie przysługuje osobie, której dane dotyczą**.

Obecność w przepisie pogrubionych słów: *[...]* ***Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia***. skutkuje po stronie administratora i osób, których dane dotyczą, w sposób wskazany poniżej.

Jeżeli zgłoszenie przekazano organowi nadzorczemu po upływie 72 godzin, to **na administratorze spoczywa obowiązek** dołączenia do zgłoszenia wyjaśnienia przyczyn opóźnienia.

Jeżeli zgłoszenie przekazano organowi nadzorczemu po upływie 72 godzin, to **osobie, której dane dotyczą, przysługuje prawo** do tego, by administrator dołączył do zgłoszenia wyjaśnienie przyczyn opóźnienia.

5. Art. 33 ust. 1 Konkretyzacja zasad

Art. 33 ust. 1 RODO, do pewnego stopnia postrzegany łącznie z art. 33 ust. 2 RODO konkretyzuje wymienione poniżej zasady.

Zasada zgodności z prawem

Trudno dopatrzeć się istotnego związku art. 33 ust. 1 RODO z zasadą. Zgłoszenie lub niezgłoszenie, sam namysł nad ewentualnym zgłoszeniem do PUODO następują po tym, jak zaistniało naruszenie ochrony danych osobowych, czyli kiedy dane zostały (najprawdopodobniej) przetworzone niezgodnie z prawem, lub kiedy zaistniało zagrożenie przetworzeniem danych osobowych w sposób niezgodny z prawem. Właśnie w zdarzeniach, które nie skutkują niezgodnym

z prawem przetworzeniem danych osobowych, ale które grożą takim przetworzeniem, dostrzec można związek zasady z omawianym przepisem. Zdarzenie zachodzi, zdarzenie ma charakter zagrożenia naruszeniem praw i wolności, w tym naruszeniem zasady zgodności z prawem. Ocena takiego naruszenia, samo jego odnotowanie oraz zwłaszcza środki podjęte po naruszeniu, aby takie naruszenie więcej nie miało miejsca, sprzyjają realizacji zasady zgodności z prawem. Związek ten – jak widać – nie jest zbyt silny, jakiś jednak zachodzi.

Mocniejszy związek zachodzący między zasadą zgodności z prawem a art. 33 ust. 1 RODO jest taki, że kiedy zaistnieje naruszenie ochrony danych osobowych, wtedy administrator przystępuje do oceny ryzyka naruszenia praw i wolności osoby, której dane dotyczą. Jednym z tych praw jest prawo do przetwarzania danych osobowych w sposób zgodny z prawem wynikające z art. 5 ust. 1 lit. a RODO. Analogiczny związek zachodzi między pozostałymi zasadami a art. 33 ust. 1 RODO.

Przypominam, że obowiązek dokonywania oceny ryzyka naruszenia praw i wolności osób fizycznych przez pryzmat praw i wolności zapisanych w zasadach z art. 5 RODO wynika z koncepcji racjonalnego prawodawcy i z dyrektywy języka prawnego. Jeżeli racjonalny prawodawca umieszcza prawa i wolności w akcie prawnym, w tym przypadku w art. 5 RODO i następnie ten sam racjonalny prawodawca odsyła w różnych miejscach tego samego aktu prawnego do praw i wolności, to oczywiste jest, że odsyła do praw i wolności, które jako prawodawca w przedmiotowym akcie prawnym umieścił. Wspomniane prawa i wolności dla porządku wskazuję poniżej.

Zasada rzetelności

Przepis ma pewien związek z zasadą rzetelności. Jeżeli administrator informuje organ o naruszeniu, to może to doprowadzić (choć z samego przepisu to nie wynika) do poinformowania o naruszeniu, co z kolei skutkuje, że osoba zostaje (może po raz kolejny) poinformowana o przetwarzaniu, co sprzyja realizacji zasady rzetelności.

Zasada przejrzystości

Jednocześnie jeżeli osoba, której dane dotyczą, wie o przetwarzaniu danych, to może ją to zachęcić do skorzystania na przykład z uprawnienia wynikającego z art. 15 RODO, co z kolei sprzyja realizacji zasady przejrzystości.

Zasada minimalizacji danych
Zasada prawidłowości
Zasada ograniczenia przechowywania
Zasada ograniczenia celu

Również tutaj trudno jest dopatrzeć się istotnego związku art. 33 ust. 1 RODO z zasadami. Jedyny związek, który dostrzegam, jest taki, że namysł nad naruszeniem ochrony danych osobowych a zdarzeniom mającym charakter takich naruszeń. Faktem jest, że namysł taki ma miejsce w sytuacji naruszenia lub ewentualnego naruszenia i o ile w odniesieniu do przedmiotowego ocenianego naruszenia ochrony danych osobowych, związek z zasadami jest słaby, o tyle sama koncepcja czy też – już w konkretnej sytuacji – perspektywa dokonywania kolejnych ocen, gdyby podobne naruszenie miało zaistnieć, mogą sprzyjać realizacji wskazanych zasad.

Zasada integralności
Zasada poufności

Mam na uwadze, że ocena skutków naruszenia ma miejsce po zaistnieniu naruszenia. Zachodzi naruszenie ochrony danych osobowych i wskutek tego faktu administrator przystępuje do oceny ryzyka naruszenia praw i wolności osoby, której dane dotyczą. Wszystko to ma miejsce już po zaistnieniu naruszenia, a tak naprawdę zwykle po zaistnieniu obydwu naruszeń, czyli naruszenia ochrony danych osobowych i naruszenia (bądź co najmniej ryzyka naruszenia) praw i wolności osoby, której dane dotyczą. Mimo tej świadomości, mam jednak poczucie, że wszelkie oceny związane czy to z naruszeniem ochrony danych osobowych, czy to z naruszeniem praw i wolności mają silniejszy związek ze wskazanymi zasadami niż z pozostałymi zasadami. Mam świadomość, że trudno jest mi zasygnalizowane poczucie uzasadnić w sposób przekonujący. Wydaje się, że źródłem mojego poczucia dotyczącego związku wskazanych zasad z art. 33 ust. 1 RODO jest fakt, że jednak najczęściej – jak się wydaje – naruszenia ochrony danych osobowych dotyczą sfery poufności i integralności. Drugim argumentem, który przemawia za moim prezentowanym tu odczuciem, jest analiza treści art. 4 pkt 12 RODO, czyli definicji naruszenia ochrony danych osobowych. Zdarzenia, stany, zjawiska – wskazane w art. 4 pkt 12 RODO mają charakter zdarzeń, stanów, zjawisk związanych

właśnie ze sferą integralności lub sferą poufności danych osobowych. Po pewnym namyśle, drugi argument wydaje się być racjonalniejszy.

Zasada odpowiedzialności administratora danych (osobowych)

Realizacja obowiązku denuncjacyjnego może w prosty sposób doprowadzić do poniesienia przez administratora danych odpowiedzialności administracyjnej.

Zasada rozliczalności (Artykuł 5 ust. 2 RODO)

Artykuł 33 ust. 5 jest – na co zwraca uwagę W. Chomiczewski – *[...] przejawem realizacji zasady rozliczalności*[301]. Wskazany autor ma tu rację. Z przepisu wynika obowiązek dokumentowania naruszeń ochrony danych, co idealnie wpisuje się w obowiązek dokumentowania realizacji zasad wynikający z art. 5 ust. 2 RODO.

6. Art. 33 Postulaty *de lege ferenda*

6.1. Art. 33 Postulat 1

Jak liczyć termin 72-godzinny

Wyżej w analizie (*1. Art. 33 ust. 1. Analiza*) zastanawiam się nad tym, od jakiego momentu należy liczyć 72-godzinny termin do zgłoszenia naruszenia do PUODO. Wnioski nie są optymistyczne. Uczciwie patrząc, nie do końca wiadomo, jak termin ten liczyć należy. Wydaje się, że dobrze by było, gdyby przepis to w jakiś nieco bardziej precyzyjny sposób precyzował. Ważny jest nie tylko termin, ale i to, jak go liczyć należy. Można sobie wyobrazić, że przepis zawiera regulację, która właśnie precyzuje sposób liczenia terminu. Projekt takiej regulacji wskazuję poniżej, jednak raczej jako luźną propozycję czy też zaproszenie do dyskusji. Przepis warto by zmienić, by termin był łatwiejszy do liczenia, czy zmienić go akurat tak, jak proponuję – inna sprawa.

W związku z powyższym postuluję nowelizację art. 33 ust. 1 RODO we wskazany poniżej sposób.

Postuluję, by fragment przepisu, o którym tu mowa, miał postać:

[301] W. Chomiczewski, op. cit., s. 710.

„W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia **przez uprawnionego pracownika administratora** – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 […]"
(Czcionką wytłuszczoną oznaczono elementy wstawione do przepisu.)

6.2. Art. 33 Postulat 2

Wskazanie praw i wolności

W uwadze (*3.4. Art. 33 ust. 1 Uwaga 4. Prawa i wolności w RODO. Naruszenie łącznie z naruszeniem innych praw i wolności*) wywodzę, że prawa i wolności z art. 5 ust. 1 RODO są istotne, ponieważ jeżeli naruszeniem z art. 4 pkt 12 RODO naruszono inne prawa i wolności, to te z art. 5 ust. 1 RODO naruszono na pewno (podobnie rzecz ma się z zagrożeniem naruszeniem praw i wolności).

W związku z powyższym postuluję nowelizację art. 33 ust. 1 RODO we wskazany poniżej sposób.

Postuluję, by fragment przepisu, o którym tu jest mowa, miał postać:
„W przypadku naruszenia ochrony danych osobowych, administrator […] zgłasza je organowi nadzorczemu […] chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. **Przez prawa i wolności osób fizycznych, o których mowa w przepisie, należy rozumieć zasady dotyczące przetwarzania danych osobowych zapisane w art. 5 ust. 1 RODO**" .
(Czcionką pogrubioną oznaczono elementy dodane do przepisu.)

6.3. Art. 33 Postulat 3

Uczytelnienie przepisu

Zasadnicze studia nad definicją naruszenia ochrony danych osobowych prowadzę w jednej z wcześniejszych książek z cyklu, w której omówieniu definicji naruszenia poświęcam 44 strony. Wyżej w uwadze (*3.11. Art. 33 Uwaga 11. Naruszenie ochrony danych osobowych – metoda ustalenia*) i w uwadze (*3.13. Art. 33 Uwaga 13. Naruszenie zdaniem EROD. Polemika*) ponownie, w zakresie koniecznym dla

prowadzonych w niniejszej publikacji wywodów, zastanawiam się nad definicją naruszenia ochrony danych osobowych. Stawiam tam kilka postulatów nowelizacyjnych, nie widzę więc sensu, by je tu powtarzać, tym bardziej że mimo upływu około trzech lat od pisania wskazanej książki (publikacja w 2020 roku), moje zdanie na temat ewentualnej nowelizacji w zasadzie się nie zmieniło. Lektury utwierdziły mnie jedynie w przekonaniu, że przepis bywa niewłaściwie rozumiany. Skoro przepis bywa niewłaściwie rozumiany, to należy go zmienić tak, by był dobrze rozumiany. By nie powtarzać ustaleń, które podtrzymuję, rzecz sygnalizuję jedynie poniżej, skrótowo.

Po pierwsze, należy usunąć z przepisu pojęcie „naruszenie bezpieczeństwa". Pojęcie to jest nieostre, problemy z jego interpretacją mogą prowadzić do tego, że konkretne zdarzenie, które spełnia warunki naruszenia ochrony danych osobowych, nie zostanie uznane za naruszenie ochrony danych osobowych, ponieważ nie zostanie uznane za naruszenie bezpieczeństwa. W związku z tym należy słowa „naruszenie bezpieczeństwa" zastąpić słowem: „zdarzenie". Piszę o tym we wcześniejszej publikacji (*6.1 Art. 6. pkt 12. Postulat 1. Usunięcie z przepisu błędu „nieznane przez nieznane"*)[302]. W postulacie, na który wskazuję, zwracam uwagę na błąd „nieznane przez nieznane" znajdujący się w przepisie. Aktualnie dodatkowo dostrzegam to, co zapisałem powyżej, niewłaściwe rozumienie pojęcia „naruszenie bezpieczeństwa" może doprowadzić do niezastosowania przepisu, a tym samym do naruszenia zasad z art. 5 RODO, w zakresie odpowiednim do naruszenia.

Po drugie, należy tak zmienić przepis, by nie było wątpliwości, że nie tylko zdarzenia wskazane w przepisie, ale że już samo zagrożenie zaistnieniem któregokolwiek z tych zdarzeń stanowi naruszenie ochrony danych osobowych. W tym celu należy słowa: „prowadzące do" zastąpić słowami, które nie pozostawiają swobody interpretacyjnej, np. słowami: „które polega na lub zagraża". Piszę o tym, proponując przy tym nieco inne słowa, we wcześniejszej publikacji (*6.2 Art. 6. pkt 12. Postulat 2. Rozjaśnienie treści przepisu*[303]). Użycie konkretnych słów nie jest tu istotne, o ile tylko słowa użyte w znowelizowanym

[302] J. Rzymowski, *RODO – GDPR. Przedmiot i cele…,* s. 528–529.

[303] Ibidem, 529–530.

przepisie nie pozostawiałyby pola dla niewłaściwych interpretacji omawianego przepisu.

W związku z powyższym postuluję nowelizację art. 4 pkt 12 RODO we wskazany poniżej sposób.

Postuluję, by fragment przepisu, o którym tu mowa, miał postać:

„naruszenie ochrony danych osobowych" oznacza ~~naruszenie bezpieczeństwa~~ **zdarzenie,** ~~prowadzące do~~ **które polega na lub zagraża** ~~przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu~~ **przypadkowym lub niezgodnym z prawem zniszczeniu, utraceniu, zmodyfikowaniu, nieuprawnionym ujawnieniu lub nieuprawnionym dostępie** do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych".

(Czcionką przekreśloną oznaczono elementy usunięte z przepisu, czcionką pogrubioną oznaczono elementy wstawione do przepisu.)

Artykuł 33 ust. 2 RODO

Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

1. Art. 33 ust. 2 Analiza

Z przepisu wynika obowiązek zgłoszenia naruszenia. Podmiot przetwarzający zgłasza naruszenie administratorowi danych osobowych. Obowiązek wynikający z przepisu, spoczywa na podmiocie przetwarzającym. Podmiot przetwarzający zdefiniowano w art. 4 pkt 8 RODO. Obowiązek powinien zostać zrealizowany przez podmiot przetwarzający po tym, jak podmiot ten stwierdzi naruszenie ochrony danych osobowych. Z przepisu nie wynika, że obowiązek musi być zrealizowany natychmiast po stwierdzeniu naruszenia. Obowiązek może być zrealizowany ze zwłoką, jednak – jak wynika z przepisu – zwłoka ta nie może być zbędna. Zbędność czy niezbędność zwłoki należy oceniać odpowiednio do konkretnego stwierdzonego przez podmiot przetwarzający naruszenia. Należy podkreślić, że podmiot przetwarzający zgłasza administratorowi naruszenie ochrony danych niezależnie od tego, jaki poziom w kontekście tego naruszenia przyjmuje ryzyko naruszenia praw i wolności osób fizycznych. Zgłoszenie naruszenia przez podmiot przetwarzający administratorowi daje administratorowi możliwość dokonania oceny poziomu ryzyka naruszenia praw i wolności i tym samym podjęcia dalszych decyzji, np. o zgłoszeniu naruszenia organowi nadzorczemu, a to o niezgłoszeniu organowi nadzorczemu, a to o poinformowaniu osób, których dane dotyczą, a to o nieinformowaniu osób, których dane dotyczą.

Na doniosłość obowiązku zgłoszenia naruszenia przez podmiot przetwarzający, uwagę zwraca P. Fajgielski[304].

[304] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679…,* Kom. do art. 33.

Ze słów pogrubionych w cytacie: ***Podmiot przetwarzający*** *po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi*, wnioskujemy, że obowiązek wynikający z dalszej części przepisu, spoczywa na podmiocie przetwarzającym. Podmiot przetwarzający zdefiniowano w art. 4 pkt 8 RODO.

Ze słów pogrubionych w cytacie: ***Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych*** *bez zbędnej zwłoki zgłasza je administratorowi*, wnioskujemy, że obowiązek wynikający z dalszej części przepisu powinien zostać zrealizowany przez podmiot przetwarzający po tym, jak podmiot ten stwierdzi naruszenie ochrony danych osobowych.

Podobnie jak w odniesieniu do art. 33 ust. 1 RODO, nie wiadomo, jaki moment należy uznać za stwierdzenie naruszenia ochrony danych osobowych.

Artykuł 33 ust. 2 RODO zawiera nakaz zgłoszenia naruszenia administratorowi przez podmiot przetwarzający. Nakaz ten jest prosty do zrozumienia, niestety jednak jedynie pozornie.

Ze słów pogrubionych w cytacie: ***Podmiot przetwarzający*** *po stwierdzeniu naruszenia ochrony danych osobowych* ***bez zbędnej zwłoki*** *zgłasza je administratorowi*", wnioskujemy, że obowiązek wynikający z dalszej części przepisu powinien zostać zrealizowany bez zbędnej zwłoki. Z przepisu nie wynika, że obowiązek musi być zrealizowany natychmiast po stwierdzeniu naruszenia. Obowiązek może być zrealizowany ze zwłoką, jednak – jak wynika z przepisu – zwłoka ta nie może być zbędna. Zbędność czy niezbędność zwłoki należy oceniać odpowiednio do konkretnego stwierdzonego przez podmiot przetwarzający naruszenia.

Na niezwykle ciekawą, choć z pozoru oczywistą rzecz zwraca uwagę P. Fajgielski[305]. Otóż podmiot przetwarzający nie jest zobowiązany do poinformowania o naruszeniu w ciągu 72 godzin. Przepis stanowi tylko o konieczności informowania bez zbędnej zwłoki, jednak nie doprecyzowuje terminów. Należy tu zwrócić uwagę na pewien szczegół. Otóż w art. 33 ust. 1 RODO mowa jest o stwierdzeniu naruszenia (pod katem zgłoszenia go organowi) i w art. 33 ust. 2 RODO mowa jest o stwierdzeniu naruszenia (pod kątem zgłoszenia go administratorowi przez podmiot przetwarzający). Zarówno w jednym, jak

[305] Ibidem.

i w drugim przepisie mowa jest o stwierdzeniu naruszenia ochrony danych osobowych. Wydaje się, że faktów tych nie należy utożsamiać, jedno bowiem stwierdzenie naruszenia to stwierdzenie naruszenia przez administratora, drugie stwierdzenie naruszenia, to stwierdzenie naruszenia przez podmiot przetwarzający.

Należy się jednak zastanowić nad jednym. Otóż podmiot przetwarzający stwierdza naruszenie i informuje o tym administratora. Informuje bez zbędnej zwłoki, ale nie ma rąk związanych 72-godzinnym terminem, czyli teoretycznie może poinformować administratora po godzinie od stwierdzenia naruszenia, ale może też po tygodniu lub po siedmiu tygodniach lub (teoretycznie) po każdym czasie, o ile zwłoka będzie uzasadniona.

Wracając jednak do rozważań… Administrator zostaje poinformowany o naruszeniu przez podmiot przetwarzający. Następnie administrator musi podjąć decyzję, czy poinformować organ o naruszeniu czy nie, oraz czy (o tym piszę niżej przy omawianiu art. 34 RODO) poinformować osoby, których dane dotyczą. Decyzja ta uzależniona jest od poziomu ryzyka naruszenia praw i wolności osób fizycznych. Administrator musi zatem ten poziom ocenić i stosownie do niego podjąć odpowiednie decyzje. Niestety, pozostaje jeszcze kwestia terminu. Nie wiadomo, w jakim terminie administrator powinien powiadomić organ o naruszeniu (oczywiście o ile powiadomienie ma miejsce). Wydaje się, że terminy zawarte w art. 33 ust. 1 RODO należy wtedy potraktować jako wskazówki czy też jako coś na kształt terminów instrukcyjnych.

Zarówno P. Barta, P. Litwiński i M. Kawecki[306], jak i K. Wygoda[307] zwracają uwagę na motyw 85 Preambuły RODO, w którym prawodawca utożsamia reakcję na naruszenie (czy to po stronie administratora, czy to po stronie osób, których dane dotyczą) ze zgłoszeniem naruszenia organowi. Wskazani autorzy odnoszą się do powołanego motywu (tak mi się wydaje) w sposób aprobatywny. Muszę tu zgłosić swoją niezgodę. Uważam, że jedynym albo prawie jedynym celem zgłoszenia naruszenie organowi jest ułatwienie pracy organowi właśnie i ułatwienie mu nakładania kar. Uważam tak, ponieważ do-

[306] Por P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 353.

[307] K. Wygoda, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie…,* s. 349.

strzegam, że zgłoszenie naruszenia organowi może mieć miejsce (i to jeśli jest dokonane na czas) po kilkudziesięciu godzinach od zdarzenia. Jeżeli naruszenie było wygenerowane w sposób przestępczy, to to co przestępca chciał z danymi zrobić, w ciągu kilkudziesięciu godzin dawno zrobił. Jeżeli naruszenie zostało wywołane w sposób przypadkowy, to z kolei nic złego się nie stanie. Horrory związane z ujawnieniem adresu mailowego czy nawet pesela powinny zostać raczej w salach kinowych podczas seansów dla tych, co lubią się bać.

Ze słów pogrubionych w cytacie: ***Podmiot przetwarzający*** *po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki* ***zgłasza je*** *administratorowi,* wnioskujemy, że z przepisu wynika obowiązek zgłoszenia naruszenia.

Trafnie uwagę zwraca A. Krasuski[308], że spoczywający na podmiocie przetwarzającym obowiązek zgłoszenia naruszenia administratorowi danych osobowych nie jest uzależniony od poziomu ryzyka naruszenia praw i wolności.

Ze słów pogrubionych w cytacie: *Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki* ***zgłasza je administratorowi***, wnioskujemy, że podmiot przetwarzający zgłasza naruszenie administratorowi danych osobowych.

Paweł Barta, P. Kawecki i P. Litwiński zwracają uwagę[309] na fakt, że zgadzają się z poglądami P. Fajgielskiego i W. Chomiczewskiego, którzy uważają, że podmiot przetwarzający zgłasza administratorowi każdy przypadek naruszenia ochrony danych. Uzasadniają to w ten sposób, że ograniczenie obowiązku nie zostało zawarte w przepisie i że administrator jest zagrożony odpowiedzialnością administracyjną. Nie pozostaje mi nic innego, jak zwrócić uwagę na fakt, że zgadzam się ze wskazanymi autorami. Jednocześnie niepokoi mnie fakt, że jestem kolejnym autorem, który potwierdza poprawność poglądu, który w sposób oczywisty wynika z przepisu.

[308] A. Krasuski, [w:] A. Krasuski, P Siembida, op. cit., s. 74.

[309] Por. P. Barta, M. Kawecki, P. Litwiński, op. cit.

2. Art. 33 ust. 2 Wnioski z analizy

Z przepisu wynika spoczywający na podmiocie przetwarzającym obowiązek zgłoszenia naruszenia administratorowi. Bywa to też nazywane obowiązkiem notyfikacji naruszenia ochrony danych[310].

Podmiot przetwarzający zgłasza naruszenie administratorowi (danych osobowych). Podmiot przetwarzający zdefiniowano w art. 4 pkt 8 RODO.

Obowiązek powinien zostać zrealizowany przez podmiot przetwarzający po tym, jak podmiot ten stwierdzi naruszenie ochrony danych osobowych.

Z przepisu nie wynika, że obowiązek musi być zrealizowany natychmiast po stwierdzeniu naruszenia. Obowiązek może być zrealizowany ze zwłoką, jednak – jak wynika z przepisu – zwłoka ta nie może być zbędna. Zbędność czy niezbędność zwłoki należy oceniać odpowiednio do konkretnego stwierdzonego przez podmiot przetwarzający naruszenia.

3. Art. 33 ust. 2 Uwagi

3.1. Art. 33 ust. 2 Uwaga 1

Stwierdzenie naruszenia

Artykuł 33 ust. 2 RODO zawiera obowiązek zgłoszenia naruszenia administratorowi przez podmiot przetwarzający. Obowiązek ten jest prosty do zrozumienia, niestety jednak jedynie pozornie. Pozornie, dlatego że przepis uzależnia realizację obowiązku od zrealizowania się pewnych warunków, od zajścia pewnych zdarzeń. Niestety zdarzenia te są w przepisie jedynie wskazane i jednocześnie nie sposób się doszukać w RODO ich definicji.

Podobnie jak w art 33 ust 1 RODO napotykamy tu problem ustalenia, jaka zwłoka jest zbędna, a jaka nie jest zbędna, analizuję to wyżej w (*1. Art. 33 ust. 2. Analiza*).

Również podobnie jak w art 33 ust 1 RODO napotykamy tu problem ustalenia, czym jest „stwierdzenie naruszenia ochrony danych osobowych". Jeśli chodzi o samo *naruszenie ochrony danych osobowych,* to jest ono zdefiniowane w art 4 pkt 12 RODO. Problemem nie

[310] K. Wygoda, op. cit., s. 68.

jest jednak zdefiniowanie naruszenia ochrony danych osobowych, problemem jest ustalenie, kiedy w strukturze podmiotu przetwarzającego zachodzi stwierdzenie tegoż naruszenia. Analizuję to wyżej w odniesieniu do art 33 ust 1 RODO (*1. Art. 33 ust. 1. Analiza*), uważam więc że prowadzonych tam rozważań nie ma sensu tu powtarzać. Uważam też, że dobrze by było, gdyby przepis był nieco bardziej zrozumiały, w związku z tym stawiam niżej postulat nowelizacyjny (*6.1. Art. 33 ust. 2. Postulat 1. Osoba stwierdzająca naruszenie*).

3.2. Art. 33 ust. 2 Uwaga 2

Miejsce stwierdzenia naruszenia

Analogicznym problemem do problemu z ustaleniem, co należy rozumieć przez stwierdzenie naruszenia ochrony danych osobowych, jest problem z ustaleniem, gdzie ma zajść naruszenie, by uznać, że zaszło. Na pierwszy rzut oka nie wydaje się to być problemem. Podmiot przetwarzający stwierdza naruszenie ochrony danych osobowych, więc podmiot przetwarzający informuje administratora o fakcie zaistnienia tego naruszenia. Należy jednak zadać pytanie o to, jak daleko niejako sięga podmiot przetwarzający w związku ze stwierdzeniem naruszenia. Oczywiste wydaje się, że jeżeli podmiot przetwarzający stwierdzi naruszenie ochrony danych osobowych u siebie, w swojej organizacji, w swoim przedsiębiorstwie, to o takim właśnie naruszeniu podmiot przetwarzający ma obowiązek poinformować administratora.

Należy jednak zwrócić uwagę na fakt, że do tego, iż podmiot przetwarzający ma obowiązek zgłosić to naruszenie, które zachodzi w jego strukturze, dochodzimy jedynie na drodze interpretacji przepisu i to – jak się wydaje – na drodze interpretacji celowościowej. Interpretacja językowa przepisu nie jest tu wystarczająca. Wydaje się, że taka właśnie celowościowa interpretacja przepisu, zgodnie z którą podmiot przetwarzający zgłasza administratorowi naruszenie ochrony danych osobowych, które zaistniało w jego, czyli podmiotu przetwarzającego strukturze, jest poprawna. Możliwe są też jednak inne interpretacje przepisu, uważam przy tym, że interpretacje te są raczej dodatkowe wobec interpretacji wskazanej niż ją zastępujące. Dla porządku możliwe interpretacje przepisu wymieniam poniżej i numeruję.

Pierwsza interpretacja to interpretacja wskazana powyżej zgodnie z którą podmiot przetwarzający ma obowiązek poinformować

administratora o zaistnieniu naruszenia, jeżeli naruszenie to zaistnieje w strukturze podmiotu przetwarzającego.

Druga interpretacja to interpretacja, zgodnie z którą podmiot przetwarzający ma obowiązek poinformować administratora o zaistnieniu naruszenia, jeżeli naruszenie to zaistnieje w strukturze podmiotu przetwarzającego, któremu podmiot przetwarzający (z punktu widzenia którego prowadzimy rozumowanie) powierzył przetwarzanie danych osobowych. Innymi słowy, mamy do czynienia z trzema podmiotami, a to z administratorem, z podmiotem przetwarzającym pierwszego rzędu i z podmiotem przetwarzającym drugiego rzędu. Podmiot przetwarzający pierwszego rzędu powierza przetwarzanie danych osobowych podmiotowi przetwarzającemu drugiego rzędu. Mamy zatem do czynienia z powierzeniem przetwarzania, które zachodzi między administratorem a podmiotem przetwarzającym i z dalszym powierzeniem przetwarzania, które zachodzi między podmiotem przetwarzającym pierwszego rzędu a podmiotem przetwarzającym drugiego rzędu. I właśnie jeżeli naruszenie ochrony danych osobowych ma miejsce w strukturze podmiotu przetwarzającego drugiego rzędu, to podmiot przetwarzający pierwszego rzędu powinien o tym (jak się wydaje) poinformować administratora. Pojawia się tu jednak ciekawy problem, mianowicie kogo powinien poinformować o naruszeniu ochrony danych osobowych podmiot przetwarzający drugiego rzędu. Wydaje się, że podmiot przetwarzający drugiego rzędu powinien o naruszeniu ochrony danych osobowych informować administratora. Problem ten jest na tyle ważny, że poświęcam mu niżej osobną uwagę (*3.3. Art. 33 ust. 2. Uwaga 3. Stwierdzenie naruszenia w realiach dalszego powierzenia przetwarzania*).

Trzecia interpretacja to interpretacja, zgodnie z którą podmiot przetwarzający ma obowiązek poinformować o zaistnieniu naruszenia ochrony danych osobowych, jeżeli naruszenie to zaistnieje w strukturze administratora. Można sobie wyobrazić sytuację, w której naruszenie ma miejsce w strukturze administratora, jednak z uwagi na specyfikę usług świadczonych przez podmiot przetwarzający administratorowi, podmiot przetwarzający dowiaduje się o naruszeniu, które miało miejsce nie w jego, czyli podmiotu przetwarzającego strukturze, ale w strukturze administratora. Nie ma powodu, by uznać że w takiej sytuacji podmiot przetwarzający jest zwolniony z obowiązku informowania administratora o naruszeniu.

3.3. Art. 33 ust. 2 Uwaga 3

Stwierdzenie naruszenia

w realiach dalszego powierzenia przetwarzania

Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. Problemem, nad którym należy się zastanowić, jest problem zgłoszenia naruszenia przez podmiot przetwarzający, któremu przetwarzanie danych osobowych powierzy nie administrator, ale inny podmiot przetwarzający. Mamy tu zatem do czynienia z powierzeniem przetwarzania drugiego rzędu, podpowierzeniem przetwarzania danych osobowych, dalszym powierzeniem przetwarzania danych osobowych. Łańcuch podmiotów, których działaniu się przyglądamy, jest tu nieco dłuższy niż tylko administrator i podmiot przetwarzający. Łańcuch ten składa się z (co najmniej) trzech podmiotów. Na łańcuch ten składają się: administrator, podmiot przetwarzający i podmiot podprzetwarzający (inaczej mówiąc – podmiot przetwarzający drugiego rzędu).

Nie mam wątpliwości, że podmiot przetwarzający zgłasza naruszenie ochrony danych administratorowi, ma bowiem taki obowiązek, o którym piszemy wyżej. Nie mam tej wątpliwości w relacji, która zachodzi między dwoma podmiotami, tj. między administratorem a podmiotem przetwarzającym. W takiej relacji podmiot przetwarzający zgłasza administratorowi naruszenie ochrony danych osobowych. Jeżeli jednak łańcuch podmiotów branych pod uwagę wydłuża się o (co najmniej) jeszcze jeden podmiot przetwarzający, to sytuacja odrobinę się komplikuje. Podmiot przetwarzający pierwszego rzędu zawiera umowę powierzenia przetwarzania danych osobowych z podmiotem przetwarzającym drugiego rzędu, jednak należy zwrócić uwagę na fakt, że podmiot przetwarzający drugiego rzędu jest podmiotem przetwarzającym. Jest podmiotem przetwarzającym, tyle że drugiego rzędu. Nikim innym być nie może, bo przecież przetwarza dane w imieniu administratora, z tym jednak zastrzeżeniem, że zlecenie przetwarzania nie pochodzi od administratora, ale od podmiotu przetwarzającego pierwszego rzędu. Ponieważ podmiot przetwarzający drugiego rzędu jest podmiotem przetwarzającym, to obowiązek zgłoszenia naruszenia przez podmiot przetwarzający administratorowi rozciąga się również na podmiot przetwarzający drugiego rzędu. Innymi słowy, podmiot

przetwarzający drugiego rzędu ma obowiązek zgłoszenia naruszenia ochrony danych administratorowi. Wynika to z kilku przyczyn.

Po pierwsze, podmiot przetwarzający drugiego rzędu jest podmiotem przetwarzającym, tyle że drugiego rzędu, ale ponieważ jest podmiotem przetwarzający, to spoczywa na nim jako na podmiocie przetwarzającym, obowiązek wskazany w art. 33 ust. 2 RODO.

Po drugie, obowiązek zgłoszenia naruszenia administratorowi powinien być zapisany w umowie powierzenia przetwarzania. Wynika to z art. 28 ust. 3 lit. f RODO. Z przepisu tego wynika, że umowa powierzenia przetwarzania powinna zobowiązywać podmiot przetwarzający między innymi do tego, by podmiot przetwarzający pomagał *administratorowi wywiązać się z obowiązków określonych w art. 32–36*.

Można sobie oczywiście wyobrazić pomoc udzielaną administratorowi przez podmiot przetwarzający drugiego rzędu za pośrednictwem podmiotu przetwarzającego pierwszego rzędu i gdybyśmy sobie to wyobrazić mieli, to okaże się, że podmiot przetwarzający drugiego rzędu powinien zgłaszać naruszenia nie administratorowi, ale podmiotowi przetwarzającemu pierwszego rzędu. Interpretacja taka nie wydaje się być poprawna, z pewnym jednak zastrzeżeniem. Należy otóż zauważyć, że jeżeli podmiot przetwarzający drugiego rzędu nie poinformuje podmiotu przetwarzającego pierwszego rzędu o naruszeniu ochrony danych osobowych, ale sam poinformuje administratora, to postępowanie takie będzie – jak uważam – poprawne. Poprawne, ponieważ administrator, który został poinformowany o naruszeniu ochrony danych, może podjąć dalsze kroki, do których jest zobowiązany przepisami. Niestety, w opisanej sytuacji podmiot przetwarzający pierwszego rzędu nie poinformuje administratora o zaistnieniu naruszenia w strukturze podmiotu przetwarzającego drugiego rzędu z tego powodu że po prostu nie będzie o tym wiedzieć. Nie jestem jednak przekonany, czy stanowi to jakikolwiek problem.

Rozpatrzmy bowiem sytuację po kolei:

– Jest administrator,
– jest podmiot przetwarzający pierwszej kategorii (rzędu),
– jest podmiot przetwarzający drugiej kategorii (rzędu).
– Ma miejsce naruszenie ochrony danych i zachodzi ono w strukturze podmiotu przetwarzającego drugiej kategorii (rzędu).

– Podmiot przetwarzający drugiej kategorii (rzędu) zgłasza naruszenie administratorowi i tym samym realizuje swój obowiązek z art 33 ust. 2 RODO.

Wydaje się, że w zasygnalizowanym stanie faktycznym, obowiązki wynikające z przepisów zostały zrealizowane.

Można poczynić tu jedną jeszcze uwagę. Otóż nic nie stoi na przeszkodzie, by podmiot przetwarzający drugiej kategorii informował o naruszeniu zarówno administratora, jak i podmiot przetwarzający pierwszej kategorii. Można by tu zaryzykować tezę, że podmiot przetwarzający drugiej kategorii powinien poinformować taki podmiot czy takie podmioty, do poinformowania których zobowiązuje go umowa z podmiotem przetwarzającym pierwszej kategorii, nie wydaje się jednak, by teza ta była trafna. Należy pamiętać że art 33 ust. 2 RODO zobowiązuje podmiot przetwarzający do poinformowania administratora o naruszeniu, jest to obowiązek wynikający z przepisu prawa i jako taki nie może on być na mocy umowy zmodyfikowany.

4. Art. 33 ust. 2 Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa I

Obecność w przepisie pogrubionych słów: **P*odmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi***, skutkuje po stronie administratora i osób, których dane dotyczą, w sposób wskazany poniżej.

Jeżeli ma miejsce naruszenie ochrony danych osobowych w strukturze podmiotu przetwarzającego, ten podmiot przetwarzający ma obowiązek zgłosić to naruszenie administratorowi. Podmiot przetwarzający ma obowiązek zgłosić naruszenie bez zbędnej zwłoki.

Jeżeli ma miejsce naruszenie ochrony danych osobowych w strukturze podmiotu przetwarzającego, to osoba, której dane dotyczą, ma prawo do tego, by podmiot przetwarzający zgłosił naruszenie administratorowi. Osoba, której dane dotyczą, ma prawo, by podmiot przetwarzający zgłosił naruszenie bez zbędnej zwłoki.

5. Art. 33 ust. 2 Konkretyzacja zasady

Art. 33 ust. 2 konkretyzuje jakiekolwiek zasady w niewielkim stopniu. Jeżeli jest możliwy do odnotowania jakikolwiek znaczący

związek między przepisem a zasadami, to w konwencji konkretyzacji zasad wskazuję nań w (*5. Art. 33 ust. 1 Konkretyzacja zasad*).

6. Art. 33 ust. 2 Postulaty *de lege ferenda*

6.1. Art. 33 ust. 2 Postulat 1

Osoba stwierdzająca naruszenie

Wyżej w analizie (*1. Art. 33 ust. 1. Analiza*) zastanawiam się nad tym, od jakiego momentu należy liczyć 72-godzinny termin do zgłoszenia naruszenia do PUODO. Uczciwie patrząc, nie do końca wiadomo, jak termin ten liczyć należy. W art. 33 ust. 2 problem kształtuje się podobnie, przybiera może mniej dramatyczny kształt, ponieważ o ile w art. 33 ust. 1 RODO mowa jest o zgłoszeniu naruszenia do PUODO *bez zbędnej zwłoki nie później niż w terminie 72 godzin po stwierdzeniu naruszenia*, o tyle w art. 33 ust. 2 RODO mowa jest jedynie o tym, że podmiot przetwarzający ma obowiązek zgłosić naruszenie również *po stwierdzeniu naruszenia* i również *bez zbędnej zwłoki*, jednak nie napotykamy w przepisie na konkretny termin 72-godzinny. Brak jest terminu 72-godzinnego, zbędną zwłokę można zapewne jakoś doprecyzować, co zresztą czynię wyżej (*1. Art. 33 ust. 1. Analiza*), jednak podobnie jak w odniesieniu do art. 33 ust. 1 RODO, nie wiadomo, jak rozumieć stwierdzenie naruszenia.

Mając na uwadze powyższe, postuluję nowelizację art. 33 ust. 1 RODO we wskazany poniżej sposób.

Postuluję, by przepis, o którym tu mowa, miał postać:
„Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych **przez uprawnionego pracownika podmiotu przetwarzającego** bez zbędnej zwłoki zgłasza je administratorowi".
(Czcionką wytłuszczoną elementy wstawione do przepisu,)

Artykuł 33 ust. 5 RODO

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

1. Art. 33 ust. 5 Analiza

Ze słowa pogrubionego: ***Administrator*** *[...]* wnioskujemy, że: obowiązek wynikający z przepisu spoczywa na administratorze danych osobowych

Ze słów pogrubionych w cytacie: ***Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych****, w tym [...]* wnioskujemy, że z przepisu wynika obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych.

Na obowiązek dokumentowania naruszeń trafnie zwraca uwagę P. Fajgielski[311]. Podkreślenia wymaga, że obowiązek zgłoszenia naruszeń dotyczy wszystkich zdarzeń, które można zakwalifikować jako naruszenia na gruncie art. 4 pkt 12 RODO. Uczciwość wymaga wskazania, że P. Fajgielski prezentuje analogiczne stanowisko. Autor wskazuje, że wykładnia językowa przepisu przemawia za odnotowywaniem wszystkich naruszeń, w tym naruszeń, które nie podlegają zgłoszeniu – z tym stanowiskiem się zgadzam. Dalej jednak P. Fajgielski wskazuje, że wykładnia funkcjonalna przepisu przemawia przeciwko odnotowywaniu naruszeń, które nie podlegają zgłoszeniu – z tym stanowiskiem się nie zgadzam. Nie zgadzam się i, co więcej, nie dostrzegam uzasadnienia dla takiego poglądu. Co więcej podwójnie, uważam, że odnotowywanie naruszeń, które nie zostały zgłoszone, jest głęboko sensowne, pozwala bowiem, w przypadku kontroli na skontrolowanie, czy przypadkiem administrator nie zaniedbał zgłoszenia naruszeń, które zgłoszone być powinny.

Wskazany autor, z właściwą sobie przenikliwością, którą mogę tylko podziwiać, zauważa, że *Obowiązek dokumentowania naruszeń*

[311] P. Fajgielski, op. cit.

został nałożony na administratora, natomiast komentowany przepis nie rozciąga go na podmiot przetwarzający[312]. Mogę się tylko zgodzić, muszę jednak dokonać pewnego uzupełnienia. Otóż analizowany przepis stanowi, że administrator ma obowiązek dokumentować wszelkie naruszenia ochrony danych osobowych. Ponieważ administrator ma obowiązek dokumentować wszelkie naruszenia, to uważam, że obowiązek ten dotyczy również naruszeń, które stwierdził podmiot przetwarzający i o zaistnieniu których podmiot przetwarzający poinformował administratora. Nie widzę powodu, by słowa *wszelkie naruszenia interpretować* jako „wszelkie naruszenia stwierdzone przez administratora, ale naruszenia stwierdzone przez podmiot przetwarzający nie". Jeżeli dostrzegamy sensowność obowiązku odnotowywania naruszeń (obok ewidentnego obowiązywania tegoż obowiązku) to nie ma powodu, by uważać, że jedne naruszenia odnotowywać należy, a innych nie.

Ze słów pogrubionych w cytacie: *Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w* ***tym*** *[...]* wnioskujemy, że: doprecyzowane dalej w przepisie dokumentowanie naruszeń ochrony danych osobowych obejmuje wymienione w przepisie trzy elementy. Są to elementy obowiązkowe. Dokumentowanie może obejmować również inne, niewymienione w przepisie elementy.

Ze słów pogrubionych w cytacie: *Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w* ***tym okoliczności naruszenia ochrony danych osobowych*** *[...]* wnioskujemy, że: pierwszym z elementów dokumentowania naruszeń ochrony danych osobowych są okoliczności naruszenia tej ochrony.

Ze słów pogrubionych w cytacie: „*Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w* ***tym*** *okoliczności naruszenia ochrony danych osobowych,* ***jego skutki*** *[...]* wnioskujemy, że: drugim z elementów dokumentowania naruszeń ochrony danych osobowych są skutki naruszenia tej ochrony.

Ze słów pogrubionych w cytacie: *Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, [...] oraz* ***podjęte działania zaradcze*** *[...]* wnioskujemy, że: trzecim z elementów dokumentowania naruszeń ochrony danych osobowych są podjęte działania zaradcze.

---

[312] Ibidem.

Ze słów pogrubionych w cytacie: *Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych […]* ***Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu***, wnioskujemy, że: opisana w art. 33 ust. 5 dokumentacja naruszeń ochrony danych osobowych musi być poprowadzona na tyle szczegółowo i w sposób odpowiadający wynikającemu z przepisu schematowi, by umożliwić Prezesowi Urzędu Ochrony Danych weryfikowanie przestrzegania art. 33 RODO. W kolejnych ustępach art. 33 RODO ustanowione są kolejne obowiązki. Omówione zostały one w komentarzu do stosownych fragmentów przepisu, tu jednak zwracam uwagę na fakt, że obowiązek dokumentowania, wynikający z art. 33 ust 5 RODO, ma jedynie pozornie ogólny charakter. W istocie obowiązek ten jest bardzo szczegółowy, należy bowiem dokumentować realizacje kolejnych, szczegółowych obowiązków, wynikających z art. 33 RODO.

2. Art. 33 ust. 5 Komentarz

Obowiązek wynikający z przepisu spoczywa na administratorze (danych osobowych). Jest to obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych.

Dokumentowanie naruszeń ochrony danych osobowych obejmuje wymienione w przepisie trzy elementy. Są to elementy obowiązkowe. Dokumentowanie może obejmować również inne, niewymienione w przepisie elementy.

– **Pierwszym** z elementów dokumentowania naruszeń ochrony danych osobowych są okoliczności naruszenia tej ochrony.
– **Drugim** z elementów dokumentowania naruszeń ochrony danych osobowych są skutki naruszenia tej ochrony.
– **Trzecim** z elementów dokumentowania naruszeń ochrony danych osobowych są podjęte działania zaradcze.

Dokumentacja naruszeń ochrony danych osobowych musi być poprowadzona na tyle szczegółowo i w sposób odpowiadający wynikającemu z przepisu schematowi, by umożliwić Prezesowi Urzędu Ochrony Danych weryfikowanie przestrzegania przez administratora danych osobowych art. 33 RODO.

W kolejnych ustępach art. 33 RODO ustanowione są kolejne obowiązki. Przeanalizowane i omówione zostały one w podrozdziałach

poświęconym kolejnym fragmentom przepisu, tu jednak zwracam uwagę na fakt, że obowiązek dokumentowania, wynikający z art. 33 ust 5 RODO, ma jedynie pozornie ogólny charakter. W istocie obowiązek ten jest bardzo szczegółowy, należy bowiem dokumentować realizacje kolejnych, szczegółowych obowiązków, wynikających z art. 33 RODO.

3. Art. 33 ust. 1 i 2 i 5 Uwagi

3.4. Art. 33 Uwaga 1

Cel informowania organu nadzorczego

Wyżej w (*1. Art. 33 ust. 1. Analiza*) zastanawiam się nad tym, jak należy liczyć 72-godzinny termin do zgłoszenia naruszenia do PUODO. Nie relacjonując tamtych rozważań, pragnę poczynić tu pewną uwagę, natury raczej systemowej niż praktycznej. Paweł Fajgielski zwraca uwagę na fakt, że: *[...] administrator powinien działać możliwie szybko, aby umożliwić realizację celów omawianego mechanizmu prawnego*. I dalej ten sam autor pisze, że: *Zawiadamianie organu nadzorczego powinno być realizowane możliwie szybko, aby organ nadzorczy mógł w sposób odpowiedni zareagować na naruszenie (np. ocenić, czy administrator podjął właściwe działania)*[313].

Rozumiem stanowisko P. Fajgielskiego, uważam ponadto, że prawdopodobnie jest ono zbieżne z intencją twórców RODO, uważam jednak, że przemawia przez to stanowisko wielki optymizm wielkiego profesora. Ja tak optymistyczny nie jestem. Jeżeli naruszenie ochrony danych ma charakter zniszczenia danych osobowych, to cóż może począć organ ochrony danych. Nie jest w jego mocy cofnięcie czasu.

Można oczywiście podnosić, że organ może wskazać właściwe sposoby zabezpieczenia, skontrolować, czy sposoby przyjęte były właściwe itd. Można to podnosić, lecz uważam, że takie stwierdzenia to jedynie kolejny powiew optymizmu. Dane zostały ujawnione. W gruncie rzeczy nie można już nic zrobić. W takim przypadku organowi pozostaje jedno. Nałożyć karę. Uważam, że powinno to być powiedziane. Oczywiście organ może również kary nie nałożyć, tu jednak odnoszę się do sytuacji, w której organ jednak zadziałać pragnie. Pragnie zadziałać, podejmuje zatem dostępne mu działanie i… nakłada karę.

[313] Ibidem.

Powinno być powiedziane i powinno być napisane, że celem obowiązku denuncjacyjnego ustanowionego w art. 33 ust. 1 RODO jest ułatwienie organowi nadzorczemu nakładania kar. Jest to może pogląd radykalny, uważam jednak, że oddający istotę zagadnienia.

W podobnie jak P. Fajgielski w optymistycznym tonie, wypowiada się W. Chomiczewski, który pisze, że celem przepisu jest ochrona ***podstawowych praw i wolności*** *osób fizycznych, w szczególności ich prawa do ochrony danych osobowych*[314]. (Wytłuszczenie W. Chomiczewskiego) i – co ciekawe – realizację tego celu dostrzega w art. 32 ust. 2 RODO, czego zrozumieć nie mogę. Można próbować wywodzić, że chodzi tu o ochronę wskazanych praw w duchu prewencji ogólnej, przyznam jednak, że niechętnie uzasadniam pogląd W. Chomiczewskiego, co do którego trafności mam wątpliwość.

Na ciekawe zjawisko zwrócił uwagę C. Burton. Otóż twierdzi on, że dobrze byłoby, gdyby administratorzy dokumentowali swoje czynności w szerszym zakresie aniżeli tylko zakres minimalny wskazany w przepisie. Udokumentowanie wszystkich czynności dokonanych przez administratora jest istotne z uwagi na prawdopodobieństwo kontroli. Szczególnie niebezpiecznie sytuacja kształtuje się, jeżeli administrator nie zgłasza naruszenia. W takiej sytuacji – w jakimś zakresie – grozi mu odpowiedzialność za niezgłoszenie naruszenia. Dokumentacja, z której wynika, że administrator dokonał odpowiednich ocen, może – zwłaszcza jeżeli administrator dokonał tych ocen prawidłowo – ochronić go przed odpowiedzialnością administracyjną[315].

3. Art. 33 ust. 5 Uwagi

3.1. Art. 33 ust. 5 Uwaga 1

Odesłanie w przepisie

Przepis ustanawia obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych. Wyżej, w uwadze (*3.9. Art. 33 ust. 1 Uwaga 9. Incydent*) zastanawiam się nad pojęciem incydentu. Pewne zagrożenie dla administratora mogą stworzyć sytuacje, w których zakwalifikuje on dany stan faktyczny jako incydent i w związku

[314] W. Chomiczewski, op. cit., s. 710.

[315] C. Burton, op. cit., s. 649.

z tym zaniecha on podejmowania jakichkolwiek czynności, w tym zaniecha dokumentowania naruszenia. Oczywiście najlepiej nawet napisany przepis nie stanowi panaceum na brak wiedzy administratora, wydaje się jednak, że im przepis jest jaśniejszy, im przepis jest prostszy do zrozumienia, tym mniejsze jest ryzyko niezrozumienia go przez administratora.

Naruszenie ochrony danych osobowych zostało zdefiniowane w art. 4 pkt 12 RODO. Obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych to zatem w istocie obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych zdefiniowanych w art. 4 pkt 12 RODO. Dla osoby w miarę kompetentnej w zakresie rudymentów teorii prawa i poruszającej się sprawnie w zakresie tekstu RODO, odesłanie w art. 33 ust. 5 do art. 4 pkt 12 jest oczywiste. By było oczywiste dla wszystkich należy tu postawić postulat *de lege ferenda* (*6.1 Art. 33 ust. 5 Postulat 1. Doprecyzowanie odesłania*).

3.2. Art. 33 ust. 5 Uwaga 2

Dokumentowanie naruszeń

Z art. 33 ust. 5 RODO wynika obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych (*any personal data breaches*). Jednocześnie z art. 33 ust. 2 RODO wynika leżący po stronie podmiotu przetwarzającego, obowiązek zgłaszania administratorowi naruszenia ochrony danych osobowych. W takim razie administrator dysponuje wiedzą na temat naruszeń ochrony danych osobowych, które miały miejsce w jego strukturze i o naruszeniach ochrony danych osobowych, które miały miejsce w strukturze podmiotu przetwarzającego. Uważam, że obowiązek dokumentowania wszelkich naruszeń, leżący po stronie administratora obejmuje również naruszenia, które miały miejsce w strukturze podmiotu przetwarzającego. Wniosek ten wysnuwam z użycia przez prawodawcę słowa „wszelkich", w odniesieniu do *naruszeń ochrony danych osobowych*. Użycie „any" w wersji anglojęzycznej potwierdza – moim zdaniem – ten wniosek. Również użycie słowa „veškeré", czyli „wszystkie" w wersji czeskojęzycznej, potwierdza wniosek.

Za wskazanym podejściem przemawia – jak uważam – jeden jeszcze argument. Otóż na końcu art. 33 ust. 5 RODO czytamy o dokumentacji, że *Dokumentacja ta musi pozwolić organowi nadzor-*

czemu weryfikowanie przestrzegania niniejszego artykułu. Przez przestrzeganie artykułu rozumiem przestrzeganie go odpowiednio przez administratora i przez podmiot przetwarzający. Zgłoszenie naruszenia administratorowi przez podmiot przetwarzający jest elementem przestrzegania artykułu. Dla umożliwienia organowi weryfikacji przestrzegania art. 33 RODO, w zakresie zgłoszenia naruszenia przez podmiot przetwarzający, konieczne jest, by administrator dokumentował to zgłoszenie i szczegóły naruszenia, które miało miejsce w strukturze podmiotu przetwarzającego.

Wywodzę wyżej, że uważam, iż obowiązek dokumentowania naruszeń, który spoczywa na administratorze, obejmuje również naruszenia, które miały miejsce w strukturze podmiotu przetwarzającego. Uzasadniam to wyżej dwiema drogami, uważam jednak, że dobrze byłoby, gdyby fakt, że obowiązek dokumentowania naruszeń przez administratora dotyczy również naruszeń, które mają miejsce w strukturze podmiotu przetwarzającego, wynikał z przepisu w sposób jednoznaczny. Skutkuje to postawieniem odpowiedniego postulatu *de lege ferenda* (*6.2 Art. 33 ust. 5 Postulat 2. Doprecyzowanie obowiązku dokumentowania naruszeń*).

Jeśli chodzi o dokumentowanie naruszeń, to C. Burton zwraca uwagę na motyw 85 Preambuły RODO, z którego wynika, że jeżeli administrator nie zgłasza naruszenia, to powinien je on udokumentować na tyle dokładnie, by był *[...] w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych*[316].

4. Art. 33 ust. 5 Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa I

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

Obecność w przepisie pogrubionych słów: ***Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze*** *[...]* skutkuje po stronie administratora i osób, których dane dotyczą, w sposób wskazany poniżej.

[316] C. Burton, op. cit.

Administrator ma obowiązek dokumentować wszelkie naruszenia ochrony danych osobowych. Obowiązek dokumentowania naruszenia obejmuje: okoliczności naruszenia, skutki naruszenia i działania zaradcze podjęte w związku z naruszeniem.

Osoba, której dane dotyczą, ma prawo do tego, by administrator dokumentował wszelkie naruszenia ochrony danych osobowych. Tym samym osoba, której dane dotyczą, ma prawo do tego, by administrator dokumentował okoliczności naruszenia, skutki naruszenia i działania zaradcze podjęte w związku z naruszeniem.

Obecność w przepisie pogrubionych słów: *[...]* ***Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu***, skutkuje po stronie administratora i osób, których dane dotyczą, w sposób wskazany poniżej.

Administrator ma obowiązek dokumentować wszelkie naruszenia ochrony danych osobowych w taki sposób, by tworzona w ten sposób dokumentacja pozwalała organowi nadzorczemu na weryfikację przestrzegania art. 33 RODO.

Osoba, której dane dotyczą, ma prawo do tego, by administrator dokumentował wszelkie naruszenia ochrony danych osobowych w taki sposób, by tworzona w ten sposób dokumentacja pozwalała organowi nadzorczemu na weryfikację przestrzegania art. 33 RODO.

5. Art. 33 ust. 5 Konkretyzacja zasad

Realizacja obowiązku wynikającego z art. 13 RODO, czyli udostępnianie informacji wynikających z tego przepisu, sprzyja realizacji zasad w sposób opisany poniżej.

Zasada rozliczalności

Zasada rozliczalności oznacza, że administrator ma obowiązek wykazania przestrzegania zasad wynikających z art. 5 ust. 1 RODO. Zasady z art. 5 ust. 1 RODO są realizowane przez przepisy szczegółowe RODO, czyli obowiązek wykazania przestrzegania zasada oznacza obowiązek wykazania przestrzegania przepisów szczegółowych RODO[317].

Przepis konkretyzuje przede wszystkim tę właśnie zasadę. Konkretyzuje ją w sposób niejako przykładowy. Artykuł 33 RODO składa

[317] J. Rzymowski, *RODO – GDPR. Zasady dotyczące…*, s. 303.

się z pięciu ustępów. Ustępy od 1 do 4 statuują pewne obowiązki po stronie administratora. Ustęp, o którym tu jest mowa, statuuje obowiązek dokumentowania realizacji obowiązków z ustępów od 1 do 4.

Zasada zgodności z prawem

Przetwarzanie zgodne z zasadą zgodności z prawem to przetwarzanie zgodne z art. 6 RODO i ewentualnie z art. 9 RODO i z art. 10 RODO. Artykuł 33 ust 1 i 2 RODO dotyczy namysłu nad naruszeniem ochrony danych osobowych i nad jego skutkami w sferze praw i wolności osoby, której dane dotyczą. Naruszenie ochrony danych osobowych, a na pewno naruszenie w postaci faktycznego zdarzenia, a nie jedynie zagrożenia tym zdarzeniem, ma – jak uważam – charakter przetwarzania danych osobowych niezgodnego z prawem, czyli przetwarzania z naruszeniem zasady zgodności z prawem. Może się też zdarzyć, że o ile samo naruszenie nie jest tożsame z przetwarzaniem niezgodnym z prawem, o tyle naruszenie skutkuje przetwarzaniem niezgodnym z prawem.

Ustęp 5 artykułu 33 RODO dotyczy wykazania tego, czy i jak wskazany namysł się odbywał. O ile zatem artykuł 33 ust 1 i 2 RODO dotyczą realizacji zasady zgodności z prawem, o tyle art. 33 ust. 5 ma charakter metaprzepisu, który sam może nie dotyczy zasady zgodności z prawem, dotyczy jednak dokumentowania przepisów, które zasady tej dotyczą. Można więc powiedzieć, że o ile art. 33 ust. 1 i 2 RODO dotyczą realizacji zasady zgodności z prawem w sposób bezpośredni, o tyle art. 33 ust. 5 RODO dotyczy realizacji zasady zgodności z prawem w sposób pośredni.

Zasada ograniczenia celu
Zasada ograniczenia przechowywania
Zasada integralności
Zasada poufności

Związek art. 33 ust. 5 ze wskazanymi zasadami nie jest silny, jest jednak dostrzegalny. Sytuacja kształtuje się tu podobnie jak ze związkiem przepisu z zasadą zgodności z prawem. Artykuł 33 ust. 1 i 2 RODO dotyczą przetwarzania danych osobowych z naruszeniem wskazanych zasad. Zależnie od okoliczności konkretnego zdarzenia, które jest naruszeniem ochrony danych osobowych, mogą zostać naruszone poszczególne zasady. Artykuł 33 ust. 5 RODO ustanawia

obowiązek dokumentowania realizacji (m.in.) art. 33 ust. 1 i 2 RODO, więc w jakimś sensie, pośrednim, odległym, jednak dostrzegalnym, art. 33 ust. 5 dotyczy realizacji tych zasad.

Zasada ograniczenia celu

Przetwarzanie w warunkach naruszenia ochrony danych (ale jednak o charakterze zdarzenia, niezagrożenia tymże) jest niewątpliwie przetwarzaniem w innym celu niż cel, w jakim dane przez dany podmiot miały być przetwarzane, innym niż cel wskazany w informacjach, które wynikają z art. 13, 14, 15 RODO i który zapisany jest w RCPD.

Zasada ograniczenia przechowywania

Jeżeli dane zostaną ujawnione nieuprawnionemu podmiotowi, innemu niż administrator, to trudne do ustalenia jest, jak długo podmiot ten będzie te dane przechowywał, co grozi naruszeniem zasady ograniczenia przechowywania, a co najmniej nie pozwala na ustalenie, czy jest ona szanowana czy naruszana. Podobnie – jak w odniesieniu do poprzedniej zasady – art. 33 ust. 5 RODO ma tu charakter metaprzepisu.

Zasada integralności i **zasada poufności**

Mogą zostać one naruszone przetwarzaniem w warunkach naruszenia. Jedna lub druga lub obydwie. Artykuł 33 ust. 5 RODO ma również tu charakter metaprzepisu.

Zasada minimalizacji danych

Wydaje się, że podobnie jak w odniesieniu do omówionych wyżej zasad, związek tej zasady z art. 33 ust. 5 RODO jest niewielki, ale dostrzegalny. Artykuł 33 ust. 5 dotyczy dokumentowania zdarzeń (namysłu administratora nad skutkami naruszenia), które są następstwem zdarzeń, które skutkują naruszeniem zasady minimalizacji (naruszenia ochrony danych osobowych).

Zasada rzetelności i **zasada przejrzystości**

O ile w odniesieniu do pozostałych zasad, związek z art. 33 ust. 5 RODO jest słaby jednak (może z trudem, jednakowoż…) dostrzegalny, o tyle tu związku nie widzę. Można się go doszukać na siłę, twierdząc, że przetwarzanie w warunkach naruszenia ochrony danych to przetwarzanie z naruszeniem wskazanych zasad, nie mam jednak co

do tej tezy pewności. Może zjawiska związane z ujawnieniem danych godzą we wskazane zasady, bo odbiorca *contra legem* – podmiot, któremu zostaną ujawnione dane w warunkach naruszenia ochrony danych osobowych, raczej nie zrealizuje, zwłaszcza art. 14 i 15 RODO, art. 33 ust. 5 RODO zaś dotyczy dokumentowania namysłu administratora nad tą sytuacją. Może jednak związek jest tu naprawdę słabo dostrzegalny.

6. Art. 33 ust. 1, 2, 5 Postulaty *de lege ferenda*

6.1 Art. 33 ust. 5 Postulat 1

Doprecyzowanie odesłania

W art. 33 ust. 5 RODO użyto pojęcia „naruszenie ochrony danych osobowych". W istocie stanowi to klauzulę odsyłającą do definicji tego pojęcia zawartej w art. 4 pkt 12 RODO. Mniej uważny czytelnik RODO może jednak to odesłanie pominąć. Pominięcie wskazanego odesłania musi skutkować niewłaściwym zrozumieniem
Przetwarzanie danych osobowych zgodne z prawem to zatem przetwarzanie zgodnie z art. Dla zniwelowania ryzyka pominięcia odesłania dobrze byłoby, gdyby przepis odsyłający wskazywał dokładnie na przepis, do którego odsyła.

Mając na uwadze powyższe, postuluję nowelizację art. 33 ust. 5 RODO we wskazany poniżej sposób.

Postuluję, by przepis, o którym tu mowa, miał postać:
„Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych**, zdefiniowane w art. 4 pkt 12 RODO**, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu".
(Czcionką wytłuszczoną zaznaczyłem elementy wstawione do przepisu.)

6.2 Art. 33 ust. 5 Postulat 2

Doprecyzowanie obowiązku dokumentowania naruszeń

Wyżej w uwadze (*3.2. Art. 33 ust. 5 Uwaga 2. Dokumentowanie naruszeń*) przedkładam, że: *Uważam, że obowiązek dokumentowania wszelkich naruszeń, leżący po stronie administratora obejmuje również naruszenia, które miały miejsce w strukturze podmiotu prze-*

twarzającego. By nie powtarzać argumentacji, odsyłam do wskazanej uwagi/podrozdziału. Uwagę tę zamykam refleksją, że dobrze byłoby, gdyby wskazany obowiązek wynikał z przepisu w sposób niewątpliwy, co skutkuje postawieniem niniejszego postulatu nowelizacyjnego.

Mając na uwadze powyższe, postuluję nowelizację art. 33 ust. 5 RODO we wskazany poniżej sposób.

Postuluję, by przepis, o którym tu mowa, miał postać:
„Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. **Obowiązek dokumentowania dotyczy również naruszeń zgłoszonych administratorowi przez podmiot przetwarzający, w tym samego zgłoszenia.** Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu".
(Czcionką wytłuszczoną zaznaczyłem elementy wstawione do przepisu.)

7. Art. 33 Rozważania historyczne

7.1. Art. 33 Rozważanie 1

Odpowiedniki w dawnej legislacji

Artykuł 33 nie znajduje bezpośredniego odpowiednika w dawnej legislacji, jednak na co zwraca uwagę C. Burton, w okresie przed pojawieniem się RODO, w niektórych krajach Unii Europejskiej funkcjonowały obowiązki notyfikacyjne[318].

[318] C. Burton, op. cit, s. 643.

Artykuł 34 RODO

Zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d).

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

Artykuł 34 ust. 1 RODO

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

1. Art. 34 ust. 1 Analiza

Ze słów pogrubionych w przepisie: *Jeżeli* ***naruszenie ochrony danych osobowych*** *[...]* wynika, że przepis dotyczy naruszenia ochrony danych osobowych. Przez naruszenie ochrony danych osobowych rozumiemy zjawisko zdefiniowane w art. 4 pkt 12 RODO.

Ze słów pogrubionych w przepisie: ***Jeżeli naruszenie ochrony danych osobowych*** *może [...]* wynika, że przepis uzależnia zajście zdarzeń opisane dalej w przepisie od naruszenia ochrony danych.

Ze słów pogrubionych w przepisie: *[...]* ***może powodować*** *wysokie* ***ryzyko*** *[...]* wynika, że przepis dotyczy sytuacji, w której wymienione w przepisie zjawisko, czyli naruszenie ochrony danych, może powodować ryzyko.

Ze słów pogrubionych w przepisie: *[...]* ***ryzyko naruszenia praw lub wolności osób fizycznych****, [...]* wynika, że ryzyko, o którym mowa w przepisie, to ryzyko naruszenia praw lub wolności osób fizycznych. Jeśli chodzi o prawa osób fizycznych to zapewne przepis odsyła do praw, o których jest mowa w RODO. Prawa te dzielą się na prawa zasadnicze – wynikające z art. 5 RODO i prawa szczegółowe – wynikające z przepisów szczegółowych RODO. Mam tu na myśli przepisy od art. 6 RODO do art. 37. Z prawami związane są wolności.

Poziom ryzyka naruszenia praw i wolności określony jako wysoki i w ogóle sama możliwość wystąpienia ryzyka naruszenia praw i wolności osób fizycznych prowadzi do pewnej konstatacji. Otóż, jeżeli istnieje ryzyko naruszenia praw i wolności osób fizycznych, to zapewne możliwe jest też naruszenie praw i wolności osób fizycznych. Ta z kolei konstatacja prowadzi do kolejnej, związanej zdecydowanie z wysokim poziomem ryzyka naruszenia praw i wolności. Otóż skoro wysokie ryzyko naruszenia praw i wolności skutkuje obowiązkiem zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, to również

naruszenie praw i wolności osoby, której dane dotyczą, skutkuje obowiązkiem zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, co wynika z zasady znanej jako *argumentum a fortiori*[319]. Szerzej w uwadze (*3.7. Art. 34 ust. 1 Uwaga 7. Naruszenie praw i wolności osób fizycznych*). Zwracam tu jedynie uwagę na fakt, że możliwość zaistnienia naruszenia praw i wolności jest warunkiem istnienia ryzyka naruszenia tych właśnie praw i wolności. Gdyby naruszenie praw i wolności osób fizycznych nie było możliwe, to ryzyko tego naruszenia też nie byłoby możliwe.

Z użycia w przepisie funktora logicznego: *[...] praw* ***lub*** *wolności [...]* wynika, że ryzyko, które może być spowodowane przez naruszenie to ryzyko naruszenia samych tylko praw osób fizycznych albo samych tylko wolności osób fizycznych, albo praw i wolności osób fizycznych. Wydaje się jednak, że z uwagi na związek praw i wolności niemożliwe jest naruszenie praw bez naruszenia wolności i że niemożliwe jest naruszenie wolności bez naruszenia praw.

Ze słów pogrubionych w przepisie: *[...] może powodować* ***wysokie ryzyko*** *naruszenia [...]* wynika, że ryzyko, o którym mowa w przepisie, jest ryzykiem wysokim.

Ze słów pogrubionych w przepisie: *[...]* ***administrator*** *[...]* ***zawiadamia osobę,*** *[...]* wynika, że w sytuacji, która opisana jest w przepisie, administrator zawiadamia osobę, o której dalej w przepisie jest mowa. Z użycia trybu orzekającego „zawiadamia" wnioskujemy, że na administratorze spoczywa obowiązek zawiadomienia wspomnianej osoby.

Obowiązek ten nie spoczywa na podmiocie przetwarzającym. Podmiot przetwarzający, co wynika z art. 33 ust. 2 RODO, ponieważ podmiot przetwarzający ma obowiązek informować administratora danych osobowych o naruszeniu ochrony danych osobowych, na co zwraca uwagę[320] W. Chomiczewski.

Ze słów pogrubionych w przepisie: *[...]* ***administrator*** *[...]* ***zawiadamia*** *[...]* ***o takim naruszeniu*** wynika, że zawiadomienie o którym mowa, to zawiadomienie o naruszeniu, czyli o naruszeniu ochrony danych, o którym mowa na wstępie przepisu.

Ze słów pogrubionych w przepisie: *[...] zawiadamia o****sobę, której dane dotyczą,*** *[...]* wynika, że osoba, którą administrator ma

[319] L. Morawski, op. cit., s. 219–222.

[320] W. Chomiczewski, op. cit., s. 720–721.

obowiązek poinformować o naruszeniu to osoba, której dane dotyczą, czyli tzw. podmiot danych.

Ze słów pogrubionych w przepisie: *[...]* ***bez zbędnej zwłoki*** *zawiadamia [...]* wynika, że zawiadomienie, o którym mowa w przepisie, ma zostać wykonane bez zbędnej zwłoki.

2. Art. 34 ust. 1 Wnioski z analizy

Przepis dotyczy naruszenia ochrony danych osobowych. Przez naruszenie ochrony danych osobowych rozumiemy zjawisko zdefiniowane w art. 4 pkt 12 RODO.

Zaistnienie zdarzeń opisanych w przepisie uzależnione jest od zaistnienia naruszenia ochrony danych osobowych.

Przepis dotyczy sytuacji, w której wymienione w przepisie zjawisko, czyli naruszenie ochrony danych może powodować ryzyko.

Ryzyko, o którym mowa w przepisie, to ryzyko naruszenia praw lub wolności osób fizycznych. Jeśli chodzi o prawa osób fizycznych, to zapewne przepis odsyła do praw, o których jest mowa w RODO. Prawa te dzielą się na:
– prawa zasadnicze – wynikające z art. 5 RODO i
– prawa szczegółowe – wynikające z przepisów szczegółowych RODO. Mam tu na myśli przepisy od art. 6 RODO do art. 37 RODO. Z prawami związane są wolności.

Ryzyko, które może być spowodowane przez naruszenie, to teoretycznie ryzyko naruszenia samych tylko praw osób fizycznych albo samych tylko wolności osób fizycznych, albo praw i wolności osób fizycznych, wydaje się jednak, że prawa i wolności są ze sobą na tyle powiązane, że niemożliwe jest naruszenie jednego bez naruszenia drugiego.

Ryzyko, o którym mowa w przepisie, jest ryzykiem wysokim.

W sytuacji zaistnienia wysokiego ryzyka, na administratorze spoczywa obowiązek zawiadomienia osób, których dane dotyczą.

Również naruszenie praw i wolności osoby, której dane dotyczą, skutkuje obowiązkiem zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych.

Zawiadomienie, o którym mowa, to zawiadomienie o naruszeniu ochrony danych osobowych, o którym mowa na wstępie przepisu.

Zawiadomienie, o którym mowa w przepisie, ma zostać wykonane bez zbędnej zwłoki.

3. Art. 34 ust. 1 Uwagi

3.1. Art. 34 ust. 1 Uwaga 1

Analogie do art. 33 ust. 1

Należy mieć świadomość, że art. 34 RODO, w tym analizowany tu art. 34 ust. 1 RODO, dotyczy sytuacji niezwykle podobnej do tej, której dotyczy art. 33 RODO. Ma miejsce zdarzenie, zdarzenie to jest albo nie jest naruszeniem opisanym w art. 4 pkt 12 RODO. Jeżeli zdarzenie jest takim naruszeniem, to administrator przystępuje do analizy zdarzenia – teraz już naruszenia ochrony danych osobowych. Administrator analizuje zdarzenie… I tu właśnie pojawia się różnica wobec art. 33 RODO.

– Na gruncie art. 33 ust. 1 RODO administrator ustala, czy naruszenie skutkuje ryzykiem dla praw i wolności osób, których dane dotyczą, „ryzykiem", czyli ryzykiem o poziomie, który nie jest niski i który nie jest wysoki. Administrator ustala również, czy naruszenie nie skutkuje niskim ryzykiem dla praw i wolności osób, których dane dotyczą. (Mowa więc, nieco upraszczając, o ryzyku o niskim poziomie i o ryzyku o średnim poziomie.)
– Na gruncie art. 34 ust. 1 RODO administrator ustala, czy naruszenie może skutkować lub skutkuje wysokim ryzykiem dla praw i wolności osób, których dane dotyczą. Ustala i postępuje stosownie do poziomu tego ryzyka, a mianowicie informuje osoby, których dane dotyczą. I w tym właściwie miejscu, rozważania nad art. 34 RODO mogłyby mieć swój finał. Można oczywiście poczynić kilka dodatkowych uwag i zajmują one kilka dalszych stron książki, jednak trzeba pamiętać, że z uwagi na analogię między brzmieniem przepisów a po prawdzie i obowiązkami, które z nich wynikają, uwagi te również nieco paralelne być muszą.

Zgodnie ze swoją metodą i praktyką badawczą, paraleli tych nie ukrywam, ale wręcz przeciwnie, wskazuję je i podkreślam, uważam bowiem, że jeżeli ten sam autor prowadzi wywód prawdziwie równoległy, to postępuje nierozsądnie, marnuje bowiem czas swój i czytelników na rozważania, które przeprowadził wcześniej. Poza tym skoro prowadzimy badania, to prowadzimy je po coś, a mianowicie po to, by z nich korzystać, zarówno w badaniach dalszych, jak i w praktyce. Z uwagi na nie tylko naukowy, ale również – mam nadzieję – praktyczny, charakter książki, zamieszczam niżej rozważania, które, o ile do

pewnego stopnia powtarzają rozważania dotyczące analogicznych fragmentów art. 34 RODO, o tyle mają one pewien walor praktyczny oraz – jak (tym razem z kolei) mam nadzieję – naukowy. Jeśli chodzi o rozważania uzasadniające niektóre tezy, to staram się je skracać i ewentualnie odsyłać do analogicznych, rozważań prowadzonych wyżej.

3.2. Art. 34 ust. 1 Uwaga 2

Ocena ryzyka naruszenia praw i wolności

Należy zwrócić uwagę, że podobnie jak na gruncie art. 33 ust. 1 RODO, z art. 34 ust. 1 RODO wynika obowiązek dokonania (wykonania, przeprowadzenia – wszystko jedno, jak czynność nazwiemy) oceny ryzyka naruszenia praw i wolności.

Podobnie jak w odniesieniu do art. 33 ust. 1 RODO, oceniający ryzyko naruszenia praw i wolności musi rozważyć dwa problemy. Są to te same dwa problemy, które podlegają rozważaniu na gruncie art. 33 ust. 1 RODO i jest to – być może – największym wyzwaniem w interpretacji art. 33 RODO. Jest tak, ponieważ związane są z tym właśnie dwa problemy, wymienione niżej.

– Po pierwsze – jakie prawa i wolności należy brać pod uwagę przy dokonywaniu oceny skutków naruszenia.
– Po drugie – jak należy dokonywać oceny skutków naruszenia. Jeżeli rozważania nad wskazanymi tu problemami są prowadzone po przeprowadzeniu analogicznych rozważań na gruncie art. 33 ust. 1 RODO, to okazuje się, że znaczna część rozważań tu, czyli na gruncie art. 34 RODO, jest analogiczna wobec rozważań prowadzonych na gruncie art. 33 RODO. Ujmując rzecz najkrócej,
– po pierwsze – prowadząc rozważania na gruncie art. **34** ust. 1 RODO, należy brać pod uwagę te same prawa i wolności, które są brane pod uwagę na gruncie art. **33** ust. 1 RODO,
– po drugie – prowadząc rozważania na gruncie art. **34** ust. 1 RODO, oceny skutków naruszenia należy dokonywać w ten sam sposób, w jaki skutki te oceniane są na gruncie art. **33** ust. 1 RODO.

Oczywiście jeżeli ktoś zacznie pracę, poczynając od art. 34 RODO i następnie przystąpi do pracy nad art. 33 RODO, to wniosek będzie analogiczny, tyle, że wtedy uzyskamy rozumowanie:

– po pierwsze – prowadząc rozważania na gruncie art. **33** ust. 1 RODO, należy brać pod uwagę te same prawa i wolności, które są brane pod uwagę na gruncie art. **34** ust. 1 RODO,
– po drugie – prowadząc rozważania na gruncie art. **33** ust. 1 RODO, oceny skutków naruszenia należy dokonywać w ten sam sposób, w jaki skutki te oceniane są na gruncie art. **34** ust. 1 RODO.

Intencjonalnie używam powyżej takich samych zdań dla podkreślenia podobieństwa między stosowaniem art. 33 ust. 1 RODO i art. 34 ust.1 RODO. Treść przepisów, na poziomie języka prawnego, różni się znacznie, uważam to jednak za błąd prawodawcy. Przepisy powinny być do siebie zbliżone – powiem więcej – uważam, że nic nie stoi na przeszkodzie, by treść obydwu przepisów połączona była w jednym przepisie. Uważam tak, ponieważ obydwa przepisy są stosowane w tych samych (nie tylko takich samych, ale dosłownie tych samych) stanach faktycznych. Ma miejsce zdarzenie, administrator ocenia ryzyko naruszenia praw i wolności i jedyne, co odróżnia przepisy od siebie, to obowiązek, który administrator musi zrealizować po wykonaniu oceny. Zawarcie całości zjawiska oceny skutków naruszenia w jednym przepisie ułatwiłoby dokonywanie tej oceny. Z tego też względu stawiam postulat nowelizacyjny, a nawet kilka (*6.1. Art. 34 ust. 1. Postulat 1. Połączenie przepisów. Wersja minimalistyczna*) i (*6.2. Art. 34 ust. 1. Postulat 2. Połączenie przepisów. Wersja pełniejsza*).

3.3. Art. 34 ust. 1 Uwaga 3

Prawa i wolności w RODO

Jak wskazuję wyżej: *Artykuł 34 ust. 1 RODO uzależnia zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych od poziomu ryzyka naruszenia praw i wolności osób fizycznych.* Dla realizacji tego obowiązku kluczowe jest ustalenie, jakie prawa i wolności należy brać pod uwagę przy dokonywaniu oceny na gruncie art. 34 ust. 1 RODO. Zagadnieniem tym zajmuję się w książce *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*[321] oraz w niniejszej książce w uwagach (*3.1. Art. 24 Uwaga 1. Prawa i wolności*), (*3.2. Art. 24 Uwaga 2. Przykładowe prawa i wolności*

[321] J. Rzymowski, *RODO – GDPR. Przedmiot i cele…*

zasadnicze), (*3.2. Art. 24 Uwaga 2. Przykładowe prawa i wolności szczegółowe*), (*3.4. Art. 24 Uwaga 4. Inne prawa i wolności*); uwagi te tyczą się art. 24 RODO. Zajmuję się tym również w niniejszej książce w uwagach (*3.4 Art. 32 ust. 1 i 2 i 3 Uwaga 4. Błędy w ocenie ryzyka*) i (*3.5 Art. 32 ust. 1 i 2 i 3 Uwaga 5. Prawa i wolności*), poczynionych przy okazji analizy art. 32 RODO. Również w uwagach (*3.1. Art. 33 ust. 1 Uwaga 1. Ocena ryzyka naruszenia praw i wolności*), (*3.2. Art. 33 ust. 1 Uwaga 2. Prawa i wolności przy ocenie skutków naruszenia*), (*3.3. Art. 33 ust. 1 Uwaga 3. Prawa i wolności w RODO. Zarys zagadnień*), (*3.4. Art. 33 ust. 1 Uwaga 4. Prawa i wolności w RODO. Naruszenie łącznie z naruszeniem innych praw i wolności*), (*3.5. Art. 33 ust. 1 Uwaga 5. Prawa i wolności. Źródła inne niż RODO*), (*3.6. Art. 33 ust. 1 Uwaga 6. Prawa i wolności w EKPC*), (*3.7. Art. 33 ust. 1 Uwaga 7. Prawa i wolności w KPP UE*), (*3.8. Art. 33 ust. 1 Uwaga 8. Naruszenie praw lub wolności jednej osoby fizycznej*), *(3.10. Art. 33 ust. 1 Uwaga 10. Naruszenie ochrony danych – zestawienie*), (*3.11. Art. 33 Uwaga 11. Naruszenie ochrony danych osobowych – metoda ustalenia*), (*3.14. Art. 33 Uwaga 14. Naruszenie ochrony danych osobowych. Kolejność działań*), (*3.16. Art. 33 Uwaga 16. Naruszenie ochrony danych osobowych w realiach współadministrowania*) poczynionych przy okazji analizy art. 33 ust. 1 RODO. Właśnie ze względu na fakt, że tyle uwag na temat praw i wolności wyżej poczyniłem, niżej sygnalizuję tylko podstawowe zjawiska.

Podstawowym zjawiskiem, o jakim należy pamiętać, jest to, że ilekroć na gruncie RODO jest mowa o prawach i wolnościach, tylekroć jest mowa o tych samych prawach i wolnościach. Za rozumowaniem takim przemawia dyrektywa konsekwencji terminologicznej, czyli zakaz wykładni homonimicznej. W prostej wersji brzmi on: *Tym samym zwrotom nie należy nadawać różnych znaczeń*[322]. Gdyby możliwe do wskazania były argumenty za nadawaniem różnych znaczeń zwrotowi „prawa i wolności", odpowiednio do miejsca w RODO, to sytuacja wyglądałaby inaczej. Argumentów takich nie widzę. Co więcej, cztery miejsca w RODO, do których się w niniejszej publikacji odnoszę, tworzą pewien system przepisów, które są ze sobą treściowo związane, ich zaś stosowanie skutkuje związkami funkcjonalnymi.

[322] L. Morawski, op. cit., s. 104–105.

Z art. 24 ust. 1 RODO wynika, że administrator ma obowiązek uwzględnić ***ryzyko naruszenia praw lub wolności osób fizycznych*** *o różnym prawdopodobieństwie i wadze* i następnie stosownie do prawdopodobieństwa i wagi administrator ma obowiązek wdrożyć *odpowiednie środki techniczne i organizacyjne*.

Z art. 32 ust. 1 RODO wynika, że administrator ma obowiązek uwzględnić ***ryzyko naruszenia praw lub wolności osób fizycznych*** *o różnym prawdopodobieństwie i wadze* i następnie stosownie do prawdopodobieństwa i wagi administrator ma obowiązek wdrożyć *odpowiednie środki techniczne i organizacyjne*.

Wbrew pozorom, między art. 24 ust. 1 RODO i art. 32 ust. 1 RODO zachodzi pewna różnica, o ile bowiem celem wdrożenia na gruncie art. 24 ust. 1 RODO jest zgodność przetwarzania z RODO, o tyle celem wdrożenia na gruncie art. 32 ust.1 RODO jest uzyskanie stopnia bezpieczeństwa, który odpowiada ocenionemu ryzyku. Różnica zachodzi, faktem jest jednak, że z obydwu wskazanych przepisów wynika spoczywający na administratorze obowiązek wykonania oceny ryzyka naruszenia praw i wolności osób fizycznych.

– Administrator dokonuje oceny ryzyka naruszenia praw i wolności osób fizycznych.
– Następnie administrator dostosowuje środki techniczne i organizacyjne do ryzyka, tak by ryzyko to miało poziom niski. Zachowywanie ryzyka na innym poziomie nie ma sensu. Jest tak, ponieważ inny niż niski poziom ryzyka naruszenia praw i wolności osób fizycznych to poziom, który w warunkach naruszenia ochrony danych skutkuje co najmniej obowiązkiem zgłoszenia naruszenia do PUODO.
– Następnie administrator po prostu przetwarza dane osobowe.
– Następnie ma miejsce zdarzenie zdefiniowane w art. 4 pkt 12 RODO jako naruszenie ochrony danych osobowych.
– Następnie administrator ma obowiązek dokonać oceny ryzyka naruszenia praw i wolności osób fizycznych. I tu właśnie niejako docieramy do art. 34 ust. 1 RODO (i oczywiście do art. 33 ust. 1 RODO). Naruszenie jest swojego rodzaju odejściem od przetwarzania danych osobowych w sposób zgodny z prawem, w sposób (powiedzmy) bezpieczny. Jednocześnie, kiedy zajdzie naruszenie ochrony danych osobowych, to administrator przystępuje do oceny ryzyka naruszenia praw i wolności, naruszenie bowiem ochrony danych

osobowych może w te prawa i wolności godzić. Ale w jakie prawa i wolności? Otóż naruszenie ochrony danych osobowych może godzić w te właśnie prawa i wolności, które administrator brał pod uwagę, oceniając ryzyko naruszenia praw i wolności na gruncie art. 24 RODO i 32 RODO. Gdyby administrator – dla potrzeb art. 24 RODO i art. 32 RODO – brał pod uwagę inne prawa i wolności niż dla potrzeb art. 33 RODO i art. 34 RODO, to ocena taka mogłaby poprowadzić na zupełne manowce. Należy pamiętać, że omawiany system zbudowany jest na podstawie pewnych następstw:

– ocena ryzyka naruszenia praw i wolności,
– dostosowanie ryzyka praw i wolności do poziomu akceptowalnego, czyli niskiego,
– zdarzenie godzące w poszanowanie praw i wolności (naruszenie ochrony danych osobowych),
– ocena ryzyka naruszenia praw i wolności.

Kiedy sobie to uświadomimy, to okazuje się, że fakt, iż należy brać pod uwagę te same prawa i wolności na gruncie art. 24 RODO i art. 32 RODO, jak również art. 33 RODO i art. 34 RODO, staje się oczywisty. Przecież gdyby administrator brał pod uwagę inne prawa czy inne zestawy praw dla potrzeb art. 24 RODO i art. 32 RODO i inne dla potrzeb art. 33 RODO i art. 34 RODO, to mogłoby się okazać, że naruszenie ochrony danych osobowych zaskutkowało ryzykiem dla innych praw i wolności niż te prawa i wolności, które brał pod uwagę administrator danych osobowych na gruncie art. 24 RODO i art. 32 RODO. System oceny ryzyka z góry, w ewentualnym przewidywaniu naruszenia powinien być spójny z systemem oceny ryzyka z dołu, po naruszeniu, nadaje to całości ochrony techniczno-organizacyjnej i ochrony praw i wolności pewien sens. Przypominam jednocześnie, że konieczność brania pod uwagę tych samych praw i wolności wykazuję wyżej na gruncie zasad wykładni.

Wiemy zatem, że na gruncie

– art. 34 ust. 1 RODO
– i na gruncie art. 33 ust. 1 RODO,
– i na gruncie art. 32 RODO,
– i na gruncie art. 24 RODO administrator powinien brać pod uwagę te same prawa i wolności.

Podobna myśl obecna jest u W. Chomiczewskiego, który wskazuje jednak na fakt, że *Prawa i wolności* (W. Chomiczewski odnosi się do praw i wolności na gruncie art. 34 ust. 1 RODO) *należy rozumieć podobnie jak na gruncie przepisu art. 6 ust. 1 lit. f […]*[323].

Pozostaje jedynie ustalić, o jakich to dokładnie prawach i wolnościach jest mowa w RODO, kiedy jest mowa o „prawach i wolnościach". Zajmuję się tym niżej – w skrócie, zaś wcześniej, wyżej na gruncie analizy art. 24 RODO i art. 32 RODO i art. 33 RODO – szerzej.

3.4. Art. 34 ust. 1 Uwaga 4

Zasady z art. 5 RODO jako prawa i wolności

Prawa i wolności, które administrator ma obowiązek wziąć pod uwagę przy ocenie skutków naruszenia na gruncie art. 34 ust. 1 RODO (również 33 ust. 1 RODO), to prawa i wolności, które prawodawca w tym celu wskazał, ponieważ umieścił je w RODO. Odnoszę się tu oczywiście do praw i wolności zapisanych jako zasady w art. 5 RODO. Konieczność brania pod uwagę tych właśnie praw i wolności wynika z zasady racjonalności ustawodawcy, mówiąc zaś wprost, do nieprawniczych czytelników, trzeba stwierdzić, że prawodawca nie umieścił zasad w art. 5 RODO i nie sformułował ich w przemyślany i przemyślny sposób jedynie dla ozdoby. Zasady porządkują RODO, zasady przejawiają się w przepisach szczegółowych RODO i do zasad, rozumianych jako prawa i wolności prawodawca odsyła (między innymi) w art. 34 ust. 1 RODO.

Zasadami na gruncie art. 5 RODO zajmuję się najszerzej w książce *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*[324]. Nie wskazuję konkretnych tytułów rozdziałów ni numerów stron, wskazana książka, oprócz tego, że stanowi częściowo komentarz do art. 5 RODO i do art. 6 RODO, zawiera również rozważania nad ontologią zasad jako ontologią praw i obowiązków.

---

[323] W. Chomiczewski, op. cit., s. 721.

[324] J. Rzymowski, *RODO – GDPR. Zasady dotyczące...*

Podsumowując,

– zasady z art. 5 RODO są niczym innym jak obowiązkami administratora.
– Zasady są obowiązkami administratora, więc tym samym są one prawami osób, których dane dotyczą, a precyzyjniej ująwszy – prawami każdej z osób, której dane dotyczą.
– System składający się z prawa i obowiązku (praw i obowiązków) służy ochronie wolności.

Z tej racji, że prawa i wolności zostały na gruncie art. 5 RODO nazwane zasadami (dotyczącymi przetwarzania danych osobowych), uważam, że te właśnie prawa i wolności należy nazywać prawami i wolnościami zasadniczymi. Szersze rozważania na ten temat prowadzę wyżej, na gruncie art. 33 RODO.

Zestawienie obowiązków, praw i wolności zasadniczych znajduje się na końcu niniejszej książki, w części zatytułowanej: *Tabele pomocnicze, zestawienia*.

3.5. Art. 34 ust. 1 Uwaga 5

Przepisy szczegółowe RODO jako prawa i wolności

W uzupełnieniu koncepcji zasygnalizowanej powyżej, zgodnie z którą zasady z art. 5 RODO to w istocie (nieco upraszczając) prawa i obowiązki i wolności, zwracam uwagę na fakt, że zasady z art. 5 ust. 1 RODO, na poziomie aktu prawnego są konkretyzowane przez przepisy szczegółowe RODO. Z kolei na poziomie realizacji obowiązków wynikających z zasad i z przepisów szczegółowych RODO, realizacja przepisów szczegółowych RODO pozwala na realizację zasad z art. 5 ust. 1 RODO. Można nieco metaforycznie stwierdzić, że konkretyzacja zasad ma kierunek od zasad do przepisów szczegółowych (przez przepisy szczegółowe), realizacja zasad zaś ma kierunek od przepisów szczegółowych (przez przepisy szczegółowe) do zasad. Przez realizację rozumiem tu wykonywanie konkretnych, przewidzianych przepisami czynności przez odpowiednie osoby.

Niewątpliwy związek przepisów szczegółowych z zasadami każe sądzić, że system oparty na obowiązku, prawie i wolności nie kończy się na zasadach, ale że obejmuje również przepisy szczegółowe. Można zatem stwierdzić, że przepisy szczegółowe RODO ustanawiają

równie szczegółowe obowiązki i równie szczegółowe uprawnienia i służą ochronie równie szczegółowych wolności.

Zestawienie obowiązków, praw i wolności szczegółowych znajduje się na końcu niniejszej książki, w części zatytułowanej: *Tabele pomocnicze, zestawienia*.

Wydaje się, że jeżeli administrator, osoba dokonująca oceny ryzyka naruszenia praw i wolności zna treść zasad z art. 5 ust. 1 RODO, to przy wykonywaniu ocen ryzyka naruszenia praw i wolności (czyli na gruncie art. 24, 32, 33, 34 RODO) osoba taka nie musi posiłkować się zestawieniem praw i wolności szczegółowych. Jeżeli jednak, czy to z braku wiedzy, czy to z ostrożności osoba wykonująca ocenę pragnie skorzystać z praw i wolności szczegółowych, to dobrze byłoby, gdyby osoba taka wiedziała, które prawa i wolności szczegółowe składają się, na które prawa i wolności zasadnicze. Wskazuję to w wydanej w 2020 roku, książce *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*[325], w podrozdziałach warstwy „konkretyzacja zasady". Wskazań tych nie powtarzam w niniejszej publikacji, odsyłam do wskazanej, która w momencie ostatecznej redakcji publikacji niniejszej jest dostępna na papierze i w wersji elektronicznej.

Podobne podejście dostrzegalne jest u Ch. Poszwińskiego, który w 2021 roku napisał w kontekście zjawiska prywatności w fazie projektowania, po tym jak wskazał pewne szczegóły, że: *Pozwoli to na uniknięcie ryzyka naruszenia przepisów rodo, a w konsekwencji – praw lub wolności podmiotu danych*[326]. Zarówno podejście moje, jak i podejście Ch. Poszwińskiego w sposób oczywisty wskazują, że jeżeli naruszone zostają przepisy RODO, to tym samym naruszone zostają prawa lub (i) wolności. Podejście Ch. Poszwińskiego jest nieco ostrożniejsze, pisze on bowiem o „prawach lub wolnościach", zachowując wierność tekstowi prawnemu, ja zwykle piszę o „prawach i wolnościach", odchodząc od tekstu prawnego na rzecz prawniczego zrozumienia. Chrystian Poszwiński pisze, że naruszenie praw lub wolności jest konsekwencją naruszenia przepisów RODO, ja raczej utożsamiam naruszenie przepisów RODO z naruszeniem praw i wolności, jeśli jednak nie jest to jedynie różnica językowa, czy różnica w sposobie

[325] Ibidem.

[326] Ch. Poszwiński, op. cit., s. 40.

wywodu, to i tak zarówno ze stanowiska wskazanego autora, jak i ze stanowiska mojego wynika, że naruszenie przepisów RODO z naruszeniem praw i wolności jest ściśle związane.

3.6. Art. 34 ust. 1 Uwaga 6

Prawa i wolności spoza RODO

Nic nie stoi na przeszkodzie, by dla potrzeb oceny ryzyka na gruncie art. 34 ust.1 RODO brać pod uwagę również inne prawa niż tylko prawa wskazane w RODO. Trzeba jednak jednoznacznie podkreślić. Prawodawca w sposób intencjonalny, nieprzypadkowy, wskazał na prawa i wolności zamknięte w zasadach. Jeżeli osoba, która dokonuje oceny na gruncie art. 34 ust. 1 RODO (lub na podstawie art. 33 RODO, 32 RODO, 24 RODO), pragnie ocenić ryzyko naruszenia również innych praw niż tylko tych zapisanych w art. 5 RODO, to wolno jej to zrobić, jednak nie wolno jej tymi innymi prawa zastąpić praw z art. 5 RODO. Nie wolno, ponieważ wtedy osoba taka stawia się w miejscu prawodawcy, odrzuca RODO i jego rozwiązania i w to miejsce stosuje rozwiązanie, które sobie wyimaginowała.

Kolejny akt prawny, który poświęcony jest prawom to Europejska Konwencja Praw Człowieka (dalej: EKPC). Na dziewiętnaście wymienionych tam praw, z uwagi na ich treść, do wykorzystania przy ocenie ryzyka nadają się może dwa. Szerzej zajmuję się tym w uwadze (*3.6. Art. 33 ust. 1 Uwaga 6. Prawa i wolności w EKPC*), zwracam tam też uwagę na wspomniane dwa prawa.

Na gruncie Konstytucji RP wspomnieć należy o prawie do ochrony danych osobowych zapisanym w art. 51 Konstytucji.

3.7. Art. 34 ust. 1 Uwaga 7

Naruszenie praw i wolności osób fizycznych

Z art. 34 ust. 1 RODO wynika, że jeżeli poziom ryzyka naruszenia praw i wolności **może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, to administrator ma obowiązek poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych.

Skoro sama możliwość zaistnienia wysokiego ryzyka **naruszenia praw lub wolności osób fizycznych** skutkuje po stronie administratora, obowiązkiem poinformowania osoby, której dane dotyczą

o naruszeniu ochrony danych osobowych, to również zaistnienie wysokiego ryzyka **naruszenia praw lub wolności osób fizycznych** skutkuje po stronie administratora, obowiązkiem poinformowania osoby, której dane dotyczą o naruszeniu ochrony danych osobowych.

W tym miejscu należy się odwołać do konstatacji poczynionej w (*1. Art. 34 ust. 1. Analiza*). Piszę tam: skoro wysokie ryzyko naruszenia praw i wolności skutkuje obowiązkiem zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, to również naruszenie praw i wolności osoby, której dane dotyczą, skutkuje obowiązkiem zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, co wynika z zasady znanej jako *argumentum a fortiori*[327]. Należy zwrócić uwagę na fakt, że oprócz **wystąpienia** (zaistnienia) **ryzyka** naruszenia praw i wolności osób fizycznych możliwe jest również **wystąpienie** (zaistnienie) **naruszenia** praw i wolności osób fizycznych. Już nie zagrożenia ryzykiem naruszenia ale naruszenia. Gdyby naruszenie praw i wolności osób fizycznych nie było możliwe, to ryzyko tego naruszenia też nie byłoby możliwe – nie miałoby po prostu sensu. Z przepisu wiemy, że możliwe jest wysokie ryzyko naruszenia praw i wolności osób fizycznych. Wysokie, niskie (art. 33 ust. 1 RODO), średnie (art. 33 ust. 1 RODO) – jakiekolwiek ryzyko jest możliwe. Fakt, że ryzyko jest możliwe, wynika z art. 34 ust. 1 RODO (i z art. 33 ust. 1 RODO). Skoro możliwe jest ryzyko naruszenia praw i wolności osób fizycznych, to znaczy, że naruszenie praw i wolności osób fizycznych również jest możliwe. Możliwość zaistnienia naruszenia praw i wolności osób fizycznych jest warunkiem koniecznym zaistnienia ryzyka naruszenia praw i wolności osób fizycznych.

Obserwowalne są zatem następujące, wymienione niżej poziomy.

– Naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.
– Naruszenie ochrony danych osobowych powoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych.
– Naruszenie ochrony danych osobowych skutkuje naruszeniem praw i wolności osób fizycznych.

Z art. 34 ust. 1 RODO wynika, że jeżeli poziom ryzyka naruszenia praw i wolności **może powodować wysokie ryzyko naruszenia**

[327] L. Morawski, op. cit., s. 219–222.

praw lub wolności osób fizycznych, to administrator ma obowiązek poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych.

Skoro możliwość wystąpienia wysokiego ryzyka naruszenia praw i wolności osób fizycznych skutkuje obowiązkiem poinformowania osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, to możliwość wystąpienia naruszenia praw i wolności osób fizycznych również skutkuje obowiązkiem poinformowania osoby, której dane dotyczą o naruszeniu ochrony danych osobowych. Wynika to z zasady znanej jako *argumentum a fortiori*[328].

Poziom ryzyka naruszenia praw i wolności określony jako wysoki i w ogóle sama możliwość wystąpienia ryzyka naruszenia praw i wolności osób fizycznych prowadzi do pewnej konstatacji. Otóż, jeżeli istnienie ryzyko naruszenia praw i wolności osób fizycznych, to zapewne możliwe jest też naruszenie praw i wolności osób fizycznych. Ta z kolei konstatacja prowadzi do kolejnej, związanej zdecydowanie z wysokim poziomem ryzyka naruszenia praw i wolności. Otóż skoro wysokie ryzyko naruszenia praw i wolności skutkuje obowiązkiem zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, to również naruszenie praw i wolności osoby, której dane dotyczą, skutkuje obowiązkiem zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, co wynika z zasady znanej jako *argumentum a fortiori*[329].

Pewien ślad rozumienia faktu, że oprócz ryzyka naruszenia praw i wolności osób fizycznych możliwe jest też naruszenie praw i wolności osób fizycznych, dostrzec można u W. Chomiczewskiego, pisze on bowiem, że: *Omawiana przesłanka nie wymaga, by wysokie ryzyko się zmaterializowało i by faktycznie doszło do naruszenia praw lub wolności. Dlatego nie ma znaczenia, czy ostateczne ich naruszenie nastąpi*[330]. Jak widać, wskazany autor widzi różnicę między ryzykiem a naruszeniem.

Jako pewien brak odczuwam fakt, że w przepisie mowa jest o ryzyku naruszenia praw i wolności, jednak o samym naruszeniu praw i wolności już nie. Wyżej wyjaśniam, że z problemem tym moż-

---

[328] Ibidem.

[329] Ibidem.

[330] W. Chomiczewski, op. cit.

na łatwo się uporać dzięki stosowaniu zasady *argumentum a fortiori*, uważam jednak, że przepis łatwo zrozumiały lepszy jest od przepisu lekko mętnego. W związku z tym uważam, iż należy postawić postulat *de lege ferenda*, który doprowadzi do pewnego rozjaśnienia przepisu w zakresie naruszenia praw i wolności osób fizycznych. Myśl tę finalizuję w postulacie (*6.2. Art. 34 ust. 1. Postulat 2. Połączenie przepisów. Wersja pełniejsza*).

3.8. Art. 34 ust. 1 Uwaga 8

Zawiadamianie osób, zgłaszanie PUODO

Uwagi porządkujące

Dla uporządkowania warto poczynić poniższe uwagi o charakterze swojego rodzaju przewodnika po naruszeniu. Poziomy ryzyka zostały opisane wyżej, przy okazji omawiania art. 24 RODO (*3.14. Art. 24. Uwaga 14. Poziomy ryzyka*).

– Zachodzi zdarzenie, które administrator kwalifikuje jako naruszenie ochrony danych osobowych, zdefiniowane w art. 4 pkt 12 RODO.
– Następnie administrator musi ustalić, czy może zachodzić ryzyko naruszenia praw i wolności osób fizycznych. Jeżeli zdarzenie dotyczyło danych osobowych, to za pewnik można przyjąć, że ryzyko naruszenie praw i wolności osób fizycznych może zachodzić.
– Następnie administrator musi ustalić poziom ryzyka naruszenia praw i wolności osób fizycznych. Ustalenie tego poziomu jest konieczne, ponieważ od tego, jaki poziom przyjmuje ryzyko, uzależnione są dalsze czynności administratora. Należy zauważyć, że decyzje dotyczące dalszych czynności administratora zostają podjęte niejako za niego. Administrator jedynie ustala poziom ryzyka i na tym kończy, a przynajmniej powinien kończyć jego wpływ na dalsze decyzje, przy czym oczywiście odnoszę się tu do decyzji w przedmiocie informowania osób, których dane dotyczą, o naruszeniu i zgłaszania tego naruszenia PUODO.
– Jeżeli nie zachodzi ryzyko naruszenia praw i wolności (*3.14. Art. 24. Uwaga 14. Poziomy ryzyka*)[331] albo jeżeli poziom ryzyka naruszenia praw i wolności jest niski, to administrator nie informuje nikogo. Nikogo, czyli ani osób, których dane dotyczą, ani

[331] Szczególnie odsyłam, w przypadku gdyby ten poziom był nieoczywisty dla czytelnika.

nie zgłasza naruszenia PUODO (właściwemu organowi nadzorczemu) (Art. 33 ust.1 RODO: *[...] chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych*). Dosłownie patrząc, należy tu mówić o niskim prawdopodobieństwie ryzyka naruszenia praw i wolności osób fizycznych.

– Jeżeli poziom ryzyka naruszenia praw i wolności nie jest niski i nie jest wysoki, to administrator zgłasza naruszenie PUODO (właściwemu organowi nadzorczemu). Dosłownie patrząc, jest to sytuacja, w której prawdopodobne jest, że naruszenie to skutkowało ryzykiem naruszenia praw i wolności osób fizycznych i jednocześnie naruszenie nie mogło powodować i nie powodowało wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. (Art. 33 ust.1 RODO).
– Jeżeli poziom ryzyka naruszenia praw i wolności może być wysoki lub jest wysoki (dosłownie patrząc naruszenie mogło spowodować lub spowodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych) to administrator ma obowiązek wykonać dwie czynności, wskazane poniżej[332].
– Administrator zawiadamia osoby, których dane dotyczą, o takim naruszeniu. I jednocześnie
– administrator zgłasza naruszenie PUODO (właściwemu organowi nadzorczemu).

Należy poczynić tu pewne uzupełnienie. Otóż w opisanej sytuacji administrator nie zawiadamia osób, których dane dotyczą, jeżeli zachodzą zdarzenia wymienione w art. 34 ust. 3 RODO, fragmenty którego cytuję poniżej. Mimo wysokiego poziomu ryzyka administrator nie zawiadamia osób, których dane dotyczą, o naruszenia, jeżeli:

a) *administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;*
b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

[332] Podobnie: A. Krasuski, [w:] A. Krasuski, P. Siembida, op. cit., s. 74.

c) zawiadomienie wymagałoby *niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.*

Na następnej stronie zamieszczony jest analogiczny schemat, jednak w ujęciu tabelarycznym. Tabela ta jest rozwinięciem tabeli, która znajduje się wyżej, w jednym z podrozdziałów poświęconych art. 24 RODO (*3.14. Art. 24. Uwaga 14. Poziomy ryzyka*).

Poszczególne wpisy w tabeli, w ujęciu z góry na dół lub z dołu do góry oddają poziomy ryzyka naruszenia praw i wolności osób, których dane dotyczą, czyli tabela stanowi jednocześnie wykres.

Poziomy ryzyka naruszenia praw i wolności osób fizycznych			**Podmioty lub osoby**, które administrator informuje / którym zgłasza naruszenie
Nazwa skrócona	Odpowiedni fragment przepisu (podstawa prawna)	Nazwa poprawna	
Ryzyko zrealizowane	Art. 34 ust. 1 RODO + zasada *a fortiori*	Naruszenie praw i wolności osób fizycznych	Osoby, których dane dotyczą, PUODO
Poziom ryzyka wysoki	Art. 34 ust. 1 RODO *Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.*	Wysokie ryzyko naruszenia praw i wolności osób fizycznych.	Osoby, których dane dotyczą, PUODO
Poziom ryzyka wysoki z zastrzeżeniami	Art. 34 ust. 3 RODO *Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane w następujących przypadkach: […]*		PUODO
Poziom ryzyka średni (podstawowy, niższy od wysokiego, wyższy od niskiego)	Art. 33 ust. 1 RODO *W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 […]*		PUODO
Poziom ryzyka niski	Art. 33 ust. 1 RODO *[…] chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.*	Ryzyko o małym prawdopodobieństwie naruszenia praw i wolności osób fizycznych.	Nikt
Brak ryzyka naruszenia praw i wolności osób fizycznych			Nikt

Wyżej w (*2. Art. 34 ust. 1. Wnioski z analizy*) i w (*1. Art. 34 ust. 1. Analiza*) piszę, że zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony danych osobowych, kiedy może zachodzić lub zachodzi wysoki poziom ryzyka naruszenia praw i wolności osób fizycznych *ma zostać wykonane bez zbędnej zwłoki*. Prawodawca nie wskazuje, w jakim czasie od naruszenia należy dokonać zawiadomienia, poza tym że wskazuje, że zawiadomienie *ma zostać wykonane bez zbędnej zwłoki*. Na problem ten zwracają uwagę P. Barta, M. Kawecki i P. Litwiński, trafnie odsyłając[333] do motywu 86 Preambuły RODO, którego fragment stanowi: *Na przykład potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie*. Wydaje się, że właśnie cytowany fragment wskazuje właściwą drogę postępowania. Jeżeli jest to celowe, to administrator informuje jak najszybciej, jeżeli jest to celowe, to administrator informuje później. Nie od rzeczy jest zwrócić uwagę na pogląd W. Chomiczewskiego, który zauważa, że mimo że obowiązek z art. 33 ust. 1 RODO i obowiązek z art. 34 ust. 1 RODO są analogiczne, to inna jest ich funkcja. W przypadku art. 34 ust. 1 RODO funkcją tego przepisu jest poinformowanie osoby o naruszeniu, tak by mogła ona lepiej chronić prawa i wolności wystawione (jak to pięknie ujął W. Chomiczewski) *na ryzyko wynikające z naruszenia ochrony danych osobowych*[334].

Z naukowej uczciwości uważam za stosowne umieszczenie pewnej uwagi. Otóż podczas końcowej redakcji książki zaprezentowałem znajdującą się tu tabelę w jednej z fejsbukowych grup poświęconych RODO. Jeden z dyskutantów[335] stwierdził, że poziomów jest za dużo i że powyżej poziomu niskiego dostrzega poziom wysoki. Dyskusja była niezwykle ciekawa (między innymi dlatego ją relacjonuję). Najciekawszym dla mnie elementem dyskusji było, kiedy mój Interlokutor zaproponował własne poziomy ryzyka, które – jak uważał – zachodzą powyżej ryzyka niskiego. Zaproponowane zostały

[333] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 357.

[334] W. Chomiczewski, op. cit., s. 719–720.

[335] Moim dyskutantem był p. Marcin Boruciński, z którym ustaliłem później, czy moja relacja odzwierciedla treść jego poglądów.

poziomy, które wskazuję poniżej, zaproponowane zostały łącznie ze wskazanymi podstawami prawnymi.
– Poziom wysoki pełny (art. 33 RODO i art. 34 RODO).
– Poziom wysoki z wyłączeniem (art. 33 RODO i art. 34 ust. 3 RODO).
– Poziom wysoki podstawowy (art. 33 RODO).

Analiza porównawcza stanowiska mojego rozmówcy i mojego wskazuje głównie na to, że ja użyłem nazwy „Poziom ryzyka średni (podstawowy, niższy od wysokiego, wyższy od niskiego)", mój rozmówca zaś użył nazwy „Poziom wysoki podstawowy".

Jeszcze inaczej poziomy ryzyka w swoim zestawieniu nazwali T. Izydorczyk i M. Gumularz, otóż widnieje u nich w tabeli następujące zestawienie:
– *ryzyko naruszenia praw lub wolności jest mało prawdopodobne*,
– *prawdopodobieństwo ryzyka jest wyższe niż mało prawdopodobne*,
– *ryzyko naruszenia praw lub wolności jest na wysokim poziomie*[336].

Wskazani autorzy trafnie łączą z odpowiednimi poziomami ryzyka odpowiednie obowiązki administratora. Wydaje się, że zarówno w kwestii poziomów ryzyka, jak i następstw przyjmowania przez ryzyko tychże, jesteśmy zgodni, a różnimy się jedynie nieco w warstwie przekazu poczynionych ustaleń.

3.9. Art. 34 ust. 1 Uwaga 9

Adresaci przepisu

Swojego rodzaju genialną uwagę stanowi wypowiedź M. Sakowskiej-Baryły. Autorka ta pisze, że: *Adresatami przepisu są co do zasady administrator i organ nadzorczy […]*[337]. Dalej autorka pisze, równie trafnie, że do podmiotów przetwarzających i do podmiotów podprzetwarzających (podmiotów przetwarzających drugiego i kolejnych stopni czy rzędów – autorka używa tu nazwy „subprocesor") przepis stosuje się jedynie pośrednio. Tym, jako stwierdzeniem trafnym, jednak nie noszącym znamienia geniuszu, nie zajmuję się dalej.

---

[336] M. Gumularz, T. Izydorczyk, op. cit., s. 25.

[337] M. Sakowska-Baryła, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie…*, s. 373.

Wracając do myśli, że *Adresatami przepisu są co do zasady administrator i organ nadzorczy […]*[338], należy zwrócić uwagę na wynikające z niej wnioski.

Po pierwsze, myśl jest genialna, jednak tyczy się raczej art. 33 ust. 1 RODO aniżeli art. 34 ust. 1 RODO. Nie wykluczam, że autorka pisząc, że organ nadzorczy jest adresatem przepisu, odnosi się do art. 34 ust. 4 RODO. Jeśli tak właśnie jest, to nie zgłaszam zastrzeżeń, jednak z komentarza M. Sakowskiej-Baryły, z uwagi na jego formę, nie wynika, do której części przepisu, które słowa się odnoszą, choć, być może jest to jedynie wynik mojego niezrozumienia.

Po drugie, kiedy już odniesiemy myśl do art. 33 ust. 1 RODO, to okazuje się ona jeszcze genialniejsza, choć w swym geniuszu prosta. Administrator ma obowiązek zgłaszać naruszenia ochrony danych osobowych, jeżeli poziom ryzyka naruszenia praw i wolności **nie jest** niski. Z tego właśnie wynika, że jeżeli poziom ryzyka naruszenia ochrony danych osobowych **jest** niski, to organ nadzorczy nie powinien takiego zgłoszenia przyjąć. Oczywiście może się zdarzyć, że administrator zgłosi naruszenie, którego poziom właśnie jest niski. Wydaje się, że w takiej sytuacji organ nadzorczy powinien jedynie poinformować administratora, że ten błądzi, że zgłoszenie w sensie fizykalnym zostało przyjęte, jednak skutków żadnych nie wywoła; wniosek ten wywodzę z faktu, iż uważam niepotrzebne zgłoszenia za swojego rodzaju zło. Jasne wypowiedzi PUODO mogłyby im zapobiec. Jednakim, a nawet niebezpieczniejszym dla administratora złem jest niezgłoszenie naruszenie, które zgłosić należy. W tej sprawie jasne wypowiedzi PUODO również zrobiłyby wiele dobrego.

Po trzecie, jeżeli zaszło naruszenie ochrony danych osobowych i poziom ryzyka naruszenia praw i wolności osób fizycznych jest lub może być wysoki, to oczywiste jest, że **nie jest** on niski. Jest to truizm – skoro jest wysoki, to **nie jest** niski, jednak z truizmu tego wynika daleko idący wniosek, otóż jeżeli poziom jest wysoki (czyli nie niski) to na administratorze spoczywa obowiązek zgłoszenia naruszenia organowi nadzorczemu. Być może tej właśnie sytuacji dotyczy wypowiedź M. Sakowskiej-Baryły, a mianowicie, że w takiej sytuacji na organie nadzorczym spoczywa obowiązek przyjęcia zgłoszenia.

---

[338] Ibidem.

3.10. Art. 34 ust. 1 Uwaga 10

Cel informowania osób, których dane dotyczą

Wyżej w (*3.4. Art. 33 Uwaga 1. Cel informowania organu nadzorczego*) zastanawiam się nad celem informowania organu nadzorczego (np. PUODO). Wywodzę tam, że wbrew stanowisku W. Chomiczewskiego[339], celem informowania organu nadzorczego jest ułatwienie organowi ochrony nadzorczemu nakładania kar. Stanowisko jedynie sygnalizuję i doń odsyłam. Jeśli chodzi o informowanie osób, których dane dotyczą, o naruszeniu ochrony danych osobowych, to zgadzam się z C. Burtonem. Autor ten twierdzi, że *Article 34 GDPR is intended to prevent the negative consequences that may result from a personal data breach by specifically providing affected individuals with the opportunity to take appropriate mitigating measures. The sooner that an individual becomes aware of a breach, the sooner they may undertake the necessary precautions in order to prevent or minimise the damage resulting from it*[340].

Na język polski tłumaczymy to jako: „Artykuł 34 RODO jest zamierzony, by zapobiegać negatywnym następstwom, które mogą wynikać z naruszenia ochrony danych osobowych, poprzez swoiste zapewnienie osobom, których to dotyczy możliwości podjęcia stosownych działań łagodzących. Im szybciej dana osoba dowie się o naruszeniu, tym szybciej może podjąć niezbędne środki ostrożności, aby zapobiec lub zminimalizować szkody z niego wynikające”[341].

Wyżej, kiedy wywodzę, że celem informowania organu nadzorczego jest ułatwienie mu nakładania kar, wskazuję, że informowanie organu ma miejsce kiedy *Dane zostały ujawnione. W gruncie rzeczy nie można już zrobić nic. W takim wypadku organowi pozostaje jedno. Nałożyć karę*. Informowanie osób, których dane dotyczą, zachodzi w analogicznej sytuacji, w której dane zostały ujawnione, to jest niejako taka sama sytuacja, a czasem nawet ta sama. Informowanie zachodzi w analogicznej sytuacji, jednak skutki informowania są inne. Osoba, której dane dotyczą, może podjąć jakieś środki zaradcze, choćby może ona zabezpieczyć dane osobowe przed kolejnymi naruszeniami.

[339] W. Chomiczewski, op. cit, s. 710.

[340] C. Burton, op. cit., s. 655.

[341] Tłumaczenie: J. Rzymowski.

niami. Poza tym osoba, której dane dotyczą, nie może nałożyć kary. Uważam, że kiedy sobie to uświadomimy, że informowana osoba może podjąć stosowne środki, o czym pisze C. Burton, to musimy sobie uświadomić, że informowanie organu nadzorczego ma na celu głównie ułatwienie nałożenia kary.

Powiem więcej, należy wyobrazić sobie, że art. 33 ust. 1 RODO nie funkcjonuje. Że obowiązek notyfikacyjny ogranicza się do informowania osób, których dane dotyczą. Cóż się wtedy dzieje? Otóż osoby, których dane dotyczą, zostają poinformowane o zagrożeniu, mogą podjąć środki zapobiegawcze. Nie ma (pozornie) zagrożenia karą, a środki i tak zostają podjęte, co (powiedzmy, do jakiegoś stopnia) pozwala chronić prawa i wolności osób, których dane dotyczą. Co ciekawe, droga do nałożenia kary nie jest w tak wyobrażonej sytuacji zamknięta. Osoba, której dane dotyczą, poinformowana o naruszeniu ochrony danych może w każdej chwili złożyć skargę do organu nadzorczego, a ów może nałożyć karę. Niestety, tak nie jest, można jednak postawić postulat nowelizacyjny (*6.4. Art. 34 ust. 1. Postulat 4. Uchylenie przepisu*).

3.11. Art. 34 ust. 1 Uwaga 11

Moment informowania osób, których dane dotyczą

Wyżej w (*1. Art. 33 ust. 1. Analiza*) zastanawiam się nad tym, od jakiego momentu należy liczyć 72-godzinny termin do zgłoszenia naruszenia do PUODO. Odsyłam do tamtych rozważań, tu sygnalizuję jedynie, że wskazuję tam, że moment, od którego należy liczyć czas, jest niejasny, do tego stopnia, że rzecz podsumowuję postulatem *de lege ferenda* (*6.1. Art. 33. Postulat 1. Jak liczyć termin 72-godzinny*). Jeśli chodzi o art. 34 ust. 1 RODO, to wskazanie, kiedy należy poinformować osobę, której dane dotyczą, jest jeszcze trudniejsze. Przepis wskazuje – co prawda – że należy uczynić to *bez zbędnej zwłoki*, jednak po prawdzie, nie jest to odpowiedź na pytanie o to, kiedy informować. Można tu oczywiście prowadzić szerokie rozważania nad tym, kiedy zwłoka jest zbędna, a kiedy nie, nie zamierzam jednak ich prowadzić. Rozsądny wydaje mi się tu pogląd C. Burtona, który wskazuje, powołując się przy tym na stanowisko Grupy Artykułu 29, że *the individual should be contacted as soon as it is reasonably feasible to*

do so[342]. Tłumaczymy to na język polski na: „z osobą należy skontaktować się tak szybko, jak jest to rozsądnie możliwe do zrobienia”[343]. Pogląd cytowany jest mi bliski z tego względu, że uważam, iż administrator powinien się liczyć z tym, że naruszenie ochrony danych osobowych o wysokim poziomie ryzyka dla praw i wolności osób, których dane dotyczą, może wywoływać po stronie tych osób skutki, których administrator nie obejmuje swoim rozumieniem, nie powinien więc skupiać się na wewnętrznych „przeżyciach” swojej organizacji, ale powinien po prostu poinformować osobę.

Z poglądem C. Burtona koresponduje pogląd P. Barty, M. Kaweckiego i P. Litwińskiego. Otóż zwracają oni uwagę na fakt[344], że w przeciwieństwie do art. 33 RODO, art. 34 RODO nie zawiera nawet instrukcyjnego terminu, w jakim należałoby informować o naruszeniu osoby, których dane dotyczą, jednak wskazują również na motyw 86 Preambuły RODO, który stanowi, że *Administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych […]*. Również pogląd jednego z autorów czeskiego komentarza wskazuje[345] na konieczność informowania osób po to, by mogły one powziąć odpowiednie zabezpieczenia.

3.12. Art. 34 ust. 1 Uwaga 12

Informowanie jednej osoby fizycznej

Wyżej w (*3.8. Art. 33 ust. 1 Uwaga 8. Naruszenie praw lub wolności jednej osoby fizycznej*) zastanawiam się nad informowaniem organu nadzorczego (PUODO), jeżeli ryzyko (o nie niskim poziomie) dotyczy praw i wolności jednej tylko osoby fizycznej, czyli o informowaniu organu nadzorczego na gruncie art. 33 ust. 1 RODO.

---

[342] C. Burton, op. cit., *s.* 660.

[343] Tłumaczenie: J. Rzymowski.

[344] P. Barta, M. Kawecki, P. Litwiński, op. cit., s. 357.

[345] Š. Král, [w:] J. Pattynová, L. Suchánková, J. Černy, M. Růžička a kolektiv. *Obecné nařízeni o ochraně osobnich údajů (GDPR) Zákon o zpracováni osobnich údajů. Komentá,* Praha 2019, s. 272–273.

Artykuł 34 ust. 1 RODO dotyczy sytuacji, w której naruszenie ochrony danych osobowych

– może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych lub
– powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, lub
– skutkuje naruszeniem praw lub wolności osób fizycznych.

W związku z powyższym trzeba się zatrzymać nad tym, czy jeżeli naruszenie dotyczy praw i wolności jednej osoby fizycznej, to osobę tę należy informować.

Przeanalizujmy po kolei.

Najpierw zajmijmy się art. 33 RODO.

Z art. 33 ust. 1 RODO wynika, że administrator ma obowiązek informować organ nadzorczy, jeżeli naruszenie ochrony danych dotyczy praw i wolności **osób fizycznych** (liczba mnoga).

Z motywu 85 Preambuły RODO również wynika, że naruszenie, które jest zgłaszane organowi nadzorczemu, dotyczyć musi więcej niż jednej osoby fizycznej. W motywie tym czytamy bowiem, że: *[...] naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u* ***osób fizycznych***. I dalej czytamy, że administrator nie zgłasza naruszenia jeżeli: *[...] administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności* ***osób fizycznych***.

Jak widać, jeśli chodzi o art. 33 RODO, czyli o zgłoszenie naruszenia ochrony danych organowi nadzorczemu, treść art. 33 ust. 1 RODO znajduje potwierdzenie w treści motywu 85 Preambuły RODO. Jeżeli zatem naruszenie ochrony danych osobowych dotyczy jednej osoby fizycznej, to administrator nie ma obowiązku informowania organu (PUODO) o tym naruszeniu. To wynika z przepisów. Na tym wywód ten powinien się zakończyć. Nie widzę powodu, by nie dostrzegać realiów funkcjonowania PUODO i właśnie z tego powodu, mając na względzie bezpieczeństwo prawne administratora, uważam, że jeżeli naruszenie ochrony danych osobowych dotyczy jednej osoby, to administrator powinien poinformować PUODO. Nie dlatego, że ma taki obowiązek, ale dlatego, że tak nakazuje ostrożność. Oczywiście odnoszę się do sytuacji, w której poziom ryzyka naruszenia praw i wolności osób fizycznych, tu jednej osoby fizycznej, uzasadnia poinformowanie PUODO.

Teraz zajmijmy się art. 34 RODO.

Z art. 34 ust. 1 RODO na pierwszy rzut oka wynika, że administrator ma obowiązek informować osobę, której dane dotyczą, jeżeli naruszenie ochrony danych dotyczy praw i wolności **osób fizycznych** (liczba mnoga). Wnosimy to ze słów: *Jeżeli naruszenie ochrony danych osobowych może powodować wysokie* ***ryzyko naruszenia praw lub wolności osób fizycznych*** *[...]* (liczba mnoga). Uczciwość nie pozwala pominąć, że w tym samym przepisie czytamy o informowaniu osoby fizycznej (liczba pojedyncza): *administrator bez zbędnej zwłoki zawiadamia* ***osobę, której dane dotyczą****, o takim naruszeniu* (liczba pojedyncza). W związku z powyższym można by mieć wątpliwość, czy należy informować osobę fizyczną o naruszeniu na gruncie art. 34 RODO, jeżeli naruszenie dotyczy praw i wolności tej tylko jednej osoby. Uzasadniony byłby pogląd, że jeżeli naruszenie dotyczy praw i wolności jednej osoby to nie należy informować tej osoby o tym naruszeniu. Jak jednak wyżej piszę, wniosek ten jest uprawniony na pierwszy rzut oka.

Z motywu 85 Preambuły RODO wynika, że *Administrator powinien bez zbędnej zwłoki poinformować* ***osobę, której dane dotyczą****, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności* ***tej osoby*** *[...]*. Jak widać, w Preambule czytamy, że jeżeli naruszenie *[...] może [...] powodować wysokie ryzyko naruszenia praw lub wolności [...]* ***osoby*** *[...]* to administrator ma obowiązek *poinformować* ***osobę, której dane dotyczą***.

Widać zatem, że treść art. 34 ust. 1 RODO nie znajduje potwierdzenia w treści motywu 86 Preambuły RODO. Pozostaje więc pytanie o to, co czynić. Uważam, że trzeba tu przeprowadzić pewne rozumowanie. Otóż w art. 34 ust. 1 RODO zapisane jest prawo osoby, której dane dotyczą, do bycia poinformowaną o tym, że nastąpiło naruszenie ochrony danych osobowych. Prawo to jest elementem prawa osoby, której dane dotyczą do tego, by jej dane były przetwarzane w sposób przejrzysty, zapisanego w art. 5 ust. 1 lit a RODO pod postacią zasady przejrzystości.

Nie wyjaśniam tu całej koncepcji związanej z art. 5 RODO. Poświęcam mu kilkaset stron książki z cyklu, którego i niniejsza książka jest częścią i do której odsyłam, czyli *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych*

osobowych z prawem[346]. Tu ograniczam się do przypomnienia, że art. 5 ustanawia zasady. Zasady to obowiązki administratora i jednocześnie prawa (uprawnienia) osoby, której dane dotyczą i jednocześnie system składający się z prawa sprzężonego z obowiązkiem służy ochronie wolności osób, których dane dotyczą. Jednocześnie zasady z art. 5 RODO są konkretyzowane przez przepisy szczegółowe RODO. Artykuł 34 RODO jest jednym z przepisów, które konkretyzują zasadę przejrzystości. Administrator ma obowiązek realizować zasady. Realizując zasady, administrator danych osobowych przede wszystkim realizuje prawa osób, których dane dotyczą. Administrator realizuje zasady poprzez realizowanie odpowiadających zasadom przepisów szczegółowych RODO. Jeżeli administrator nie zrealizuje odpowiedniego przepisu szczegółowego RODO, to odpowiadająca mu zasada zostanie złamana lub naruszona. W przypadku zasady przejrzystości możemy mówić raczej o naruszeniu tej zasady, jest to bowiem raczej dworkinowska zasada (*a principle*) niż hartowska reguła (*a rule*).

Oczywiście nadal pozostajemy z wątpliwością, której źródłem jest to, że co innego wynika z art. 34 RODO i co innego wynika z motywu 86 Preambuły RODO. Na podstawie przeprowadzonych wyżej rozważań dotyczących konkretyzacji zasady przejrzystości przez art. 34 RODO można jednak wyprowadzić pewien wniosek. Nie ma pewności, jak realizować art. 34 ust. 1 RODO. Nie ma pewności, czy należy informować osobę fizyczną o naruszeniu, jeżeli naruszenie dotyczy tylko jej praw i wolności. Nie ma pewności ale… Ale można przyjąć, że należy starać się tak zrealizować przepis szczegółowy, by nie naruszyć zasady, którą on konkretyzuje i by dać tej zasadzie możliwie najpełniejsze miejsce do działania, emanowania, funkcjonowania.

Jeżeli administrator informuje osobę, której dane dotyczą, o naruszeniu ochrony danych, które dotyczy tylko jej danych osobowych, to zasada przejrzystości jest realizowana pełniej, niżby administrator informował osobę, której dane dotyczą, o naruszeniu ochrony danych jedynie wtedy, gdy naruszenie to dotyczy więcej niż jednej osoby fizycznej.

Podsumowując, należy stwierdzić, że jeżeli naruszenie ochrony danych o wysokim poziomie ryzyka dotyczy jednej tylko osoby fi-

[346] J. Rzymowski, *RODO – GDPR. Zasady dotyczące...*

zycznej, to administrator danych osobowych ma obowiązek poinformować tę osobę o tym naruszeniu.

3.13. Art. 34 ust. 1 Uwaga 13

Rola podmiotu przetwarzającego

w realizacji art. 34 RODO

Ciekawe spostrzeżenie znajdziemy u C. Burtona, który zwraca uwagę[347] na rolę podmiotu przetwarzającego w realizacji art. 34 RODO. W przepisie tym nie wspomina się o podmiocie przetwarzającym. Rola podmiotu przetwarzającego pozornie wyczerpuje się w art. 33 ust. 2 RODO, z którego wynika, że jeżeli podmiot przetwarzający stwierdzi naruszenie, to ma on obowiązek poinformowania administratora o tym naruszeniu. Obowiązki podmiotu przetwarzającego kończą się w tym miejscu tylko pozornie. Należy zwrócić uwagę na art. 28 ust. 3 lit. f RODO. Z przepisu tego wynika, że podmiot przetwarzający *uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36*. Cedric Burton zwraca uwagę na to, że podmioty przetwarzające powinny wspierać administratorów w komunikacji z osobami, których dane dotyczą i przypomina, że szczegóły tego wsparcia powinny być uregulowane w umowie. Pozostaje tylko dodać, że rola podmiotu przetwarzającego może być szczególnie istotna w stanie faktycznym, w którym podmiot przetwarzający zbiera i przechowuje dane osobowe w imieniu administratora. Należy pamiętać, że możliwy jest administrator, który nie styka się w sensie fizykalnym z danymi osobowymi, które są przetwarzane w jego imieniu. W takiej sytuacji administrator może nie być w stanie poinformować osób, których dane dotyczą, o naruszeniu, jeżeli w informowaniu tym podmiot przetwarzający nie udzieli mu wsparcia.

4. Art. 34 ust. 1 Podsumowanie w duchu

Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

---

[347] C. Burton, op. cit., s. 661–662.

– Art. **34 ust. 1** RODO nakłada na administratora **obowiązek** zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, jeżeli naruszenie ochrony danych osobowych może powodować lub powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Jednocześnie

– Art. **34 ust. 1** RODO przyznaje osobie, której dane dotyczą, **uprawnienie** polegające na tym, że jeżeli ma miejsce naruszenie ochrony danych osobowych i jeżeli to naruszenie może powodować lub powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to administrator ma obowiązek poinformowania tej osoby o fakcie zaistnienia naruszenia.

5. Art. 34 ust. 1 Konkretyzacja zasad

Podrozdział poświęcony konkretyzacji zasad znajduje się niżej i jest częścią podrozdziału poświęconego art. 34 ust. 3 RODO. Zastosowałem to przesunięcie, ponieważ uważam rozróżnianie poszczególnych ustępów art. 34 RODO, pod kątem konkretyzacji zasad, za niecelowe.

6. Art. 34 ust. 1 Postulaty *de lege ferenda*

6.1. Art. 34 ust. 1 Postulat 1

Połączenie przepisów. Wersja minimalistyczna

Wyżej w uwadze (*3.2. Art. 34 ust. 1 Uwaga 2. Ocena ryzyka naruszenia praw i wolności*) zwracam uwagę na fakt, że art. 33 ust. 1 RODO i art. 34 ust. 1 RODO dotyczą tej samej sytuacji, sytuacji naruszenia ochrony danych. W związku z tym racjonalne, a przede wszystkim prostsze do zrozumienia, a siłą rzeczy i do zastosowania, byłoby rozwiązanie oparte nie na dwóch przepisach, na jednym przepisie. Nowelizacja przepisu może tu iść dwiema podstawowymi drogami. Dla porządku umieszczam postulaty nowelizacyjne w osobnych podrozdziałach.

Pierwsza możliwość nowelizacji polega na prostym połączeniu obydwu przepisów. Takie minimalistyczne rozwiązanie ma pewien urok. Można otóż dopuścić, że legislatorzy, którzy obydwa przepisy pisali, poprowadzili nad regulowanym zjawiskiem jakieś studia. Ograniczenie zmian do minimum pozwala na zachowanie ewentualnego wyniku tych studiów, w postaci oryginalnych przepisów zachowanych w treści przepisu znowelizowanego. Druga możliwość nowelizacji

polega nie na samym połączeniu przepisów, ale i na uporządkowaniu ich treści.

Mając na uwadze powyższe, postuluję nowelizację art. 33 ust. 1 RODO i art. 34 ust. 1 RODO we wskazany poniżej sposób.

Postuluję, by przepis, o którym tu mowa, miał postać:

„1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia również osobę, której dane dotyczą, o takim naruszeniu".

(Podział przepisu na ustępy ma charakter jedynie techniczny, ułatwiający ewentualne powoływanie jego fragmentów.)

6.2. Art. 34 ust. 1 Postulat 2 i 3

Połączenie przepisów. Wersja pełniejsza

Uzupełnienie przepisu o naruszenie praw i wolności

Niżej przedstawiam propozycję nowelizacji przepisu, która jest mi bliższa. Wyżej w postulacie (*6.1. Art. 34 ust. 1. Postulat 1. Połączenie przepisów. Wersja minimalistyczna*) piszę o tej propozycji jako o drugiej możliwej. Uzasadnienie dla nowelizacji jest analogiczne jak do wcześniejszej i wynikające z uwag zawartych w uwadze (*3.2. Art. 34 ust. 1 Uwaga 2. Ocena ryzyka naruszenia praw i wolności*).

Mając na uwadze powyższe oraz fakt, że jestem zwolennikiem zrozumiałych przepisów, proponuję jeszcze jedną zmianę w przepisie. Piszę otóż wyżej (*3.7. Art. 34 ust. 1 Uwaga 7. Naruszenie praw i wolności osób fizycznych*), że uważam, iż niedobrze, że w przepisie nie ma mowy o naruszeniu praw i wolności osób fizycznych, a że jest jedynie mowa o ryzyku naruszenia. By ten – w moim mniemaniu – brak uzupełnić, postuluję umieszczenie w przepisie ustępu, który uzależnia poinformowanie osób, których dane dotyczą, o naruszeniu

ochrony danych osobowych również od naruszenia ich praw i wolności, a nie jedynie od ryzyka naruszenia tychże praw i wolności.

Postuluję tu również umieszczenie ustępu, który dotyczy sytuacji, w której ryzyko naruszenia praw i wolności nie zachodzi. Sytuacja ta nie wydaje się prawdopodobna, jednocześnie wydaje się możliwa, a skoro jest możliwa, to przepis powinien ją przewidywać.

Ponadto zwracam uwagę na pewną niejasność przepisu, która wynika z faktu, że znajdują się w nim pojęcia: „naruszenie ochrony danych osobowych" i „naruszenie praw i wolności osób fizycznych" i to w dodatku też w formie skróconej: „naruszenie". Dla jasności postuluję dokładne wskazywanie w przepisie, o które to naruszenie chodzi.

Kolejną rzeczą, o której należy pamiętać, jest to, że naruszenie ochrony danych mogło skutkować takim czy innym ryzykiem w momencie zaistnienia tego naruszenia, mogło skutkować w momencie wykrycia, ale może też skutkować nadal – w czasie prowadzenia rozważań nad naruszeniem przez administratora. Artykuł 33 ust. 1 RODO stanowi, że: *[...] chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych [...]*,art. 34 ust. 1 RODO zaś stanowi, że: *Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych [...]*. Jeden przepis odnosi się do ryzyka jako do zjawiska, które miało miejsce i może nadal ma miejsce, a może już nie ma miejsca, ale (chyba) już raczej nie ma miejsca. Drugi przepis odnosi się do ryzyka jako do zjawiska, które ma miejsce, czyli zapewne mogło mieć miejsce wcześniej i ma miejsce nadal. Widzę możliwość wywodzenia jakichś wniosków z różnicy między ryzykiem, które było, ryzykiem, które jest, ale już skoro naruszenie było, to zapewne nadal jest. Widzę możliwość, jednak nie widzę sensu, by wywód taki prowadzić.

Gdyby wywód poprowadzić to uzyskujemy (nieco upraszczam):
– niskie ryzyko, które było,
– niskie ryzyko, które było i jest,
– niskie ryzyko, które jest;
– średnie ryzyko, które było,
– średnie ryzyko, które było i jest,
– średnie ryzyko, które jest;
– wysokie ryzyko, które było,
– wysokie ryzyko, które było i jest,

– wysokie ryzyko, które jest;
– naruszenie, które było,
– naruszenie, które było i jest,
– naruszenie, które jest.

Można by to rozpisać w przepisie, wydaje się to jednak być pewnym szaleństwem na granicy absurdu. To szaleństwem jest, ale jednocześnie pominięcie faktu, że zjawisko może zajść i się skończyć lub zajść i nadal trwać, nie wydaje się właściwe. W związku z tym, w poniższym postulacie *de lege ferenda* postuluję między innymi uwzględnienie faktu, że ryzyko może być ryzykiem przeszłym, a może też być ryzykiem zachodzącym, podobnie jak z naruszeniem.

Mając na uwadze powyższe, postuluję nowelizację art. 33 ust. 1 RODO i art. 34 ust. 1 RODO we wskazany poniżej sposób.

Postuluję, by przepis, o którym tu mowa, miał postać:

„1. W przypadku naruszenia ochrony danych osobowych, administrator ocenia, czy naruszenie ochrony danych osobowych skutkowało lub skutkuje nadal ryzykiem naruszenia praw lub wolności osób fizycznych, lub naruszeniem praw lub wolności osób fizycznych.
2. Jeżeli naruszenie ochrony danych osobowych skutkowało lub skutkuje nadal ryzykiem naruszenia praw lub wolności osób fizycznich, lub naruszeniem praw lub wolności osób fizycznych, to administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia ochrony danych osobowych – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
3. Jeżeli jest mało prawdopodobne, że naruszenie ochrony danych osobowych skutkowało lub skutkuje nadal ryzykiem naruszenia praw lub wolności osób fizycznych, lub naruszeniem praw lub wolności osób fizycznych, to administrator nie zgłasza naruszenia ochrony danych osobowych organowi nadzorczemu.
4. Jeżeli naruszenie ochrony danych osobowych mogło lub może nadal powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, lub naruszenie praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu".

Mimo możliwości graficznych, nie zaznaczam elementów postulowanych, ponieważ przepis – na dobra sprawę – prawie cały ma charakter postulatu *de lege ferenda*.

6.4. Art. 34 ust. 1 Postulat 4

Uchylenie przepisu

Wyżej w uwadze (*3.10. Art. 34 ust. 1 Uwaga 10. Cel informowania osób, których dane dotyczą*) i w uwadze (*3.4. Art. 33 Uwaga 1. Cel informowania organu nadzorczego*) zwracam uwagę na fakt, że art. 33 ust. 1 RODO służy głównie temu, by organowi nadzorczemu łatwiej było nakładać kary administracyjne. Ślad takiego poglądu dostrzegam w wypowiedzi M. Gumularza i T. Izydorczyka, którzy piszą, że identyfikowanie i szacowanie ryzyka ma na celu dostosowanie wdrożenia wymogów RODO do realiów administratora i wspominają przy tym o art. 24, 25, 32 i 35 RODO[348]. Jak widać z powoływanej wypowiedzi, w art. 33 i 34 nie chodzi o wdrożenie. Nie chcę słów wskazanych autorów nadinterpretować, ale nie sposób nie zauważyć, że pisząc o wdrożeniu, pominęli art. 33 i art. 34 RODO. Likwidacja art. 33 RODO utrudniłaby nakładanie kar, ponieważ organ nadzorczy nie dowiadywałby się automatycznie, po naruszeniu, że to naruszenie miało miejsce. Mimo tego likwidacja art. 33 RODO nie uniemożliwiałaby nakładania kar związanych z naruszeniami ochrony danych, gdyby bowiem nadal informowano o naruszeniach osoby, których dane dotyczą, to te osoby mogłyby składać skargi do organu nadzorczego. Przełożyłoby to znaczną część decyzji o ukaraniu z rąk organu nadzorczego w ręce osób, których dane dotyczą, czyli osób prawdziwie pokrzywdzonych naruszeniem, a co najmniej nim dotkniętych. Ponadto nie uważam, by utrudnienie nakładania kar było jakimkolwiek problemem. Nie uważam, by celem regulacji takich jak RODO było nakładanie kar. Celem jest uregulowanie jakiejś relacji, może ochrona praw i wolności, choć tu mam wątpliwości, ale nakładanie kar celem nie jest, a przynajmniej być nie powinno.

Mając na uwadze powyższe, postuluję nowelizację art. 33 RODO poprzez jego uchylenie.

---

[348] M. Gumularz, T. Izydorczyk, op. cit., s. 104.

Mam świadomość, że postulat niniejszy jest pozornie sprzeczny z postulatem (*6.1. Art. 34 ust. 1. Postulat 1. Połączenie przepisów. Wersja minimalistyczna*) i z postulatem (*6.2. Art. 34 ust. 1. Postulat 2. Połączenie przepisów. Wersja pełniejsza*), jednak jest to sprzeczność pozorna. Badam przepisy i stawiam kolejne postulaty. RODO widzę jako pewien ogród. Zaprojektowany, zaplanowany, przemyślany, jednak niedopracowany. Widać w nim rękę i myśl projektanta, nie widać jednak ręki troskliwego wykonawcy. Niektóre drzewa trzeba usunąć, inne trzeba nieco zmienić, przyciąć, są też jednak takie, które można czy to przyciąć, czy to usunąć i niezależnie od tego co się uczyni, efekt będzie lepszy, niż obecnie jest.

6.5. Art. 34 ust. 1 Postulat 5

Zmiana funktora

Wyżej, na przykład w uwagach (*3.2. Art. 34 ust. 1 Uwaga 2. Prawa i wolności w RODO*) i (*3.4. Art. 34 ust. 1 Uwaga 4. Zasady z art. 5 RODO jako prawa i wolności*) wywodzę na temat zjawiska praw i wolności. By nie powtarzać prowadzonych tam rozważań, tu stwierdzam jedynie, że nie sądzę, by możliwe było naruszenie praw bez naruszenia wolności i jednocześnie nie sądzę, by możliwe było naruszenie wolności bez naruszenia praw. Tym samym użycie przez prawodawcę funktora „lub" jest błędem, może bowiem sugerować możliwość naruszenia praw bez naruszenia wolności i naruszenie wolności bez naruszenia praw.

Mając na uwadze powyższe, postuluję nowelizację art. 34 ust. 1 RODO we wskazany poniżej sposób.

Postuluję, by przepis, w zakresie proponowanej zmiany, o której tu mowa, miał postać:

„Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw ~~lub~~ **i** wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu […]".

(Czcionką przekreśloną zaznaczyłem element usunięty z przepisu, czcionką pogrubioną i podkreśloną zaznaczyłem element wstawiony do przepisu.)

6.6. Art. 34 ust. 1 Postulat 6

Wskazanie praw i wolności

W wielu uwagach do art. 33 RODO zastanawiam się nad zjawiskiem praw i wolności, zjawisko to istotne jest też dla realizacji art. 34 RODO. Artykuł 33 RODO i art. 34 RODO dotyczą tej samej kategorii stanów faktycznych, a jedynie przewidują inne skutki, stosownie do poziomu ryzyka naruszenia praw i wolności. Przepisy te są tak wzajemnie bliskie, że wyżej proponuję mi.in. ich połączenie (*6.2. Art. 34 ust. 1. Postulat 2 i 3. Połączenie przepisów. Wersja pełniejsza. Uzupełnienie przepisu o naruszenie praw i wolności*). Prawa i wolności są więc ważne dla realizacji art. 33 RODO, jak i 34 RODO. Jeżeli jeden administrator bada naruszenie ochrony danych przez pryzmat jakichś praw i wolności, a inny przez pryzmat innych praw i wolności, to w odniesieniu do analogicznego naruszenia mogą zostać podjęte różne decyzje. Samo to może nie jest niewłaściwością, po prostu administratorzy nieco inaczej dokonują subsumpcji. Jeśli jednak zagadnieniu przyjrzymy się bliżej, to okazuje się, że godzi to w pewność prawa. Osoba, której dane dotyczą, ma prawo oczekiwać, że jeżeli zajdzie zdarzenie o charakterze naruszenia ochrony danych osobowych, to administrator to naruszenie oceni pod kątem ryzyka naruszenia praw i wolności i postąpi stosownie do wyniku tej oceny. Jeżeli jednak administrator może zupełnie swobodnie decydować o tym, jakie prawa i wolności bierze pod uwagę, to zarówno prawo osoby, której dane dotyczą, jak i obowiązek administratora stają się iluzoryczne.

Drugi problem polega na tym, że jeżeli administrator oceni ryzyko naruszenia praw i wolności, wziąwszy przy tym pod uwagę niewłaściwe prawa i wolności, zwłaszcza te, których w danej sytuacji nie naruszono lub którym nie zagrożono, to administrator taki podejmie niewłaściwą decyzję dotyczącą zgłoszenia naruszenia do PUODO i poinformowania osób. Zagrożenie (naruszenie) praw i wolności ma miejsce, administrator ocenia inne prawa niż naruszone i wskutek tego nie zgłasza naruszenia. W opisywanej sytuacji prawo osoby, której dane dotyczą, do tego, by poinformowano PUODO lub (odpowiednio), by poinformowano tę osobę i PUODO, zostaje naruszone (piszę tu oczywiście o stanach faktycznych, w których poziom ryzyka naruszenia praw i wolności uzasadnia co najmniej poinformowanie PUODO).

Trzeci problem polega na tym, że administrator, który ocenił ryzyko naruszenia praw i wolności przez pryzmat naruszenia niewłaściwych praw i wolności, sam naraża się na oskarżenie o to, że nie zgłosił naruszenia, mimo że powinien był to uczynić.

Zasygnalizowane tu problemy są następstwem tego, że z art. 33 ust. 1 RODO i z art. 34 ust. 1 RODO wynika obowiązek oceny ryzyka naruszenia praw i wolności, jednak prawodawca nie wskazuje, o jakich prawach i wolnościach mowa. Uważam, że przede wszystkim należy brać pod uwagę prawa i wolności wskazane w art. 5 RODO. Jestem w stanie wyobrazić sobie obowiązek oceny innych praw i wolności, jednak obowiązek, by traktować go poważnie, by w ogóle zaistniał, musi być zapisany w przepisie, a nie wymagać wyimaginowania go przez interpretatorów.

W związku z powyższym postuluję, by w art. 34 ust. 1 RODO i w art. 34 ust. 1 RODO wskazano, jakie prawa i wolności administrator powinien brać pod uwagę, kiedy ocenia ryzyko naruszenia praw i wolności osób, których dane dotyczą.

Postuluję, by przepis w zakresie proponowanej zmiany, o której tu mowa, miał postać:

„W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, **wskazanych w art. 5 RODO**. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

(Czcionką pogrubioną zaznaczyłem element wstawiony do przepisu.)

Podkreślam, że istotą tego postulatu nie jest taka czy inna dokładnie treść przepisu, istotą jest wskazanie, jakie prawa i wolności administrator ma obowiązek brać pod uwagę w realiach naruszenia ochrony danych osobowych.

Art. 34 ust. 3 RODO

Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

1 i 2 Art. 34 ust. 3

Analiza i wnioski z analizy

W odróżnieniu od reszty książki, w niniejszym podrozdziale łączę zawartość potencjalnego podrozdziału warstwy „wnioski z analizy" z zawartością potencjalnego podrozdziału warstwy „analiza".

Pierwszą przyczyną, dla której to czynię, jest racjonalność (tak jak ją rozumiem) prowadzenia wywodu. Uważam, że Czytelnikom,

zwłaszcza mniej biegłym, łatwiej będzie czytać analizowany i omawiany przepis w takim nieco skomasowanym ujęciu.

Drugą przyczyną, dla której to czynię, jest chęć pełniejszej prezentacji możliwości jakie daje etapowa analiza semantyczna. W innych rozdziałach i podrozdziałach niniejszej publikacji i pozostałych publikacji z cyklu, stosuję pewien schemat omawiania przepisu. Schemat ten nie jest jednak nierozerwalnie związany z przyjętą metodą badawczą. Etapowa analiza semantyczna może być z powodzeniem stosowana w oderwaniu od schematu, w którym najpierw zapisujemy komentarz, jednak wcześniej jeszcze przeprowadzamy analizę (jak czyniłem w książkach poprzednich) lub w którym najpierw zapisujemy przeprowadzana analizę, a następnie zapisujemy wnioski z analizy, czy krótki komentarz (jak z uwagi na życzenie Wydawcy czynię w książce niniejszej). Czynności te, a zwłaszcza ich prezentacja, mogą mieć różną kolejność, mogą też być połączone i właśnie w niniejszym rozdziale połączone są.

Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

Ze słów pogrubionych w przepisie: ***Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:*** wynika, że zawiadomienie osoby, której dane dotyczą, nie jest konieczne, administrator nie ma obowiązku informować osoby, której dane dotyczą o naruszeniu ochrony danych, mimo wysokiego ryzyka naruszenia praw i wolności tej osoby, jeżeli zachodzi jeden z przypadków opisanych w kolejnych punktach (literach) art. 34 ust. 3 RODO.

Należy zwrócić uwagę na fakt, że środki o których mowa, są niezależne od siebie. Treść art. 34 ust. 3 lit b RODO może na pierwszy rzut oka budzić myśl, że może przepis ten jest uzupełnieniem art. 34 ust. 3 lit a RODO. Myśl tę należy jednak odrzucić. Odrzucić, ponieważ zwrot *zastosował następnie* odnosi się do naruszenia, czyli należy to czytać jako „zastosował następnie po naruszeniu ochrony danych osobowych". Zwrot ten nie odnosi się do art. 34 ust. 3 lit. a RODO.

Należy zwrócić uwagę, że środki organizacyjne i techniczne, o których mowa w przepisie, muszą być zastosowane przed naruszeniem, inne po naruszeniu. Zastosowanie środków przed naruszeniem minimalizuje ryzyko naruszenia praw i wolności osób fizycznych,

choć należy pamiętać, że cały art. 34 RODO dotyczy sytuacji, kiedy ryzyko naruszenia praw i wolności osób fizycznych jest wysokie. Mimo tego przepis zachowuje sens. Ryzyko jest wysokie, więc administrator powinien poinformować osoby o naruszeniu, jednak jednocześnie, mimo wysokiego ryzyka, okazuje się, że administrator zastosował środki organizacyjne i techniczne. Ryzyko prawdopodobnie nadal jest wysokie, jednak zastosowanie środków organizacyjnych i technicznych obniża to ryzyko na tyle, że poinformowanie osób, których dane dotyczą, przestaje być konieczne.

Widoczne jest to zwłaszcza po treści art. 34 ust. 2 lit. a RODO, w którym mowa jest o tym, że jednym ze środków jest szyfrowanie. Jeżeli naruszenie ochrony danych osobowych polega na ujawnieniu tych danych, to nie sposób mówić nawet o samym tylko **ryzyku** dla praw i wolności, ale zachodzi **naruszenie** tych praw i wolności. Jeżeli jednak ujawnione dane zostały wcześniej zaszyfrowane, to ujawnienie jednocześnie i ma miejsce, i nie ma miejsca. Ma miejsce, dane bowiem w sensie fizykalnym ujawnione zostały. Nie ma miejsca, z uwagi bowiem na fakt, że dane są zaszyfrowane, nikt się z ich treścią nie może zapoznać, mimo faktu fizykalnego ujawnienia danych. Gdyby zastosowanie środków miało miejsce po naruszeniu, to przepis traci sens.

Wyobraźmy sobie, że ma miejsce naruszenie ochrony danych osobowych. Ktoś nieupoważniony się z tym danymi zapoznaje. Administrator sobie to uświadamia i szyfruje dane osobowe, z którymi ktoś się wcześniej zapoznał. Administrator szyfruje dane, pozornie podnosi poziom bezpieczeństwa, ale przecież zło już się stało – dane zostały ujawnione. Ponieważ dane zostały ujawnione, to ich zaszyfrowanie nie ma już znaczenia dla praw i wolności osób, których dane dotyczą, oczywiście nie ma znaczenia w kontekście naruszenia, które jest przedmiotem namysłu.

Z kolei art. 34 ust. 3 lit b RODO dotyczy sytuacji, kiedy to miało miejsce naruszenie, jednak administrator po zaistnieniu naruszenia podjął środki, których celem jest eliminacja wysokiego ryzyka naruszenia praw i wolności osoby. Wydaje się, że przepis ten dotyczy raczej sytuacji, które zachodzą wewnątrz struktury administratora.

Wyobraźmy sobie, że ma miejsce naruszenie ochrony danych osobowych. Dane zostają narażone na zniszczenie lub ujawnienie. Administrator sobie to uświadamia i podejmuje kroki przeciwdziałające odpowiednio zniszczeniu lub ujawnieniu danych. Tu zło zostało

skonsumowane w postaci zagrożenia wystąpieniem wysokiego ryzyka, jednak administrator podjął środki i w ten sposób obniżył poziom tego zagrożenia.

Artykuł 34 ust. 3 lit. c RODO zdecydowanie odnosi się do czynności administratora, które mają miejsce po zaistnieniu naruszenia ochrony danych osobowych. Wyobraźmy sobie, że miało miejsce naruszenie ochrony danych osobowych. Tu raczej rodzaj tego naruszenia nie ma znaczenia dla rozważań, za to znaczenie ma jego skala. Naruszenie miało zatem miejsce. Naruszenie to mogło spowodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Administrator dochodzi jednak do wniosku, że jego wysiłek związany z poinformowaniem osób, których dane dotyczą, byłby „niewspółmierny". Zapewne niewspółmierny do ryzyka, choć można tu mieć wątpliwość, skoro ryzyko jest wysokie. W takim wypadku administrator miast informować detalicznie kolejne osoby, wydaje publiczny komunikat lub stosuje środek do komunikatu podobny.

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

Ze słów pogrubionych w przepisie: ***administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych***, wraz z fragmentem wprowadzającym art. 34 ust. 2 RODO wynika, że słowa te opisują pierwszy z trzech warunków, których realizacja zwalnia administratora ze zgłaszania naruszenia organowi ochrony danych

Ze słów pogrubionych w przepisie: ***administrator wdrożył*** *[...]* ***środki ochrony*** *[...]* wynika, że pierwszym z warunków jest wdrożenie przez administratora danych osobowych środków ochrony doprecyzowanych w przepisie.

Ze słów pogrubionych w przepisie: *[...]* ***odpowiednie*** *[...]* ***środki ochrony*** *[...]* wynika, że środki ochrony, o których mowa, określone są jako „odpowiednie", wydaje się więc, że choćby z uwagi na obowiązek rozliczalności wynikający z art. 5 ust. 2 RODO, administrator powinien stworzyć i zachować pewne dowody. Dowody, z których wynika, że środki ochrony, o których mowa w przepisie, rzeczywiście są odpowiednie i że administrator to wie, ponieważ fakt odpowiedniości środków ocenił. Zapewne ocenił jeszcze na etapie realizacji art. 32 ust. 2 RODO.

Ze słów pogrubionych w przepisie: *[...]* ***techniczne i organizacyjne środki ochrony*** *[...]* wynika, że środki o których mowa w przepisie, mają charakter techniczny i organizacyjny.

Ze słów pogrubionych w przepisie: *[...]* ***i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie****, […]* wynika, że jeżeli środki, o których mowa w przepisie, mają być brane pod rozwagę, to administrator ma je obowiązek nie tylko wdrożyć, ale i jednocześnie zastosować je do tych danych osobowych, których dotyczy naruszenie ochrony danych osobowych.

Wydaje się, że przepis dotyczy sytuacji, w której środki zostały zastosowane w dwóch możliwych grupach sytuacji.

– Pierwsza to sytuacje, w których jest sens mówić o środkach, jeżeli zostały one zastosowane przed naruszeniem, czyli na etapie wdrażania art. 32 RODO.
– Druga to sytuacje, w których można mówić o środkach, które zastosowano po zaistnieniu naruszenia.

To czy ma miejsce pierwsza czy druga sytuacja zależy zarówno od zastosowanych środków, jak i przede wszystkim od charakteru naruszenia.

– Jeśli naruszenie ochrony danych osobowych ma charakter zdarzenia, które zaistniało i jego skutkom nie ma już jak zapobiec, to mamy do z pierwszą grupą sytuacji. Przy naruszeniach należących do tej grupy możemy mówić o środkach, o których mowa w przepisie, jeżeli środki te zostały zastosowane przed zaistnieniem naruszenia ochrony danych, zapewne na etapie realizacji art. 32 RODO.
– Jeśli naruszenie ochrony danych osobowych ma charakter zagrożenia zdarzeniem lub zdarzenia, którego skutkom jest jeszcze jak zapobiec po zaistnieniu naruszenia ochrony danych, to mamy do czynienia z drugą grupą sytuacji. Przy naruszeniach należących do

tej grupy możemy mówić o środkach, o których mowa w przepisie, jeżeli środki te zostały zastosowane po zaistnieniu naruszenia ochrony danych, na etapie realizacji omawianego przepisu, czy też szerzej, całego art. 34 RODO.

Ze słów pogrubionych w przepisie: *[...]* ***w szczególności środki takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych*** wynika, że administrator może zastosować różne środki techniczne i organizacyjne, jednak z uwagi na użycie zwrotu „w szczególności", administrator powinien zastosować środki wymienione w przepisie. Należy przy tym zauważyć, że w przepisie jest w istocie mowa o jednym środku, jakim jest szyfrowanie danych osobowych. Istotą środków, o których jest mowa w przepisie, jest, by środki te uniemożliwiały odczyt danych osobowych osobom nieuprawnionym. Środkiem takim wydaje się też być pseudonimizacja.

Przepis odnosi się do sytuacji, w której administrator ma przeciwdziałać ujawnieniu danych osobowych i jak się wydaje dostępowi do tych danych. Sytuacje takie, o charakterze ryzyk, omówione zostały wyżej przy okazji analizowania art. 32 ust. 2 RODO w (*1.2.1.5 Art. 32 ust. 2. Analiza szczegółowa dalsza* ***Ryzyka związane z dostępem do danych osobowych***). Ryzyka te następnie zostawione zostały wyżej w (*3.2. Art. 32 ust. 1 i 2 i 3 Uwaga 2. Zagrożenia uporządkowane w oparciu o kryterium konkretnego zagrożenia*). Dla ułatwienia lektury, powtarzam niżej same listy ryzyk.

„Ryzyka związane z ujawnieniem danych osobowych.

– Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych,
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych,
– Przypadkowe i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych,
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych,
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.

– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych,
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych,
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.

Ryzyka związane z dostępem do danych osobowych
– Przypadkowy i nieuprawniony dostępu do danych osobowych przesyłanych,
– Przypadkowy i nieuprawniony dostęp do danych osobowych przechowywanych,
– Przypadkowy i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych,
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych,
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.,
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych".

Jeżeli jedno ze wskazanych wyżej zdarzeń zajdzie, zwłaszcza jeżeli zajdzie jedno ze zdarzeń z grupy: ***Ryzyka związane z ujawnieniem danych osobowych***, jeżeli ryzyko się zrealizuje, to wszelkie działania administratora są już daremne. Dane zostały ujawnione, nic nie pomoże, że po ujawnieniu administrator te same dane na przykład zaszyfruje, jeżeli zostały one ujawnione w wersji niezaszyfrowanej. Tutaj działania administratora, o których stanowi przepis, mają sens, jeżeli zostały zastosowane przed zaistnieniem naruszenia ochrony danych. W przypadku zdarzeń z grupy: ***Ryzyka związane z dostępem do danych osobowych*** sytuacja wygląda analogicznie. Możliwa jest też jednak sytuacja, kiedy stosowanie na przykład szyfrowania ma sens.

Jeżeli żadne ze wskazanych zdarzeń nie zajdzie, a jedynie zajdzie wysokie ryzyko zaistnienia takiego zdarzenia, czyli na przykład jeżeli ma miejsce ryzyko ujawnienia danych osobowych, to działania administratora mają sens. Dane nie zostały ujawnione, dane mogły zostać ujawnione, ale ujawnienie nie nastąpiło, ryzyko się nie zrealizowało. Tutaj działania administratora mają sens nie tylko przed zaistnieniem zdarzenia, ale i po jego zaistnieniu.

Z działaniami przed zaistnieniem zdarzenia mamy do czynienia, jeżeli zagrożenie zdarzeniem miało miejsce wobec danych, w stosunku do których, przed zaistnieniem zdarzenia zastosowano środki ***uniemożliwiające odczyt***.

Z działaniami po zaistnieniu zdarzenia mamy do czynienia, jeżeli zagrożenie zdarzeniem miało miejsce wobec danych, w stosunku do których przed zaistnieniem zdarzenia nie zastosowano „środków uniemożliwiających odczyt", wtedy uniemożliwiające odczyt zastosowano po zaistnieniu zdarzenia, ale że zdarzenie miało charakter zagrożenia ujawnieniem danych, a nie ujawnienia danych i dane ujawnione nie zostały, to nic złego się nie stało, a na przyszłość zadziałają zapewne wdrożone właśnie środki ***uniemożliwiające odczyt***.

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

Ze słów pogrubionych w przepisie: ***administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1***, wraz z fragmentem wprowadzającym art. 34 ust. 2 RODO wynika, że słowa te opisują drugi z trzech warunków, których realizacja zwalnia administratora ze zgłaszania naruszenia organowi ochrony danych

Ze słów pogrubionych w przepisie: ***administrator zastosował*** *[...]* ***środki*** *[...]* wynika, że pierwszym z warunków jest zastosowanie przez administratora środków doprecyzowanych w przepisie.

Ze słów pogrubionych w przepisie: *[...]* ***zastosował następnie*** *[...]* wynika, że środki o których mowa mają być zastosowane następnie. Fakt, że środki mają być zastosowane następnie odróżnia je

od środków, o których mowa jest w art. 32 ust. 2 lit. a RODO. O ile środki, o których mowa w art. 32 ust. 2 lit. a RODO powinny być zastosowane przed naruszeniem, w jego ewentualnym przewidywaniu, o tyle środki o których tu mowa to środki zastosowane po naruszeniu.

Ze słów pogrubionych w przepisie: *[...]* ***zastosował*** *następnie* ***środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1***, wynika, że środki o których mowa to środki, które eliminują prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osoby, której dane dotyczą i które to dane zostały dotknięte naruszeniem ochrony danych osobowych.

Jak zatem widać, mamy tu do czynienia z sytuacją, w której zachodzi naruszenie ochrony danych osobowych, które *może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 34 ust. 1 RODO)*, jednak po zdarzeniu o charakterze naruszenia ochrony danych administrator stosuje środki, które eliminują możliwość zaistnienia wysokiego ryzyka praw i wolności. Skoro ryzyko przestaje być wysokie, a przestaje być wysokie, bo wysokie ryzyko zostało wyeliminowane działaniem, o którym tu mowa, to administrator nie informuje osób, których dane dotyczą, o naruszeniu. Nie informuje, ponieważ ryzyko co prawda było wysokie, jednak wprowadzenie środków owo ryzyko obniżyło.

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Ze słów pogrubionych w przepisie: ***wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób***, wraz z fragmentem wprowadzającym art. 34 ust. 2 RODO wynika, że słowa te opisują trzeci z trzech warunków, których realizacja zwalnia administratora ze zgłaszania naruszenia organowi ochrony danych

Ze słów pogrubionych w przepisie: ***wymagałoby ono** […] **wysiłku**. […]* wynika, że administrator nie informuje osób których dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli informowanie wymagałoby wysiłku. Wysiłku zapewne po stronie administratora lub po stronie podmiotu przetwarzającego, który w jakiś sposób mógłby być w ewentualne, ale niedoszłe informowanie zaangażowany.

Ze słów pogrubionych w przepisie: *[…]* ***niewspółmiernie dużego wysiłku**. […]* wynika, że wysiłek, który miałby być podjęty przez administratora byłby niewspółmiernie duży. Należy zwrócić baczną uwagę na obydwa słowa. Przede wszystkim przedmiotowy wysiłek, którego podjęcie zwalniałoby z informowania osób, których dane dotyczą, musiałby być duży. Oprócz tego wysiłek ten, co wydaje się nie mniej, a może i bardziej ważne, musiałby być niewspółmiernie duży. Zwracam szczególną uwagę na niewspółmierność wysiłku. Zwracam też uwagę na fakt, że współmierność czy niewspółmierność, by miała sens, musi być odnoszona do jakiegoś zjawiska. Tu zjawiskiem tym jest zapewne informowanie osób, których dane dotyczą, o naruszeniu ochrony danych osobowych w sytuacji, w której naruszenie to może skutkować wysokim poziomem ryzyka naruszenia praw i wolności osób fizycznych.

Ze względu na bezpieczeństwo prawne administratora właściwe się wydaje, by administrator sporządził i zachował dokument będący dowodem na to, że dokonano oceny współmierności wysiłku, że była ona niewspółmierna, kto jej dokonał, kiedy.

3. Art. 34 ust. 3 Uwagi

3.1. Art. 34 ust. 3 Uwaga 1

Brak obowiązku

Przepis dotyczy sytuacji, w której nastąpiło naruszenie ochrony danych osobowych (zdefiniowane w art. 4 pkt 12 RODO), naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, jednak administrator nie ma obowiązku zgłaszać takiego naruszenia jeżeli zachodzi któreś ze zjawisk opisanych w przepisie. Do zjawisk tych odnoszę się wyżej, tu zwracam uwagę na doniosły element wynikający ze zwrotu wprowadzającego. Zwrot ten brzmi: *Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach*. Czytamy, że: *Zawiadomienie […] nie jest*

wymagane, należy zatem zapewne uznać, że należy to rozumieć tak, że w przypadkach opisanych w przepisie, administrator danych nie ma obowiązku zawiadamiać osoby, której dane dotyczą. Administrator nie ma takiego obowiązku, jednak nadal wolno mu to zrobić. Nie jestem zwolennikiem realizowania obowiązków „na wszelki wypadek", jednak w sytuacji, w której administrator naprawdę miałby wątpliwość, czy poinformować osobę (osoby), czy nie poinformować, to spojrzywszy przez pryzmat jego bezpieczeństwa prawnego, można uznać, że lepiej, by poinformował osoby, niżby miał tego nie czynić.

3.2. Art. 34 ust. 3 Uwaga 2

Moment zastosowania środków

Wydaje się, że szczególnej uwagi wymaga moment w którym administrator danych osobowych musi zastosować środki organizacyjne i techniczne, aby zastosowanie środków zwalniało go z obowiązku informowania osób o naruszeniu. Problem ten dotyczy zjawisk opisanych w art. 34 ust. 3 lit a RODO i lit. b RODO. Właśnie jeśli chodzi o te dwa zjawiska, to moment ich zaistnienia, o którym mowa w przepisie, jest zupełnie inny.

Jeśli chodzi o wdrożenie środków technicznych i organizacyjnych, które uniemożliwiają odczyt danych osobom nieuprawnionym, to ważne, by to „wdrożenie" miało miejsce przed zaistnieniem naruszenia ochrony danych osobowych. Ujmując to nieco inaczej, dane, których dotyczyło naruszenie muszą to być dane, wobec których wcześniej zastosowano środki uniemożliwiające odczyt tych danych. Przepis ma sens jedynie wtedy, jeżeli środki zastosowane właśnie przed naruszeniem, czyli kiedy ujawnieniu uległy zaszyfrowane dane osobowe. Wydaje się, że przepis można zastosować również, kiedy ujawnieniu uległy spseudonimizowane dane osobowe, oczywiście pod warunkiem, że informacje, które umożliwiają odwrócenie pseudonimizacji, nie zostały ujawnione razem z danymi.

Jeśli chodzi o zastosowanie środków eliminujących prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, to zastosowanie to może mieć miejsce po zaistnieniu naruszenia ochrony danych osobowych. Oczywiście ma to sens, jeżeli środki dotyczą tych danych, których dotyczyło naruszenie. Czyli jeżeli na przykład naruszenie miało charakter uszkodzenia noś-

nika z danymi, jednak dane udało się odzyskać, to takie odzyskanie danych osobowych to właśnie środki, o których mowa w przepisie.

3.3. Art. 34 ust. 3 Uwaga 3

Możliwość stosowania przepisu

Wyżej w (*3.7. Art. 34 ust. 1 Uwaga 7. Naruszenie praw i wolności osób fizycznych*) zastanawiam się nad zjawiskiem naruszenia praw i wolności osób fizycznych. Wywodzę tam, że art. 34 ust. 1 RODO dotyczy głównie trzech zjawisk związanych z wysokim ryzykiem naruszenia danych osobowych. Zjawiska te wymieniam poniżej.

– Naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
– Naruszenie ochrony danych osobowych powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
– Naruszenie ochrony danych osobowych powoduje naruszenie praw lub wolności osób fizycznych.

Wydaje się, że art. 34 ust. 3 RODO nie nadaje się w całości do zastosowania w każdej ze wskazanych wyżej sytuacji. Dlaczego tak uważam? Otóż kiedy analizuję art. 34 ust. 3 RODO, to widzę, że dotyczy on sytuacji, w której ma miejsce naruszenie ochrony danych osobowych, naruszenie to może skutkować wysokim ryzykiem naruszenia praw i wolności osób fizycznych, jednak (i tego właśnie głównie dotyczy przepis) administrator podejmuje kroki, wskutek których ryzyko naruszenia praw i wolności osób fizycznych zostaje obniżone. Obniżenie ryzyka ma jednak sens wtedy, kiedy rzeczywiście fakt, czynność, akt obniżenia ryzyka, rzeczywiście zmniejsza prawdopodobieństwo zaistnienia naruszenia praw i wolności osób fizycznych. Czynność obniżenia ryzyka nie może mieć charakteru czynności obrzędowo konwencjonalnej typu: przygotowanie dokumentów czy przeszkolenie pracowników. Czynność obniżenia ryzyka musi mieć charakter czynności, która rzeczywiście ryzyko związane z danym naruszeniem obniża. Jednak dostrzegam tu pewne niebezpieczeństwo. Może się otóż zdarzyć, że zajdzie naruszenie ochrony danych, jednak w związku z tym naruszeniem nie da się obniżyć ryzyka naruszenia praw i wolności. Nie da się obniżyć, ponieważ jest to naruszenie ochrony danych osobowych, w związku z którym nie mamy do czynienia z ryzykiem naruszenia praw i wolności, ale z naruszeniem praw i wol-

ności. Niżej odnoszę się do każdej ze wskazanych wyżej sytuacji, patrząc na nie przez pryzmat art. 34 ust. 3 RODO. Świadomie powtarzam znaczne fragmenty rozumowań, by w ten sposób podkreślić elementy, które odróżniają opisywane sytuacje.

– Naruszenie ochrony danych osobowych **może powodować wysokie ryzyko** naruszenia praw lub wolności osób fizycznych.

I jednocześnie:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

lub

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1.

Takie rozwiązanie ma sens. Ma miejsce naruszenie ochrony danych osobowych. Ryzyko naruszenia praw i wolności może być wysokie. Ryzyko wysokie nie jest, ale może się takim okazać.

Okazuje się jednak, że zachodzi jedna z dwóch sytuacji, opisuję je poniżej.

– Wcześniej, przed naruszeniem ochrony danych osobowych administrator danych osobowych wdrożył środki ochrony, o których mowa w art. 34 ust. 1 lit. a RODO. Administrator danych osobowych wdrożył takie środki i namysł nad całością zdarzenia pozwala uznać, że z faktu, że wdrożono środki, wynika, że odczytanie danych osobowych przez osoby nieuprawnione jest niemożliwe. W związku z tym **administrator danych osobowych nie informuje osób**, których dane dotyczą o tym, że miało miejsce naruszenie ochrony danych osobowych.

– Po naruszeniu ochrony danych osobowych administrator danych osobowych zastosował środki, o których mowa w art. 34 ust. 1 lit. b RODO. Administrator danych osobowych zastosował takie środki i namysł nad całością zdarzenia pozwala uznać, że z faktu, że zastosowano środki, wynika, że wyeliminowano *prawdopodobieństwo wysokiego ryzyka naruszenia* praw i wolności osoby (osób), której dane dotyczą. W związku z tym **administrator danych osobowych nie informuje**

tej osoby lub tych osób, których dane dotyczą, o tym, że miało miejsce naruszenie ochrony danych osobowych.

– Naruszenie ochrony danych osobowych **powoduje wysokie ryzyko** naruszenia praw lub wolności osób fizycznych.

I jednocześnie:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

lub

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1.

Takie rozwiązanie również ma sens. Ma miejsce naruszenie ochrony danych osobowych. Ryzyko naruszenia praw i wolności jest wysokie. Ryzyko wysokie nie tylko (jak wyżej) może się wysokim okazać, ale już wysokie jest.

Okazuje się jednak, że zachodzi jedna z dwóch sytuacji, opisuję je poniżej.

– Wcześniej, przed naruszeniem ochrony danych osobowych administrator danych osobowych wdrożył środki ochrony, o których mowa w art. 34 ust. 1 lit. a RODO. Administrator danych osobowych wdrożył takie środki i namysł nad całością zdarzenia pozwala uznać, że z faktu, że wdrożono środki, wynika, że odczytanie danych osobowych przez osoby nieuprawnione jest niemożliwe. W związku z tym **administrator danych osobowych nie informuje osób**, których dane dotyczą, o tym, że miało miejsce naruszenie ochrony danych osobowych.
– Po naruszeniu ochrony danych osobowych administrator danych osobowych zastosował środki, o których mowa w art. 34 ust. 1 lit. b RODO. Administrator danych osobowych zastosował takie środki i namysł nad całością zdarzenia pozwala uznać, że z faktu, że zastosowano środki, wynika, że wyeliminowano *prawdopodobieństwo wysokiego ryzyka naruszenia* praw i wolności osoby (osób), której dane dotyczą. W związku z tym **administrator danych osobowych nie informuje**

tej osoby lub tych osób, których dane dotyczą, o tym, że miało miejsce naruszenie ochrony danych osobowych.

– Naruszenie ochrony danych osobowych **powoduje naruszenie** praw lub wolności osób fizycznych.

I jednocześnie:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

lub

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1.

Takie rozwiązanie (w przeciwieństwie do dwóch poprzednich) nie ma sensu. „Nie ma sensu" – rozumiem przez to, że nie ma w takiej sytuacji sensu stosować art. 34 ust. 1 lit. a RODO lub lit. b RODO. Ma miejsce naruszenie ochrony danych osobowych. Ryzyko naruszenia praw i wolności nie tylko może być wysokie, nie tylko jest wysokie, ale ryzyko się zrealizowało i zachodzi naruszenie praw i wolności osób, których dane dotyczą.

– Wcześniej, przed naruszeniem ochrony danych osobowych administrator danych osobowych być może wdrożył środki ochrony, o których mowa w art. 34 ust. 1 lit. a RODO, jednak środki te nie zadziałały, nie udało się uniemożliwić odczytu danych osobowych osobom nieuprawnionym W związku z tym administrator danych osobowych **informuje osoby**, których dane dotyczą, o tym, że miało miejsce naruszenie ochrony danych osobowych.

– Po naruszeniu ochrony danych osobowych administrator danych osobowych zastosował środki, o których mowa w art. 34 ust. 1 lit. b RODO. Administrator danych osobowych zastosował takie środki, jednak naruszenie praw i wolności miało miejsce. Zastosowanie środków nie ma sensu, ponieważ „zło już się stało". W związku z tym administrator danych osobowych **informuje tę osobę lub te osoby**, których dane dotyczą, o tym, że miało miejsce naruszenie ochrony danych osobowych.

3.4. Art. 34 ust. 3 Uwaga 4

Informowanie w interesie osób, których dane dotyczą

Rację ma M. Sakowska-Baryła, która zwraca uwagę na fakt[349], że informowanie osoby, której dane dotyczą o naruszeniu ochrony danych jest instytucją nową. Ze swojej strony dodam, że uważam, iż jest to instytucja doniosła. Instytucja ta – moim zdaniem – koresponduje z obowiązkami, które wynikają z art. 13 i art. 14 RODO. Z przepisów tych wynika obowiązek informowania o fakcie przetwarzania i o szczegółach tego przetwarzania. Naruszenie, prawdziwe, zwłaszcza takie o wysokim poziomie ryzyka dla praw i wolności osób fizycznych jest na tyle istotnym zdarzeniem, że dobrze, by osoba, której dane dotyczą, o zdarzeniu tym wiedziała. Temu właśnie służy omawiany przepis. I właśnie z tej racji, że informowanie o naruszeniu jest ważne już nawet tylko przez pryzmat zasad, należy bardzo ostrożnie i rzekłbym oszczędnie podchodzić do możliwości nieinformowania osób o naruszeniu.

W ten sam nurt wpisuje się wypowiedź C. Burtona, który pisze, że: *The sooner that the individual becomes aware of a breach, the sooner they may undertake the necessary precautions in order to prevent or minimise the damage resulting from it*.[350] Na język polski tłumaczymy to jako: „Im szybciej osoba stanie się świadoma naruszenia, tym szybciej może ona podjąć niezbędne zabezpieczenia, aby zapobiec lub zminimalizować szkodę z nich wynikającą”[351].

3.5. Art. 34 ust. 3 Uwaga 5

Związek z art. 32 RODO

Ciekawa jest wypowiedź C. Burtona, który zwraca uwagę na związek art. 34 RODO nie tylko z art. 33 RODO, który to związek jest oczywisty, ale i na nie tak już oczywisty związek art. 34 RODO z art. 32 RODO[352]. Wskazany autor dostrzega w art. 34 RODO pokrewień-

---

[349] M. Sakowska-Baryła, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 373.

[350] C. Burton, op. cit., s. 655.

[351] Tłum. J. Rz.

[352] C. Burton, op. cit., s. 656.

stwo do art. 32 RODO ustanawiającego obowiązek zapewnienia odpowiednich zabezpieczeń. W uzupełnieniu poglądu C. Burtona należy zwrócić uwagę, że zagrożenia wymienione w art. 32 ust. 2 RODO są tożsame z kolejnymi rodzajami naruszenia ochrony danych z art. 4 pkt. 12 RODO. Można nawet zaryzykować tezę, że administrator, który ocenia ryzyko na podstawie art. 32 ust. 2 RODO, ocenia prawdopodobieństwo zaistnienia zdarzeń, o których mowa w art. 4 pkt 12 RODO, czyli tym samym ocenia prawdopodobieństwo wystąpienia naruszenia ochrony danych osobowych.

3.6. Art. 34 ust. 3 Uwaga 6

Możliwość modyfikacji

obowiązków wynikających z przepisu

Na ciekawy szczegół zwraca uwagę wspomniany wyżej Cedric Burton. Otóż autor ten zwraca uwagę na fakt[353], że z art. 23 RODO wynika, że państwa członkowskie mogą modyfikować obowiązki wynikające z art. 34 RODO. Uwaga ta jest trafna, pozostaje tylko podziękować Temidzie, że fantazja prawodawcy polskiego, który stworzył dwa akty prawne rzekomo wdrażające RODO nie dotknęła art. 34 RODO. Niekompetencja twórców polskich aktów prawnych, które towarzyszą RODO, okazała się tu błogosławieństwem. Nie zauważyli, że mogą zepsuć, więc nie zepsuli. Gorzkie te słowa są zwłaszcza wynikiem lektury Ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[354]. Dziesiątki przepisów, które czy to nakazują administratorom, by ci zobowiązywali osoby, których dotyczą do zachowania tajemnicy, czy to nakazują tym osobom, by zobowiązały się do zachowania danych w tajemnicy, upoważnienia – to wszystko tworzy prawodawczy horror.

---

[353] Ibidem, s. 658.

[354] Dz.U. 2019, poz. 730.

4. Art. 34 ust. 3 Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa

Podsumowując w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa, należy stwierdzić, jak poniżej.

– Art. 34 ust. 3 lit. a RODO uzupełnia **obowiązek**, który nakłada na administratora art. 34 ust. 1 RODO. Artykuł 34 ust. 1 RODO nakłada zatem na administratora obowiązek zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, art. 34 ust. 3 lit. a RODO zaś uzupełnia wskazany obowiązek w sposób opisany poniżej.
  – Administrator nie ma obowiązku zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych w sytuacji, w której naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, jeżeli administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.
– Jednocześnie 34 ust. 3 lit. a RODO ustanawia **uprawnienie**, które przysługuje każdej osobie której dane dotyczą, polegające na tym, że osoba, której dane dotyczą, ma prawo oczekiwać, że administrator poinformuje tę osobę o naruszeniu ochrony danych osobowych w sytuacji, w której naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, jeżeli administrator nie wdrożył odpowiednich technicznych i organizacyjnych środków ochrony i środki te nie zostały zastosowane do danych osobowych, których dotyczy naruszenie; w szczególności mowa tu o środkach, takich jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

– Art. 34 ust. 3 lit. b RODO uzupełnia **obowiązek**, który nakłada na administratora art. 34 ust. 1 RODO. Artykuł 34 ust. 1 RODO nakłada zatem na administratora obowiązek zawiadomienia osoby,

której dane dotyczą o naruszeniu ochrony danych osobowych, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, art. 34 ust. 3 lit. b RODO zaś uzupełnia wskazany obowiązek w sposób opisany poniżej.

  – Administrator nie ma obowiązku zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych w sytuacji, w której naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, jeżeli administrator zastosował następnie, czyli po tym, jak zaistniało naruszenie ochrony danych osobowych, środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1.

– Jednocześnie 34 ust. 3 lit. b RODO ustanawia **uprawnienie**, które przysługuje każdej osobie, której dane dotyczą, polegające na tym, że osoba, której dane dotyczą, ma prawo oczekiwać, że administrator poinformuje tę osobę o naruszeniu ochrony danych osobowych w sytuacji, w której naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, jeżeli administrator nie zastosował następnie, czyli po tym, jak zaistniało naruszenie ochrony danych osobowych, środków eliminujących prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1.
– Art. 34 ust. 3 lit. c RODO uzupełnia **obowiązek**, który nakłada na administratora art. 34 ust. 1 RODO. Artykuł 34 ust. 1 RODO nakłada zatem na administratora obowiązek zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, art. 34 ust. 3 lit. c RODO zaś uzupełnia wskazany obowiązek w sposób opisany poniżej.

  – Administrator nie ma obowiązku zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych w sytuacji, w której naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, jeżeli poinformowanie osoby, której dane dotyczą,

wymagałoby niewspółmiernie dużego wysiłku. Na administratorze spoczywa w takim wypadku obowiązek wydania publicznego komunikatu lub zastosowania podobnego środka, za pomocą którego osoby, których dane dotyczą, zostają poinformowane o naruszeniu w sposób równie skuteczny, jak byłyby poinformowane z wykorzystaniem publicznego komunikatu.

– Jednocześnie 34 ust. 3 lit. c RODO ustanawia **uprawnienie**, które przysługuje każdej osobie, której dane dotyczą, polegające na tym, że osoba, której dane dotyczą, ma prawo oczekiwać, że administrator poinformuje tę osobę o naruszeniu ochrony danych osobowych w sytuacji, w której naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, jeżeli poinformowanie osoby, której dane dotyczą, nie wymagałoby niewspółmiernie dużego wysiłku.

5. Art. 34 ust. 1 Konkretyzacja zasad

Podrozdział poświęcony konkretyzacji zasad znajduje się niżej i jest częścią podrozdziału poświęconego art. 34 ust. 3 RODO. Zastosowałem to przesunięcie, ponieważ uważam rozróżnianie poszczególnych ustępów art. 34 RODO, pod kątem konkretyzacji zasad, za niecelowe i utrudniające ewentualną lekturę.
Art. 34 ust. 1 RODO konkretyzuje wymienione poniżej zasady.

Zasada zgodności z prawem

Związek przepisu z zasadą jest znaczny. Przepis co prawda nie konkretyzuje zasady, bo konkretyzują ją: art. 6 RODO, art. 9 RODO i art. 10 RODO, ale na pewno sprzyja jej realizacji. Sprzyja o tyle, że prowadzi do wykrycia zdarzeń, które mają charakter zagrożenia naruszeniem zasady lub naruszenia zasady. Przetwarzanie w warunkach naruszenia to zwykle, o ile nie zawsze, przetwarzanie, które nie jest objęte żadną z podstaw przetwarzania z art. 6 ust. 1 RODO. Innymi słowy, przepis dotyczy sytuacji, w której zasada zostaje naruszona. W opisanym zjawisku dostrzegam związek przepisu z zasadą.

Przez przetwarzanie w warunkach naruszenia rozumiem przede wszystkim dwie grupy stanów faktycznych. Przede wszystkim możliwy jest stan faktyczny, który polega na tym, że administrator danych osobowych wskutek jakiegoś zdarzenia dopuszcza do przypadkowego lub nieuprawnionego dostępu do danych osobowych przechowywa-

nych przez niego samego. Dostęp jest nieuprawniony, jednak dane zostają udostępnione własnemu pracownikowi. Pozornie nic się nie dzieje, poza tym że dane przetwarza nieuprawniony pracownik. W opisanym stanie faktycznym mamy do czynienia z naruszeniem ochrony danych osobowych i jednocześnie z naruszeniem zasady zgodności z prawem. Druga grupa stanów faktycznych może polegać na zdarzeniach związanych z zapoznawaniem się z danymi osobowymi przez osoby spoza organizacji administratora. Po prostu dane zostają udostępnione osobie nieuprawnionej lub osoba ta sama taki dostęp uzyskuje. Niewątpliwie samo udostępnienie, jak i dalsze przetwarzanie przez osobę, której dane udostępniono lub która ten dostęp sama uzyskała, narusza zasadę zgodności z prawem. Trzecia grupa stanów faktycznych to zdarzenia związane ze zniszczeniem danych, jednak ze zniszczeniem, które nie powinno mieć miejsca, np. z przypadkowym zniszczeniem danych przez administratora, ze zniszczeniem danych przed czasem, kiedy dane powinny zostać zniszczone. W takiej sytuacji mamy również do czynienia z naruszeniem zasady zgodności z prawem. Trudno z pewnością powiedzieć, czy każde naruszenie ochrony danych osobowych narusza zasadę zgodności z prawem, ale na pewno wiele naruszeń owszem. Wydaje się, że zasadę zgodności z prawem naruszają zwłaszcza naruszenia ochrony danych osobowych, które mają charakter zdarzenia, a nie tylko zagrożenia zdarzeniem.

Zasada rzetelności

Przepis służy realizacji zasady rzetelności. Można stwierdzić, że jeżeli, w związku z naruszeniem administrator informuje osobę, której dane dotyczą o tym naruszeniu, to uświadamia jej, że jest administratorem (mogła wcześniej tego nie być świadoma) i że przetwarza dane, które jej dotyczą. Jeżeli administrator uświadamia osobie, której dane dotyczą, że jest administratorem, to tym samym realizuje on zasadę rzetelności. Uprawnione jest – jak się wydaje – twierdzenie, że art. 34 RODO w pewnym względzie konkretyzuje zasadę rzetelności, co pociąga za sobą obowiązek jego realizacji nie tylko dlatego, że jest on w przepisie ustanowiony, ale i dlatego, że realizacja przepisu służy realizacji zasady. To z kolei pociąga za sobą konieczność wykazania realizacji przepisu, by móc wykazać jedną ze składowych realizacji zasady.

Zasada przejrzystości

Przepis służy realizacji również tej zasady. Zasada przejrzystości dotyczy szczegółów przetwarzania danych osobowych. Przypominam treść zasady. *Zasada przejrzystości oznacza obowiązek przetwarzania danych osobowych w taki sposób, że osoba, której dane dotyczą, zna szczegóły przetwarzania dotyczących jej danych, wymienione odpowiednio w art. 13 RODO, art. 14 RODO, art. 15 RODO*.

Przetwarzanie danych osobowych w sposób przejrzysty to przetwarzanie w taki sposób, że osoba, której dane dotyczą, zna szczegóły przetwarzania dotyczących jej danych, wymienione odpowiednio w art. 13 RODO, art. 14 RODO, art. 15 RODO[355].

Poinformowanie osoby, której dane dotyczą o szczegółach przetworzenia danych osobowych, które zaszło w warunkach naruszenia ochrony danych, sprzyja realizacji zasady. Również w odniesieniu do tej zasady można z powodzeniem stwierdzić, że art. 34 RODO konkretyzuje zasadę.

Jeżeli zajdzie przetwarzanie w warunkach naruszenia, to zwykle osoba, której dane dotyczą, nie wie o fakcie tego przetwarzania. Poinformowanie osoby, której dane dotyczą o fakcie przetworzenia (rzetelność), czy nawet tylko o możliwości przetworzenia danych osobowych w warunkach naruszenia, sprzyja realizacji zasady przejrzystości. Trafnie zwraca na to uwagę W. Chomiczewski[356], z którego wypowiedzi widać, że prawdziwie rozumie znaczenie zasady.

Podobne wrażenie odnoszę, czytając wypowiedź M. Sakowskiej-Baryły. Autorka ta, niezwykle pięknie pisze: *[...] obowiązek zawiadamiania osoby, której dane dotyczą o naruszeniu, powinien być uznawany za korespondujący z zasadą przejrzystości przetwarzania*[357]. Koresponduje to z kompetentną wypowiedzią A. Nerki, na temat zasady przejrzystości, w tym samym komentarzu[358]. Niestety, wypowiedź tej samej A. Nerki na temat zasady rzetelności jest dowodem na to, że

---

[355] J. Rzymowski, *RODO – GDPR. Zasady dotyczące*..., s. 195.

[356] W. Chomiczewski, op. cit., s. 719.

[357] M. Sakowska-Baryła, op. cit., s. 374.

[358] A. Nerka, [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 143.

o ile zasada przejrzystości jest dla polskich autorów zrozumiała, o tyle zasada rzetelności – niekoniecznie[359].

Zasada ograniczenia celu

Poinformowanie osoby, której dane dotyczą o naruszeniu ochrony danych, zwłaszcza jeżeli naruszenie to wiązało się z ujawnieniem danych, może mieć pewien wpływ na realizację zasady. Osoba, której dane dotyczą, może zapobiec lub choć próbować zapobiec przetwarzaniu ujawnionych danych osobowych – unieważnić dokumenty, kartę kredytową itp.

Zasada minimalizacji danych

Związek przepisu z zasadą jest podobny jak z zasadą ograniczenia celu. Dane zostają ujawnione, narusza to zasadę minimalizacji, administrator informuje o tym osobę, której dane dotyczą, osoba podejmuje kroki, które mogą do pewnego stopnia zapobiec dalszemu naruszaniu zasady. Podobnie sytuacja kształtuje się w odniesieniu do wymienionych niżej zasad. Należy jednak podkreślić, że związek przepisu z tymi zasadami jest daleki.

Zasada prawidłowości

Zasada ograniczenia przechowywania

Zasada integralności

Zasada poufności

Zasada odpowiedzialności administratora danych (osobowych)

Związek przepisu z zasadą jest dostrzegalny. Administrator jest odpowiedzialny za realizację zasad. Kiedy administrator informuje osobę, której dane dotyczą, że nastąpiło naruszenie ochrony danych osobowych, to może to doprowadzić do poniesienia przez niego odpowiedzialności cywilnej. Samo naruszenie może prowadzić oczywiście do odpowiedzialności administracyjnej.

Zasada rozliczalności

Związek przepisu z rozliczalnością jest taki, że kiedy administrator poinformuje osobę, której dane dotyczą o naruszeniu ochrony danych, to tym samym wytwarza on dowód, że owo naruszenie

[359] Ibidem.

zaistniało, a kiedy zachowuje dowody, że poinformował o naruszeniu, tym samym wytwarza dowód, że zrealizował przepis.

6. Art. 34 ust. 3 Postulaty *de lege ferenda*

6.1. Art. 34 ust. 4 Postulat 1

Uporządkowanie pojęciowe

Artykuł 34 ust. 3 RODO składa się z trzech punktów. Należy zwrócić uwagę na fakt, że każdy z tych punktów odnosi się do sytuacji, w której zachodzi zdarzenie skutkujące lub mogące skutkować wysokim ryzykiem naruszenia praw i wolności osób fizycznych. Co do zasady, wysokie ryzyko naruszenia praw i wolności osób fizycznych, o czym wiemy z artykułu 34 ust. 1 RODO, skutkuje obowiązkiem poinformowania tychże osób o fakcie zaistnienia naruszeń. Artykuł 34 ust. 3 RODO stanowi wyjątek od tego obowiązku, prawodawca bowiem zakłada, że w pewnych sytuacjach, mimo wysokiego poziomu ryzyka naruszenia praw i wolności osób fizycznych, jeżeli zajdą pewne dodatkowe zdarzenia (zajdą, czy też wcześniej mają miejsce), to administrator nie ma obowiązku informować osób, których dane dotyczą o naruszeniu. Jeżeli zajdą te zdarzenia, to uzyskujemy taki stan czy też poziom ryzyka naruszenia praw i wolności osób fizycznych, o jakim mowa jest w artykule 33 ustęp 1 RODO.

W wyniku działań administratora uzyskujemy zatem stan analogiczny do „ryzyka naruszenia praw i wolności osób fizycznych" lub „niskiego ryzyka naruszenia praw i wolności osób fizycznych". Należy jednak zwrócić uwagę, że jeżeli wskutek działania administratora na gruncie artykułu 34 ust. 3 RODO administrator uzyskuje coś na kształt „ryzyka" lub „niskiego ryzyka", to stan ten nie zwalnia go (na gruncie art. 34 RODO) z obowiązku informowania organu nadzorczego. I tu właśnie zwrócić należy uwagę na pewien szczegół. Otóż w artykule 34 ust. 3 RODO mamy do czynienia z trzema punktami oznaczonymi trzema kolejnymi literami a to: „a", „b", „c". W każdym z tych punktów opisany jest pewien stan, którego zaistnienie zwalnia administratora z obowiązku poinformowania osób, których dane dotyczą o fakcie zaistnienia naruszenia ochrony danych osobowych. W przepisach tych dostrzegam jednak pewną niekonsekwencję. W punkcie „a" mowa jest o zdarzeniu, w punkcie „b" mowa jest o zdarzeniu i modyfikacji poziomu ryzyka naruszenia praw i wol-

ności, w punkcie „c” mowa jest o zdarzeniu. Jak więc widać, zachodzi tu pewna niekonsekwencja prawodawcza. Jeśli chodzi o punkt „c”, to tę niekonsekwencję można pozostawić na boku, w gruncie rzeczy na podstawie punktu „c” administrator informuje osoby, których dane dotyczą o zaistnieniu naruszania, tyle tylko że nie dokonując tego w sposób detaliczny, a dokonuje tego niejako hurtowo, w sposób opisany w przepisie, na przykład z wykorzystaniem komunikatu publicznego. Jeśli zatem chodzi o punkt „c”, to można nawet powiedzieć, że tutaj niekonsekwencji prawodawczej nie ma. Jeśli chodzi o punkty „a” i „b”, to niekonsekwencja jest. Wydaje się, że mając to na względzie, należałoby dokonać korekty treści wskazanych przepisów, tak by zarówno w jednym, jak i w drugim treść odnosiła się do poziomu ryzyka naruszenia praw i wolności osób fizycznych.

Tabele pomocnicze

Zestawienia

Zagrożenia uporządkowane na podstawie kryterium konkretnego zagrożenia

Zagrożenia te powinny być brane pod uwagę jako element konieczny oceny ryzyka przetwarzania na gruncie art. 32 ust. 2 RODO. Ocena ta jest elementem oceny ryzyka naruszenia praw i wolności osób fizycznych na gruncie art. 32 ust. 1 RODO. Dalej zagrożenia te uporządkowane są na podstawie kryterium czynności, podczas wykonywania której dane zagrożenie może mieć miejsce i ujęte są w gotową do stosowania tabelę.

Zagrożenia związane ze zniszczeniem danych osobowych

– Przypadkowe zniszczenie danych osobowych przesyłanych.
– Przypadkowe zniszczenie danych osobowych przechowywanych.
– Przypadkowe zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).
– Niezgodne z prawem zniszczenie danych osobowych przesyłanych.
– Niezgodne z prawem zniszczenie danych osobowych przechowywanych.
– Niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).

Zagrożenia związane z utratą danych osobowych

– Przypadkowa utrata danych osobowych przesyłanych.
– Przypadkowa utrata danych osobowych przechowywanych.
– Przypadkowa utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).
– Niezgodna z prawem utrata danych osobowych przesyłanych.
– Niezgodna z prawem utrata danych osobowych przechowywanych.
– Niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).

– Przypadkowa i niezgodna z prawem utrata danych osobowych przesyłanych.
– Przypadkowa i niezgodna z prawem utrata danych osobowych przechowywanych.
– Przypadkowa i niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).

Zagrożenia związane z modyfikacją danych osobowych
– Przypadkowa modyfikacja danych osobowych przesyłanych.
– Przypadkowa modyfikacja danych osobowych przechowywanych.
– Przypadkowa modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).
– Niezgodna z prawem modyfikacja danych osobowych przesyłanych.
– Niezgodna z prawem modyfikacja danych osobowych przechowywanych.
– Niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przesyłanych.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przechowywanych.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).

Zagrożenia związane z ujawnieniem danych osobowych
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Przypadkowe i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.

– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).

Zagrożenia związane z dostępem do danych osobowych

– Przypadkowy i nieuprawniony dostępu do danych osobowych przesyłanych.
– Przypadkowy i nieuprawniony dostęp do danych osobowych przechowywanych.
– Przypadkowy i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych(inaczej niż przez przesyłanie lub przechowywanie).

Ocena ryzyka przez pryzmat oceny wymienionych w art. 32 ust. 2 RODO, zagrożeń dla danych osobowych. Uporządkowane według zagrożeń				
Czynność:	**Prawdopodobieństwo zaistnienia zdarzenia**			
Zagrożenie	Nie może mieć miejsca	Niskie	Średnie	Wysokie
Zagrożenia związane ze zniszczeniem danych osobowych				
– Przypadkowe zniszczenie danych osobowych przesyłanych.				
– Przypadkowe zniszczenie danych osobowych przechowywanych.				
– Przypadkowe zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Niezgodne z prawem zniszczenie danych osobowych przesyłanych.				
– Niezgodne z prawem zniszczenie danych osobowych przechowywanych.				
– Niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych.				
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych.				
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
Zagrożenia związane z utratą danych osobowych				
– Przypadkowa utrata danych osobowych przesyłanych.				
– Przypadkowa utrata danych osobowych przechowywanych.				
– Przypadkowa utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Niezgodna z prawem utrata danych osobowych przesyłanych.				

– Niezgodna z prawem utrata danych osobowych przechowywanych.				
– Niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Przypadkowa i niezgodna z prawem utrata danych osobowych przesyłanych.				
– Przypadkowa i niezgodna z prawem utrata danych osobowych przechowywanych.				
– Przypadkowa i niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
Zagrożenia związane z modyfikacją danych osobowych				
– Przypadkowa modyfikacja danych osobowych przesyłanych.				
– Przypadkowa modyfikacja danych osobowych przechowywanych.				
– Przypadkowa modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Niezgodna z prawem modyfikacja danych osobowych przesyłanych.				
– Niezgodna z prawem modyfikacja danych osobowych przechowywanych.				
– Niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przesyłanych.				
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przechowywanych.				
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
Zagrożenia związane z ujawnieniem danych osobowych				
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych.				
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych.				
– Przypadkowe i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie				

lub przechowywanie).				
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.				
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.				
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
Zagrożenia związane z dostępem do danych osobowych				
– Przypadkowy i nieuprawniony dostępu do danych osobowych przesyłanych.				
– Przypadkowy i nieuprawniony dostęp do danych osobowych przechowywanych.				
– Przypadkowy i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.				
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.				
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych(inaczej niż przez przesyłanie lub przechowywanie).				

Zagrożenia uporządkowane na podstawie kryterium czynności

Zagrożenia te powinny być brane pod uwagę jako element konieczny oceny ryzyka przetwarzania na gruncie art. 32 ust. 2 RODO. Ocena ta jest elementem oceny ryzyka naruszenia praw i wolności osób fizycznych na gruncie art. 32 ust. 1 RODO. Wyżej zagrożenia te uporządkowane są przedmiotowo, na podstawie kryterium zagrożenia.

Zagrożenia dotyczące danych osobowych przesyłanych

– Przypadkowe zniszczenie danych osobowych przesyłanych.
– Niezgodne z prawem zniszczenie danych osobowych przesyłanych.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych.
– Przypadkowa utrata danych osobowych przesyłanych.
– Niezgodna z prawem utrata danych osobowych przesyłanych.
– Przypadkowa i niezgodna z prawem utrata danych osobowych przesyłanych.
– Przypadkowa modyfikacja danych osobowych przesyłanych.
– Niezgodna z prawem modyfikacja danych osobowych przesyłanych.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przesyłanych.
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.
– Przypadkowy i nieuprawniony dostępu do danych osobowych przesyłanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.

Zagrożenia dotyczące danych osobowych przechowywanych

– Przypadkowe zniszczenie danych osobowych przechowywanych.

– Niezgodne z prawem zniszczenie danych osobowych przechowywanych.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych.
– Przypadkowa utrata danych osobowych przechowywanych.
– Niezgodna z prawem utrata danych osobowych przechowywanych.
– Przypadkowa i niezgodna z prawem utrata danych osobowych przechowywanych.
– Przypadkowa modyfikacja danych osobowych przechowywanych.
– Niezgodna z prawem modyfikacja danych osobowych przechowywanych.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przechowywanych.
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.
– Przypadkowy i nieuprawniony dostęp do danych osobowych przechowywanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.

Zagrożenia dotyczące danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie

– Przypadkowe zniszczenie danych osobowych w inny sposób przetwarzanych.
– Niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych.
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych.
– Przypadkowa utrata danych osobowych w inny sposób przetwarzanych.
– Niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych.

– Przypadkowa i niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych.
– Przypadkowa modyfikacja danych osobowych w inny sposób przetwarzanych.
– Niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych.
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych.
– Przypadkowe i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.
– Przypadkowy i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.

Uwaga, dane *w inny sposób przetwarzane*, to dane osobowe przetwarzane w sposób inny niż przez przesyłanie i przechowywanie.

Ocena ryzyka przez pryzmat oceny wymienionych w art. 32 ust. 2 RODO, zagrożeń dla danych osobowych. Uporządkowane według czynności na danych osobowych				
Czynność	**Prawdopodobieństwo zaistnienia zdarzenia**			
Zagrożenie	Nie może mieć miejsca	Niskie	Średnie	Wysokie
Zagrożenia dotyczące danych osobowych przesyłanych				
– Przypadkowe zniszczenie danych osobowych przesyłanych.				
– Niezgodne z prawem zniszczenie danych osobowych przesyłanych.				
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych.				
– Przypadkowa utrata danych osobowych przesyłanych.				
– Niezgodna z prawem utrata danych osobowych przesyłanych.				
– Przypadkowa i niezgodna z prawem utrata danych osobowych przesyłanych.				
– Przypadkowa modyfikacja danych osobowych przesyłanych.				
– Niezgodna z prawem modyfikacja danych osobowych przesyłanych.				
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przesyłanych.				
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych.				
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.				
– Przypadkowy i nieuprawniony dostępu do danych osobowych przesyłanych.				
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.				

Zagrożenia dotyczące danych osobowych przechowywanych				
– Przypadkowe zniszczenie danych osobowych przechowywanych.				
– Niezgodne z prawem zniszczenie danych osobowych przechowywanych.				
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych.				
– Przypadkowa utrata danych osobowych przechowywanych.				
– Niezgodna z prawem utrata danych osobowych przechowywanych.				
– Przypadkowa i niezgodna z prawem utrata danych osobowych przechowywanych.				
– Przypadkowa modyfikacja danych osobowych przechowywanych.				
– Niezgodna z prawem modyfikacja danych osobowych przechowywanych.				
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przechowywanych.				
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych.				
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.				
– Przypadkowy i nieuprawniony dostęp do danych osobowych przechowywanych.				
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.				
Zagrożenia dotyczące danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie				
– Przypadkowe zniszczenie danych osobowych w inny sposób przetwarzanych.				
– Niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych.				
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych.				
– Przypadkowa utrata danych osobowych w inny sposób				

przetwarzanych.				
– Niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych.				
– Przypadkowa i niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych.				
– Przypadkowa modyfikacja danych osobowych w inny sposób przetwarzanych.				
– Niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych.				
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych.				
– Przypadkowe i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.				
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych.				
– Przypadkowy i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.				
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych.				

Prawa i wolności zasadnicze

Prawa i wolności zasadnicze, które należy wziąć pod uwagę przy dokonywaniu oceny ryzyka naruszenia praw i wolności osób fizycznych, na gruncie art. 32 RODO i na gruncie art. 24 RODO.

W takim przypadku należy ocenić prawdopodobieństwo zagrożenia i wagę zagrożenia. Należy mieć świadomość, że ocena prawdopodobieństwa zagrożenia jest niczym innym jak przewidywaniem przyszłości, a tę przewidywać niełatwo.

Uważam, że prawdziwie uczciwa ocena prawdopodobieństwa zagrożenia powinna się ograniczyć do ustalenia, czy zaistnienie danego zagrożenia jest prawdopodobne czy nie. Wszelkie stopniowanie prawdopodobieństwa budzi mój niepokój co do rzetelności tegoż stopniowania. Dlaczego tak uważam? Otóż, jeżeli oceniamy, czy zagrożenie jest prawdopodobne, to oceniamy stan obecny, oceniamy „jak jest", to „jak jest", możemy ustalić. Przyszłość, stan przyszły, „jak będzie" jest, jak stwierdziłem przewidywaniem przyszłości.

Jeśli chodzi o wagę zagrożenia, to RODO nie zawiera racjonalnych wskazówek dotyczących oceniania tej wagi. Motyw 75 Preambuły RODO wymienia w sposób raczej kazuistyczny sfery, w których mogą zaistnieć następstwa naruszenia praw i wolności, jednak ocena przez pryzmat wskazanych okoliczności, o ile racjonalna, o tyle grozi oceniającemu, że wpadnie on w pewną pułapkę. Może się zdarzyć, że naruszenie praw i wolności nie zachodzi w sferach wskazanych w motywie 75 Preambuły RODO, a i tak jest doniosłe. Jeżeli więc administrator uzna, że zjawiska wymienione we wskazanym motywie są wymienione w sposób wyczerpujący, to ocena wagi może się okazać błędna. Z ostrożności można więc przyjąć, że waga zachodzi, że jest stała i oceniać raczej prawdopodobieństwo niż wagę.

Zwracam jednocześnie uwagę, że podejście, które tu prezentuję, jest podejściem jednym z co najmniej dwóch możliwych. W podejściu tym najpierw ocenia się prawdopodobieństwo zaistnienia zdarzeń, które wymienione są w art. 32 ust. 2 RODO i następnie ocenia się ryzyko naruszenia praw i wolności osób fizycznych.

– Prawdopodobieństwo zaistnienia zdarzeń, które wymienione są w art. 32 ust. 2 RODO, można ocenić z wykorzystaniem tabeli, która znajduje się poniżej, pod tabelą praw i wolności zasadniczych. Jest to tabela „Prawdopodobieństwo zaistnienia zagrożeń z art. 32 ust. 2 RODO".

– Ryzyko naruszenia praw i wolności osób fizycznych można ocenić z wykorzystaniem tabeli znajdującej się poniżej. Jest to tabela: „Ryzyko naruszenia praw i wolności zasadniczych (zapisanych w art. 5 ust. 1 RODO)".

Możliwe jest też inne podejście. Piszę o nim w uwagach (*3.30. Art. 24. Uwaga 30. Ryzyko. Pojęcie na gruncie art. 32. Stałość zależności*) i (*3.31. Art. 24. Uwaga 31. Zdarzenie a naruszenie prawa – zasady*).

W podejściu tym oceniamy prawdopodobieństwo zaistnienia zdarzenia, a wagą jego zaistnienia jest naruszenie, lub ryzyko naruszenia zasady związanej z tym zdarzeniem.

Sporządzenie czytelnych tabel możliwych do zastosowania w kontekście tego właśnie podejścia nie jest proste, wydaje mi się jednak, że znalazłem do tego klucz. Tabelę prezentuję dalej pod tytułem: „Ryzyko naruszenia praw i wolności związane z zaistnieniem zagrożenia wobec konkretnej czynności z art. 32 ust. 2 RODO". Tabela oparta jest na podobnym pomyśle jak ten, na którym oparta jest tabela M. Gumularza i T. Izydorczyka, z tym jednak zastrzeżeniem, że ja z zasadami zestawiam zagrożenia z art. 32 ust. 2 RODO, wskazani zaś autorzy z zasadami zestawiają coś, co nazywają „przykładowymi procesami przetwarzania[360]. Zaznaczam, że wskazane tu zależności między zaistnieniem zagrożeń związanych z konkretną czynnością na danych a naruszeniem zasad z art. 5 RODO mają na razie raczej charakter propozycji niż ostatecznych wyników i ustaleń. Koncepcję stałych zależności w RODO rozwijam w kolejnej, przygotowywanej właśnie, monografii.

[360] M. Gumularz, T. Izydorczyk, op. cit., s. 80–81.

Ryzyko naruszenia praw i wolności zasadniczych (zapisanych w art. 5 ust. 1 RODO)		
Przepis **Prawo** **Wolność**	**prawdopodo-bieństwo**	**waga**
Artykuł 5 ust. 1 lit. a RODO. – **Prawo do** przetwarzania danych osobowych **w sposób zgodny z prawem**, przysługujące osobie, której dane dotyczą. – **Wolność od** przetwarzania danych osobowych **w sposób niezgodny z prawem**.		
Artykuł 5 ust. 1 lit. a RODO. – **Prawo do** przetwarzania danych osobowych **w sposób rzetelny**, przysługujące osobie, której dane dotyczą. – **Wolność od** przetwarzania danych osobowych **w sposób nierzetelny.**		
Artykuł 5 ust. 1 lit. a RODO. – **Prawo do** przetwarzania danych osobowych **w sposób przejrzysty**, przysługujące osobie, której dane dotyczą. – **Wolność od** przetwarzania danych osobowych **w sposób nieprzejrzysty**.		
Artykuł 5 ust. 1 lit. b RODO. – **Prawo do** przetwarzania danych osobowych **w sposób ograniczony co do celu**, przysługujące osobie, której dane dotyczą. – **Wolność od** przetwarzania danych osobowych **w sposób nieograniczony co do celu**.		
Artykuł 5 ust. 1 lit. c RODO. – **Prawo do** przetwarzania danych osobowych **w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania**, przysługujące osobie, której dane dotyczą. – **Wolność od** przetwarzania danych osobowych **w sposób nieograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania**.		

Artykuł 5 ust. 1 lit. d RODO. – **Prawo do** przetwarzania danych osobowych **w sposób prawidłowy**, przysługujące osobie, której dane dotyczą. – **Wolność od** przetwarzania danych osobowych **w sposób nieprawidłowy**.		
Artykuł 5 ust. 1 lit. e RODO. – **Prawo do** przetwarzania danych osobowych **w sposób ograniczony co do przechowywania**, przysługujące osobie, której dane dotyczą. – **Wolność od** przetwarzania danych osobowych **w sposób nieintegralny**.		
Artykuł 5 ust. 1 lit. f RODO. – **Prawo do** przetwarzania danych osobowych **w sposób integralny,** przysługujące osobie, której dane dotyczą. – **Wolność od** przetwarzania danych osobowych **w sposób nieintegralny**.		
Artykuł 5 ust. 1 lit. f RODO. – **Prawo do** przetwarzania danych osobowych **w sposób poufny**, przysługujące osobie, której dane dotyczą. – **Wolność od** przetwarzania danych osobowych **w sposób niepoufny – jawny**.		

Prawdopodobieństwo zaistnienia zagrożeń z art. 32 ust. 2 RODO				
Czynność:	**Prawdopodobieństwo zaistnienia zdarzenia**			
Zagrożenie	Zdarzenie nie może mieć miejsca	Niskie	Średnie	Wysokie
Zagrożenia związane ze zniszczeniem danych osobowych				
– Przypadkowe zniszczenie danych osobowych przesyłanych.				
– Przypadkowe zniszczenie danych osobowych przechowywanych.				
– Przypadkowe zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Niezgodne z prawem zniszczenie danych osobowych przesyłanych.				
– Niezgodne z prawem zniszczenie danych osobowych przechowywanich.				
– Niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych.				
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych.				
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
Zagrożenia związane z utratą danych osobowych				
– Przypadkowa utrata danych osobowych				

przesyłanych.				
– Przypadkowa utrata danych osobowych przechowywanych.				
– Przypadkowa utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Niezgodna z prawem utrata danych osobowych przesyłanych.				
– Niezgodna z prawem utrata danych osobowych przechowywanych.				
– Niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Przypadkowa i niezgodna z prawem utrata danych osobowych przesyłanych.				
– Przypadkowa i niezgodna z prawem utrata danych osobowych przechowywanych.				
– Przypadkowa i niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
Zagrożenia związane z modyfikacją danych osobowych				
– Przypadkowa modyfikacja danych osobowych przesyłanych.				
– Przypadkowa modyfikacja danych osobowych przechowywanych.				
– Przypadkowa modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Niezgodna z prawem modyfikacja danych osobowych przesyłanych.				
– Niezgodna z prawem modyfikacja danych osobowych przechowywanych.				
– Niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przesyłanych.				

– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przechowywanych.				
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
Zagrożenia związane z ujawnieniem danych osobowych				
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych.				
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych.				
– Przypadkowe i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.				
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.				
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych.				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych.				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
Zagrożenia związane z dostępem do danych osobowych				
– Przypadkowy i nieuprawniony dostępu do danych osobowych przesyłanych.				
– Przypadkowy i nieuprawniony dostęp do danych				

osobowych przechowywanych.				
– Przypadkowy i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.				
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.				
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie).				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych.				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych(inaczej niż przez przesyłanie lub przechowywanie)				

Ryzyko naruszenia praw i wolności związane z zaistnieniem zagrożenia wobec konkretnej czynności z art. 32 ust. 2 RODO													
Czynność:										**Prawdopodobieństwo zaistnienia zdarzenia**			
Zagrożenie	Zgodność z prawem	Rzetelność	Przejrzystość	Ograniczenie celu	Minimalizacja	Prawidłowość	Ograniczenie przechow.	Integralność	Poufność	Nie może mieć miejsca	Niskie	Średnie	Wysokie
Zagrożenia dotyczące danych osobowych przesyłanych													
– Przypadkowe zniszczenie	+	–	–	+	+	+	+	+	–				
– Niezgodne z prawem zniszczenie	+	–	–	+	+	+	+	+	–				
– Przypadkowe i niezgodne z prawem zniszczenie	+	–	–	+	+	+	+	+	–				
– Przypadkowa utrata	+	+/–	+/	+/–	+	+	+	–	+				
– Niezgodna z prawem utrata	+	+/–	+/–	+/–	+	+	+	–	+				
– Przypadkowa i niezgodna z prawem utrata	+	+/–	+/–	+/–	+	+	+	–	+				
– Przypadkowa modyfikacja	+	–	–	+/–	+	+	+/–	+	–				
– Niezgodna z prawem modyfikacja	+	–	–	+/–	+	+	+/–	+	–				
– Przypadkowa i niezgodna z prawem modyfikacja	+	–	–	+/–	+	+	+/–	+	–				
– Przypadkowe i nieuprawnione ujawnienie	+	+/–	+/–	+	+	–	+	–	+				
– Niezgodne z prawem i nieuprawnione ujawnienie	+	+/–	+/–	+	+	–	+	–	+				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie	+	+/–	+/–	+	+	–	+	–	+				
– Przypadkowy i nieuprawniony dostęp	+	+/–	+/–	+	+	+/–	+/–	+/–	+				
– Niezgodny z prawem i nieuprawniony dostęp	+	+/–	+/–	+	+	+/–	+/–	+/–	+				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp	+	+/–	+/–	+	+	+/–	+/–	+/–	+				

Ryzyko naruszenia praw i wolności związane z zaistnieniem zagrożenia wobec konkretnej czynności z art. 32 ust. 2 RODO c.d.													
Czynność:										**Prawdopodobieństwo zaistnienia zdarzenia**			
	Zgodność z prawem	Rzetelność	Przejrzystość	Ograniczenie celu	Minimalizacja	Prawidłowość	Ograniczenie przechow.	Integralność	Poufność	Nie może mieć miejsca	Niskie	Średnie	Wysokie
Zagrożenia dotyczące danych osobowych przechowywanych													
– Przypadkowe zniszczenie	+	–	–	+	+	+	+	+	–				
– Niezgodne z prawem zniszczenie	+	–	–	+	+	+	+	+	–				
– Przypadkowe i niezgodne z prawem zniszczenie	+	–	–	+	+	+	+	+	–				
– Przypadkowa utrata	+	+/–	–	+	+	+	+	+	+				
– Niezgodna z prawem utrata	+	+/–	–	+	+	+	+	+	+				
– Przypadkowa i niezgodna z prawem utrata	+	+/–	–	+	+	+	+	+	+				
– Przypadkowa modyfikacja	+	–	–	+	+	+	+	+	–				
– Niezgodna z prawem modyfikacja	+	–	–	+	+	+	+	+	–				
– Przypadkowa i niezgodna z prawem modyfikacja	+	–	–	+	+	+	+	+	–				
– Przypadkowe i nieuprawnione ujawnienie	+	+/–	+/–	+	+	–	+	–	+				
– Niezgodne z prawem i nieuprawnione ujawnienie	+	+/–	+/–	+	+	–	+	–	+				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie	+	+/–	+/–	+	+	–	+	–	+				
– Przypadkowy i nieuprawniony dostęp	+	+/–	+/–	+	+	+/–	+/–	+/–	+				
– Niezgodny z prawem i nieuprawniony dostęp do	+	+/	+/–	+	+	+/–	+/–	+/–	+				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp	+	+/–	+/–	+	+	+/–	+/–	+/–	+				

Ryzyko naruszenia praw i wolności związane z zaistnieniem zagrożenia wobec konkretnej czynności z art. 32 ust. 2 RODO c.d.													
Czynność:										**Prawdopodobieństwo zaistnienia zdarzenia**			
	Zgodność z prawem	Rzetelność	Przejrzystość	Ograniczenie celu	Minimalizacja	Prawidłowość	Ograniczenie przechow.	Integralność	Poufność	Nie może mieć miejsca	Niskie	Średnie	Wysokie
Zagrożenia dotyczące danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie													
– Przypadkowe zniszczenie danych	+	–	–	+	+	+	+	+	–				
– Niezgodne z prawem zniszczenie	+	–	–	+	+	+	+	+	–				
– Przypadkowe i niezgodne z prawem zniszczenie	+	–	–	+	+	+	+	+	–				
– Przypadkowa utrata	+	+/–	+/–	+	+	+	+	+	+				
– Niezgodna z prawem utrata	+	+/–	+/–	+	+	+	+	+	+				
– Przypadkowa i niezgodna z prawem utrata	+	+/–	+/–	+	+	+	+	+	+				
– Przypadkowa modyfikacja	+	–	–	+	+	+	+	+	–				
– Niezgodna z prawem modyfikacja	+	–	–	+	+	+	+	+	–				
– Przypadkowa i niezgodna z prawem modyfikacja	+	–	–	+	+	+	+	+	–				
– Przypadkowe i nieuprawnione ujawnienie	+	+/–	+/–	+	+	+/–	+/–	+	+				
– Niezgodne z prawem i nieuprawnione ujawnienie	+	+/–	+/–	+	+	+/–	+/–	+	+				
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie	+	+/–	+/–	+	+	+/–	+/–	+	+				
– Przypadkowy i nieuprawniony dostęp	+	+/–	+/–	+	+	+/–	+/–	+/–	+				
– Niezgodny z prawem i nieuprawniony dostęp	+	+/–	+/–	+	+	+/–	+/–	+/–	+				
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp	+	+/–	+/–	+	+	+/–	+/–	+/–	+				

Te same prawa i wolności należy brać pod uwagę przy ocenie ryzyka naruszenia praw lub wolności osób fizycznych i przy ocenie naruszenia praw i wolności osób fizycznych, na gruncie art. 33 RODO i art. 34 RODO.

W takim przypadku należy ocenić ryzyko naruszenia praw i wolności. Ocena dokonywana na gruncie art. 33 RODO i art. 34 RODO jest łatwiejsza od oceny dokonywanej na gruncie art. 24 RODO i art. 32 RODO, ponieważ jest ona dokonywana po zaistnieniu zdarzenia. Administrator danych osobowych, na gruncie art. 33 i 34 RODO, ocenia, co się stało, ewentualnie co się mogło stać (co jest jedynie innym językowym ujęciem zdarzeń), ale nie musi, jak to ma miejsce na gruncie art. 24 i 32 RODO, przewidywać przyszłości.

W motywie 76 Preambuły RODO czytamy między innymi, że: *Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko*. Wydaje się, że Preambuła nie jest spójna z art. 33 i 34 RODO, ponieważ analiza tych przepisów wskazuje, że poziomów ryzyka naruszenia praw i wolności jest znacznie więcej. Szeroko opisuję to w treści książki w (*3.8. Art. 34 ust. 1 Uwaga 8. Zawiadamianie osób, zgłaszanie PUODO. Uwagi porządkujące*), tu jedynie dla porządku je wymieniam. Ryzyko na gruncie art. 33 RODO i 34 RODO kształtuje się zatem w sposób wskazany poniżej.

– Ryzyko zrealizowane (Naruszenie praw i wolności osób fizycznych)
– Poziom ryzyka wysoki (Wysokie ryzyko naruszenia praw i wolności osób fizycznych)
– Poziom ryzyka wysoki z zastrzeżeniami
– Poziom ryzyka średni (podstawowy, niższy od wysokiego, wyższy od niskiego)
– Poziom ryzyka niski
– Brak ryzyka naruszenia praw i wolności osób fizycznych

W sytuacji zaistnienia zdarzenia, co do którego administrator danych osobowych ma podejrzenie, że zdarzenie mogło być naruszeniem ochrony danych osobowych, o którym mowa w art. 4 pkt. 12 RODO, w art. 33 ust. 1 RODO i 34 ust. 1 RODO, administrator danych oso-

bowych powinien wykonać kilka czynności, czynności te może on wykonać wykorzystując zaproponowane niżej w książce tabele.

– Najpierw należy ustalić, czy zdarzenie o charakterze naruszenia ochrony danych osobowych miało miejsce. Można to zrobić posługując się tabelą: „Pytania umożliwiające ustalenie, czy miało miejsce naruszenie ochrony danych osobowych” [361]. Dla sprawdzenia ustaleń poczynionych z użyciem tabeli można ustalić, czy zdarzenie o charakterze naruszenia ochrony danych osobowych jest jednym ze zdarzeń wymienionych w wyliczeniu: „Zdarzenia, których zaistnienie oznacza, że miało miejsce naruszenie ochrony danych osobowych”.
– Po ustaleniu, czy miało lub mogło mieć miejsce naruszenie ochrony danych, warto ustalić, w jakim stopniu prawdopodobne było zaistnienie tego naruszenia. Można to zrobić, używając tabeli: „Prawdopodobieństwo zaistnienia zdarzenia o charakterze naruszenia ochrony danych osobowych”. W tabeli tej wskazałem na stałe związki, które zachodzą między zdarzeniami wskazanymi w art. 4 pkt 12 RODO a prawami i wolnościami wskazanymi w art. 5 RODO. Wskazanie to oparte jest na zjawisku stałości związków między przepisami. Zjawisko to uważam za ważne i mogące być bardzo przydatnym dla praktyki, tym bardziej uczulam na fakt, że pomysł jest nowy i że związki między konkretnymi zdarzeniami z art. 4 pkt 12 RODO a zasadami z art. 5 RODO powinny zostać przemyślane, choćby przed zastosowaniem w praktyce tabeli, którą proponuję.
– W sytuacji naruszenia ochrony danych osobowych należy zatem ocenić, który ze wskazanych powyżej poziomów przyjmuje ryzyko naruszenia kolejnych praw i wolności. Można to zrobić posługując się tabelą „Ryzyko naruszenia praw i wolności”.

[361] Obecny układ graficzny tabeli jest wypadkową pierwotnego jej układu graficznego i sugestii w kwestii tego układu, którą uprzejmie skierował do mnie kolega z jednej z grup fejsbukowych, w których dyskutujemy nad RODO, pan magister Przemysław Milbauer, któremu z tego miejsca pięknie dziękuję.

Pytania umożliwiające ustalenie, czy miało miejsce naruszenie ochrony danych osobowych Pytania dzielą się na trzy grupy. Naruszenie zaszło, jeżeli co najmniej jedna odpowiedź z każdej z grup jest pozytywna.			
	Pytania pierwszej grupy	**tak**	**nie**
Czy zdarzenie miało charakter	przypadkowy		
	niezgodny z prawem		

	Pytania drugiej grupy		
Czy zdarzenie polegało na	zniszczeniu danych osobowych		
	utraceniu danych osobowych		
	zmodyfikowaniu danych osobowych		
	nieuprawnionym ujawnieniu danych osobowych		
	nieuprawnionym dostępie do danych osobowych		
Czy zdarzenie zagrażało (prowadziło do)	zniszczeniem danych osobowych		
	utraceniem danych osobowych		
	zmodyfikowaniem danych osobowych		
	nieuprawnionym ujawnieniem danych osobowych		
	nieuprawnionym dostępem do danych osobowych		

	Pytania trzeciej grupy		
Czy zdarzenie dotyczyło danych osobowych	przesyłanych		
	przechowywanych		
	przetwarzanych inaczej niż przez przesyłanie lub przechowywanie		

Zdarzenia, których zaistnienie oznacza, że miało miejsce naruszenie ochrony danych osobowych

1. Przypadkowe zniszczenie danych osobowych przesyłanych. (Raczej przesyłanych przez administratora lub podmiot przetwarzający, nie do administratora lub podmiotu przetwarzającego, nie jest to jednak pewne.)
2. Zagrożenie przypadkowym zniszczeniem danych osobowych przesyłanych (Raczej przesyłanych przez administratora lub podmiot przetwarzający, nie do administratora lub podmiotu przetwarzającego, nie jest to jednak pewne.)
3. Przypadkowe zniszczenie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
4. Zagrożenie przypadkowym zniszczeniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
5. Przypadkowe zniszczenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
6. Zagrożenie przypadkowym zniszczeniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
7. Przypadkowe utracenie danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
8. Zagrożenie przypadkowym utraceniem danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
9. Przypadkowe utracenie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
10. Zagrożenie przypadkowym utraceniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
11. Przypadkowe utracenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
12. Zagrożenie przypadkowym utraceniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.

13. Przypadkowe zmodyfikowanie danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
14. Zagrożenie przypadkowym zmodyfikowaniem danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
15. Przypadkowe zmodyfikowanie danych osobowych, które są przechowywane przez administratora lub podmiot przetwarzający.
16. Zagrożenie. przypadkowym zmodyfikowaniem danych osobowych przechowywanych przez administratora lub podmiot przetwarzający.
17. Przypadkowe zmodyfikowanie danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający w sposób inny niż przesyłanie lub przechowywanie.
18. Zagrożenie przypadkowym zmodyfikowaniem danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
19. Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych. Przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
20. Zagrożenie przypadkowym i nieuprawnionym ujawnieniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
21. Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
22. Zagrożenie przypadkowym i nieuprawnionym ujawnieniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
23. Przypadkowe i nieuprawnione ujawnienie danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
24. Zagrożenie Przypadkowym i nieuprawnionym ujawnieniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
25. Przypadkowy i nieuprawniony dostęp do danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.

26. Zagrożenie przypadkowym i nieuprawnionym dostępem do danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
27. Przypadkowy i nieuprawniony dostęp do danych osobowych danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
28. Zagrożenie przypadkowym i nieuprawnionym dostępem do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
29. Przypadkowy i nieuprawniony dostęp do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie, czyli które są w jakikolwiek sposób (z uwzględnieniem zawartego w przepisie wyłączenia) przetwarzane.
30. Zagrożenie przypadkowym i nieuprawnionym dostępem do danych osobowych przetwarzanych w sposób inny niż przez przesyłanie lub przechowywanie przez administratora lub przez podmiot przetwarzający
31. Niezgodne z prawem zniszczenie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający. Naruszenie może mieć miejsce zwłaszcza podczas samego transferu danych osobowych między administratorem (podmiotem przetwarzającym) – nadawcą a adresatem.
32. Zagrożenie niezgodnym z prawem zniszczeniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
33. Niezgodne z prawem zniszczenie danych osobowych, przechowywanych przez administratora lub przez podmiot przetwarzający.
34. Zagrożenie niezgodnym z prawem zniszczeniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
35. Niezgodne z prawem zniszczenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.

36. Zagrożenie niezgodnym z prawem zniszczeniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
37. Niezgodne z prawem utracenie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający. Utracenie należy utożsamiać z zagubieniem, wydaje się, że z zagubieniem podczas transferu, transportu, przesyłania.
38. Zagrożenie niezgodnym z prawem utraceniem danych osobowych przesyłanych do administratora od administratora, przez administratora do podmiotu przetwarzającego, od podmiotu przetwarzającego przez podmiot przetwarzający.
39. Niezgodne z prawem utracenie danych osobowych przechowywanych przez administratora, czyli ich zagubienie przez administratora lub przez podmiot przetwarzający podczas ich przechowywania.
40. Zagrożenie niezgodnym z prawem utraceniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający, czyli ich zagubieniem podczas ich przechowywania.
41. Niezgodne z prawem utracenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie, czyli ich zagubienie podczas wykonywania czynności innych niż przesyłanie lub przechowywanie.
42. Zagrożenie niezgodnym z prawem utraceniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie, czyli ich zagubienie podczas wykonywania czynności innych niż przesyłanie lub przechowywanie.
43. Niezgodne z prawem zmodyfikowanie danych osobowych przesyłanych. Przesyłanych od administratora, przesyłanych do administratora, przesyłanych przez administratora, przesyłanych od podmiotu przetwarzającego, przesyłanych do podmiotu przetwarzającego, przesyłanych przez podmiot przetwarzający.
44. Zagrożenie niezgodnym z prawem zmodyfikowaniem danych osobowych przesyłanych. Przesyłanych od administratora, przesyłanych do administratora, przesyłanych przez administratora, prze-

syłanych od podmiotu przetwarzającego, przesyłanych do podmiotu przetwarzającego, przesyłanych przez podmiot przetwarzający.

45. Niezgodne z prawem zmodyfikowanie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający. Zmodyfikowanie bez upoważnienia lub polecenia, czyli ze złamaniem zasady integralności.
46. Zagrożenie niezgodnym z prawem zmodyfikowaniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający. Zmodyfikowaniem bez upoważnienia lub polecenia, czyli ze złamaniem zasady integralności.
47. Niezgodne z prawem zmodyfikowanie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
48. Zagrożenie niezgodnym z prawem zmodyfikowaniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
49. Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych. Przesyłanych od administratora, przesyłanych do administratora, przesyłanych przez administratora, przesyłanych od podmiotu przetwarzającego, przesyłanych do podmiotu przetwarzającego, przesyłanych przez podmiot przetwarzający.
50. Zagrożenie niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przesyłanych. Przesyłanych od administratora, przesyłanych do administratora, przesyłanych przez administratora, przesyłanych od podmiotu przetwarzającego, przesyłanych do podmiotu przetwarzającego, przesyłanych przez podmiot przetwarzający.
51. Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający. Jest to ujawnienie z naruszeniem zasady zgodności z prawem i zasady poufności, ujawnienie, nad którym nie sprawuje kontroli administrator ani podmiot przetwarzający.
52. Zagrożenie niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
53. Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przetwarzanych przez administratora lub przez podmiot prze-

twarzający w sposób inny niż przez przesyłanie lub przechowywanie.

54. Zagrożenie niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
55. Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
56. Zagrożenie niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
57. Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
58. Zagrożenie niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
59. Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
60. Zagrożenie niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
61. Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
62. Zagrożenie przypadkowym i niezgodnym z prawem zniszczeniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
63. Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.

64. Zagrożenie przypadkowym i niezgodnym z prawem zniszczeniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
65. Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
66. Zagrożenie przypadkowym i niezgodnym z prawem zniszczeniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
67. Przypadkowe i niezgodne z prawem utracenie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
68. Zagrożenie przypadkowym i niezgodnym z prawem utraceniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
69. Przypadkowe i niezgodne z prawem utracenie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
70. Zagrożenie przypadkowym i niezgodnym z prawem utraceniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
71. Przypadkowe i niezgodne z prawem utracenie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
72. Zagrożenie przypadkowym i niezgodnym z prawem utraceniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
73. Przypadkowe lub niezgodne z prawem zmodyfikowanie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
74. Zagrożenie przypadkowym lub niezgodnym z prawem zmodyfikowaniem danych osobowych przesyłanych do administratora, od ad-

ministratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.

75. Przypadkowe lub niezgodne z prawem zmodyfikowanie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
76. Zagrożenie przypadkowym lub niezgodnym z prawem zmodyfikowaniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
77. Przypadkowe i niezgodne z prawem zmodyfikowanie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
78. Zagrożenie przypadkowym i niezgodnym z prawem zmodyfikowaniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
79. Przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
80. Zagrożenie przypadkowym lub niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przesyłanych do administratora, od administratora, przez administratora, do podmiotu przetwarzającego, od podmiotu przetwarzającego, przez podmiot przetwarzający.
81. Przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
82. Zagrożenie przypadkowym lub niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
83. Przypadkowe lub niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.
84. Zagrożenie przypadkowym lub niezgodnym z prawem i nieuprawnionym ujawnieniem danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przez przesyłanie lub przechowywanie.

85. Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych.
86. Zagrożenie i niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przesyłanych przez administratora lub przez podmiot przetwarzający.
87. Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
88. Zagrożenie przypadkowym i niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przechowywanych przez administratora lub przez podmiot przetwarzający.
89. Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przesyłanie lub przechowywanie.
90. Zagrożenie przypadkowym i niezgodnym z prawem i nieuprawnionym dostępem do danych osobowych przetwarzanych przez administratora lub przez podmiot przetwarzający w sposób inny niż przesyłanie lub przechowywanie.

Prawdopodobieństwo zaistnienia zdarzenia o charakterze naruszenia ochrony danych osobowych					
Naruszenie:	**Prawdopodobieństwo**				
Zagrożenie	Zdarzenie nie mogło mieć miejsca	Niskie	Średnie	Wysokie	Zdarzenie miało miejsce
Zagrożenia związane ze zniszczeniem danych osobowych.					
– Przypadkowe zniszczenie danych osobowych przesyłanych					
– Przypadkowe zniszczenie danych osobowych przechowywanych					
– Przypadkowe zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
– Niezgodne z prawem zniszczenie danych osobowych przesyłanych.					
– Niezgodne z prawem zniszczenie danych osobowych przechowywanych					
– Niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przesyłanych					
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych przechowywanych					
– Przypadkowe i niezgodne z prawem zniszczenie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
Zagrożenia związane z utratą danych osobowych					
– Przypadkowa utrata danych osobowych przesyłanych					
– Przypadkowa utrata danych osobowych przechowywanych					
– Przypadkowa utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
– Niezgodna z prawem utrata danych osobowych przesyłanych					
– Niezgodna z prawem utrata danych osobowych przechowywanych					

– Niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
– Przypadkowa i niezgodna z prawem utrata danych osobowych przesyłanych					
– Przypadkowa i niezgodna z prawem utrata danych osobowych przechowywanych					
– Przypadkowa i niezgodna z prawem utrata danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
Zagrożenia związane z modyfikacją danych osobowych					
– Przypadkowa modyfikacja danych osobowych przesyłanych					
– Przypadkowa modyfikacja danych osobowych przechowywanych					
– Przypadkowa modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
– Niezgodna z prawem modyfikacja danych osobowych przesyłanych					
– Niezgodna z prawem modyfikacja danych osobowych przechowywanych					
– Niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przesyłanych					
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych przechowywanych					
– Przypadkowa i niezgodna z prawem modyfikacja danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
Zagrożenia związane z ujawnieniem danych osobowych					
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przesyłanych					
– Przypadkowe i nieuprawnione ujawnienie danych osobowych przechowywanych					
– Przypadkowe i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych					
– Niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych					
– Niezgodne z prawem i nieuprawnione ujawnienie danych					

osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przesyłanych					
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych przechowywanych					
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
Zagrożenia związane z dostępem do danych osobowych					
– Przypadkowy i nieuprawniony dostępu do danych osobowych przesyłanych					
– Przypadkowy i nieuprawniony dostęp do danych osobowych przechowywanych					
– Przypadkowy i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych					
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych					
– Niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych (inaczej niż przez przesyłanie lub przechowywanie)					
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przesyłanych					
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych przechowywanych					
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp do danych osobowych w inny sposób przetwarzanych(inaczej niż przez przesyłanie lub przechowywanie)					

Ryzyko naruszenia praw i wolności						
	Poziom ryzyka naruszenia praw i wolności osób fizycznych					
Przepis **Prawo** **Wolność**	Brak ryzyka	Ryzyko niskie	Ryzyko średnie	Wysokie ryzyko z zastrzeżeniami	Wysokie ryzyko	Ryzyko zrealizowane
Artykuł 5 ust. 1 lit. a RODO. – Prawo do przetwarzania danych osobowych w sposób zgodny z prawem, przysługujące osobie, której dane dotyczą. – Wolność od przetwarzania danych osobowych w sposób niezgodny z prawem.						
Artykuł 5 ust. 1 lit. a RODO. – Prawo do przetwarzania danych osobowych w sposób rzetelny, przysługujące osobie, której dane dotyczą. – Wolność od przetwarzania danych osobowych w sposób nierzetelny.						
Artykuł 5 ust. 1 lit. a RODO. – Prawo do przetwarzania danych osobowych w sposób przejrzysty, przysługujące osobie, której dane dotyczą. – Wolność od przetwarzania danych osobowych w sposób nieprzejrzysty.						
Artykuł 5 ust. 1 lit. b RODO. – Prawo do przetwarzania danych osobowych w sposób ograniczony co do celu, przysługujące osobie, której dane dotyczą. – Wolność od przetwarzania danych osobowych w sposób nieograniczony co do celu.						
Artykuł 5 ust. 1 lit. c RODO. – Prawo do przetwarzania danych osobowych w sposób ograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania, przysługujące osobie, której dane dotyczą. – Wolność od przetwarzania danych osobowych w sposób nieograniczony do czynności adekwatnych lub niezbędnych do osiągnięcia celu przetwarzania.						

Artykuł 5 ust. 1 lit. d RODO. – Prawo do przetwarzania danych osobowych w sposób prawidłowy, przysługujące osobie, której dane dotyczą. – Wolność od przetwarzania danych osobowych w sposób nieprawidłowy.						
Artykuł 5 ust. 1 lit. e RODO. – Prawo do przetwarzania danych osobowych w sposób ograniczony co do przechowywania, przysługujące osobie, której dane dotyczą. – Wolność od przetwarzania danych osobowych w sposób nieintegralny.						
Artykuł 5 ust. 1 lit. f RODO. – Prawo do przetwarzania danych osobowych w sposób integralny, przysługujące osobie, której dane dotyczą. – Wolność od przetwarzania danych osobowych w sposób nieintegralny.						
Artykuł 5 ust. 1 lit. f RODO. – Prawo do przetwarzania danych osobowych w sposób poufny, przysługujące osobie, której dane dotyczą, – Wolność od przetwarzania danych osobowych w sposób niepoufny – jawny.						

Ryzyko naruszenia praw i wolności związane z zaistnieniem naruszenia ochrony danych osobowych														
Czynność:										**Prawdopodobieństwo zaistnienia zdarzenia**				
Zagrożenie	Zgodność z prawem	Rzetelność	Przejrzystość	Ograniczenie celu	Minimalizacja	Prawidłowość	Ograniczenie przechow.	Integralność	Poufność	Nie mogło mieć miejsca	Niskie	Średnie	Wysokie	Miało miejsce
Zagrożenia dotyczące danych osobowych przesyłanych														
– Przypadkowe zniszczenie	+	+/–	+	+	+	+	+	+	–					
– Niezgodne z prawem zniszczenie	+	+/–	+	+	+	+	+	+	–					
– Przypadkowe i niezgodne z prawem zniszczenie	+	+/–	+	+	+	+	+	+	–					
– Przypadkowa utrata	+	+/-	+	+	+	+/-	+	+/-	+					
– Niezgodna z prawem utrata	+	+/–	+	+	+	+/–	+	+/–	+					
– Przypadkowa i niezgodna z prawem utrata	+	+/–	+	+	+	+/–	+	+/–	+					
– Przypadkowa modyfikacja	+	+/–	+	+	+	+	+	+	–					
– Niezgodna z prawem modyfikacja	+	+/–	+	+	+	+	+	+	–					
– Przypadkowa i niezgodna z prawem modyfikacja	+	+/–	+	+	+	+	+	+	–					
– Przypadkowe i nieuprawnione ujawnienie	+	+	+	+	+	–	+/–	–	+					
– Niezgodne z prawem i nieuprawnione ujawnienie	+	+	+	+	+	–	+/–	–	+					
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie	+	+	+	+	+	–	+/–	–	+					
– Przypadkowy i nieuprawniony dostęp	+	+	+	+	+	–	–	+/–	+					
– Niezgodny z prawem i nieuprawniony dostęp	+	+	+	+	+	–	–	+/–	+					
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp	+	+	+	+	+	–	–	+/–	+					

Ryzyko naruszenia praw i wolności związane z zaistnieniem naruszenia ochrony danych osobowych c.d.														
Czynność:										**Prawdopodobieństwo zaistnienia zdarzenia**				
	Zgodność z prawem	Rzetelność	Przejrzystość	Ograniczenie celu	Minimalizacja	Prawidłowość	Ograniczenie przechow.	Integralność	Poufność	Nie mogło mieć miejsca	Niskie	Średnie	Wysokie	Miało miejsce
Zagrożenia dotyczące danych osobowych przechowywanych														
– Przypadkowe zniszczenie	+	–	–	+	+	+	+	+	–					
– Niezgodne z prawem zniszczenie	+	–	–	+	+	+	+	+	–					
– Przypadkowe i niezgodne z prawem zniszczenie	+	–	–	+	+	+	+	+	–					
– Przypadkowa utrata	+	–	–	+	+	+	+	+	+					
– Niezgodna z prawem utrata	+	–	–	+	+	+	+	+	+					
– Przypadkowa i niezgodna z prawem utrata	+	–	–	+	+	+	+	+	+					
– Przypadkowa modyfikacja	+	–	–	+	+	+	+	+	–					
– Niezgodna z prawem modyfikacja	+	–	–	+	+	+	+	+	–					
– Przypadkowa i niezgodna z prawem modyfikacja	+	–	–	+	+	+	+	+	–					
– Przypadkowe i nieuprawnione ujawnienie	+	–	+/–	+	+	–	+	–	+					
– Niezgodne z prawem i nieuprawnione ujawnienie	+	–	+/–	+	+	–	+	–	+					
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie	+	–	+/–	+	+	–	+	–	+					
– Przypadkowy i nieuprawniony dostęp	+	–	+/–	+	+	–	–	+/–	+					
– Niezgodny z prawem i nieuprawniony dostęp do	+	–	+/–	+	+	–	–	+/–	+					
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp	+	–	+/–	+	+	–	–	+/–	+					

Ryzyko naruszenia praw i wolności związane z zaistnieniem naruszenia ochrony danych osobowych c.d.														
Czynność:										**Prawdopodobieństwo zaistnienia zdarzenia**				
	Zgodność z prawem	Rzetelność	Przejrzystość	Ograniczenie celu	Minimalizacja	Prawidłowość	Ograniczenie przechow.	Integralność	Poufność	Nie mogło mieć miejsca	Niskie	Średnie	Wysokie	Miało miejsce
Zagrożenia dotyczące danych osobowych przetwarzanych w inny sposób niż przez przesyłanie lub przechowywanie														
– Przypadkowe zniszczenie danych	+	+/–	+/–	+	+	+	+	+	–					
– Niezgodne z prawem zniszczenie	+	+/–	+/–	+	+	+	+	+	–					
– Przypadkowe i niezgodne z prawem zniszczenie	+	+/–	+/–	+	+	+	+	+	–					
– Przypadkowa utrata	+	+/–	+/–	+	+	+	+	+	+					
– Niezgodna z prawem utrata	+	+/–	+/–	+	+	+	+	+	+					
- Przypadkowa i niezgodna z prawem utrata	+	+/–	+/–	+	+	+	+	+	+					
– Przypadkowa modyfikacja	+	+/–	+/–	+	+	+	+	+	–					
– Niezgodna z prawem modyfikacja	+	+/–	+/–	+	+	+	+	+	–					
– Przypadkowa i niezgodna z prawem modyfikacja	+	+/–	+/–	+	+	+	+	+	–					
– Przypadkowe i nieuprawnione ujawnienie	+	+/–	+/–	+	+	+/–	+	+/–	+					
– Niezgodne z prawem i nieuprawnione ujawnienie	+	+/–	+/–	+	+	+/–	+	+/–	+					
– Przypadkowe i niezgodne z prawem i nieuprawnione ujawnienie	+	+/–	+/–	+	+	+/–	+	+/–	+					
– Przypadkowy i nieuprawniony dostęp	+	+/–	+/–	+	+	–	+/–	+/–	+					
– Niezgodny z prawem i nieuprawniony dostęp	+	+/–	+/–	+	+	–	+/–	+/–	+					
– Przypadkowy i niezgodny z prawem i nieuprawniony dostęp	+	+/–	+/–	+	+	–	+/–	+/–	+					

Realizacja
celów pracy

Realizacja celów pracy, dotyczących czynności o charakterze ocen

Realizacja celów pracy, dotyczących czynności o charakterze ocen (w zakresie analizy oceny ryzyka i zjawisk pochodnych), w odniesieniu do art. 24 RODO

Poniżej odpowiadam na pytania postawione w części pracy zatytułowanej: **Cele pracy w zakresie analizy oceny ryzyka i zjawisk pochodnych.** Dla zachowania jasności wywodu powtarzam kolejne pytania, w kolejności, w jakiej zostały zadane i obok pytania zamieszczam odpowiedzi.

– **Jakie czynności należy wykonać w związku z ochroną danych osobowych na gruncie RODO?**
– **Czy dana czynność jest związana z ochroną danych osobowych na gruncie RODO?**

W odniesieniu do konkretnej czynności najwygodniej jest na zadane powyżej pytania odpowiedzieć jednocześnie. Czynność oceny ryzyka naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze jest jedną z czynności, jakie należy wykonać w związku z ochroną danych osobowych na gruncie RODO.

Dana czynność, czyli ocena ryzyka naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze jest związana z ochroną danych osobowych na gruncie RODO. Należy przy tym dodać, że o ile ocena ryzyka, która wynika z art. 24 RODO, jest związana ochroną danych osobowych na gruncie RODO, o tyle ocena ryzyka, która wynika z art. 32 RODO, jest związana ochroną danych osobowych na gruncie RODO w większym stopniu.

Jeśli chodzi o czynność opisaną w art. 24 RODO, to jest ona związana z ochroną danych osobowych. Faktem jest, że związek czynności, której dotyczy art. 32 ust. 1 RODO, z ochroną danych osobowych jest może większy czy silniejszy niż związek czynności, której dotyczy art. 24 RODO, a szczególnie art. 24 ust. 1 RODO, jednak czynność, której dotyczy art. 24 ust. 1 RODO z ochroną danych osobowych związana jest.

Z art. 24 ust. 1 RODO wynika, że administrator ma wdrożyć środki techniczne i organizacyjne. Środki te mają być wdrożone, z tym że administrator ma obowiązek przy wdrażaniu tych środków wziąć pod uwagę charakter, zakres, kontekst, cele przetwarzania danych osobowych i ryzyko naruszenia praw i wolności osób fizycznych. Właśnie obowiązek wzięcia pod uwagę ryzyka naruszenia praw i wolności osób fizycznych zdaje się łączyć art. 24 RODO z ochroną danych osobowych. Głównym celem art. 24 RODO jest, „aby przetwarzanie odbywało się zgodnie z" RODO – to widzę jako główny cel tego przepisu. Obowiązek wykazania tej zgodności jest również zapisany w przepisie, jednak zwracam uwagę, że jest on poniekąd powtórzeniem zasady rozliczalności. Skoro zatem z art. 24 ust. 1 RODO wynika obowiązek dbałości o zgodność z RODO, to i ten obowiązek odnosi się po części do ochrony danych osobowych, ponieważ ochrona ta jest składową zgodności z RODO.

– Jaki jest związek danej czynności z ochroną danych osobowych?

Jeżeli odróżnimy od siebie ocenę ryzyka z art. 24 RODO i ocenę ryzyka z art. 32 RODO, to ta pierwsza jest słabiej związana z ochroną danych osobowych niż ta druga. Przypominam bowiem, że celem oceny ryzyka z art. 24 RODO jest, *aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać*, celem zaś oceny ryzyka z art. 32 RODO jest, *aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku […]*

Patrząc najogólniej, jednak już w odniesieniu do czynności związanych z ochroną danych osobowych należy zadać wymienione poniżej pytania.

– Kiedy należy wykonać czynność?

Czynność należy wykonać przed przystąpieniem do przetwarzania danych osobowych i następnie należy ją powtarzać na tyle często, by zachowana była realizacja celów czynności, czyli: *aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać*. Omawiam to w uwadze (*3.20. Art. 24. Uwaga 20. Jak i kiedy oceniać ryzyko*) i (*3.21. Art. 24. Uwaga 21. Powtarzanie ocen ryzyka*).

Ideałem byłaby – jak się zdaje – sytuacja, kiedy czynności opisane w art. 24 RODO, po raz pierwszy wykonano by przed przystąpieniem do przetwarzania danych osobowych. Następnie czynności te należy wykonywać powtarzalnie w sposób wynikający głównie ze zmian w zakresie okoliczności ocenianych podczas wykonywania czynności. Jeśli zatem zmienia się lub może się zmienić charakter, zakres, kontekst lub cele przetwarzania, lub ryzyko naruszenia praw, lub wolności osób fizycznych, to czynności należy powtórzyć.

Wskazana wyżej idealna sytuacja początkowa, kiedy to administrator danych osobowych dokonuje czynności wynikających z art. 24 RODO jeszcze przed przystąpieniem do przetwarzania, może być niemożliwa, zwłaszcza w sytuacji administratora, który przed pojawieniem się RODO już istniał i dane przetwarzał.

Kolejna zatem sytuacja idealna, to wykonanie czynności w maju roku 2018, czyli tuż po momencie, od którego RODO poczęło wywoływać skutki prawne. Kiedy i ta idealna sytuacja nie miała miejsca, to pozostaje sformułować postulat, zgodnie z którym administrator wykona czynności opisane w art. 24 RODO, kiedy tylko przystąpi do wdrażania RODO w swojej organizacji.

– Co powinno być przedmiotem czynności? (Jak należy wykonać daną czynność?) (Co należy poddać ocenie?)

Przedmiotem czynności powinno być przeprowadzenie oceny ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze. Jeśli chodzi o samo wykonanie czynności, to możliwości są różne, zależnie od tego, czy uznamy, że ocena ryzyka, o której mowie w art. 24 ust. 1 RODO, pokrywa się z oceną ryzyka, o której mowa w art. 32 ust. 1 RODO czy nie. Uważam, że oceny te się nie pokrywają, co najwyżej ocena z art. 32 ust. 1 RODO może być uznana za część oceny, z art. 24 ust. 1 RODO. Ocena z art. 24 ust. 1 RODO to ocena nakierunkowana na cel, jakim jest zgodność przetwarzania danych osobowych w sposób zgodny z prawem i jednoczesna możliwość wykazania realizacji tego celu. W związku z tym, dla poprawnego, bo zgodnego z przepisem, przeprowadzenia tej oceny konieczne jest ocenienie dwóch elementów. Pierwszy to ocena ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze. Ten element wydaje się konieczny, ponieważ w sposób dosłowny wynika z przepisu, jest w przepisie zapisany.

Wydaje się jednak, że ten element nie jest wystarczający. Nie jest wystarczający, ponieważ cel przepisu to zgodność przetwarzania z RODO i możliwość wykazania tejże. Wydaje się więc, że drugim elementem, jaki należy poddać ocenie, jest zgodność przetwarzania danych osobowych z prawem. Skoro ta zgodność jest celem i skoro należy móc ją wykazać, to trzeba to umieć wykazać, jak również trzeba po prostu wiedzieć, że przetwarza się w sposób zgodny z prawem. To z kolei można wiedzieć tylko wtedy, gdy się to oceni. Jeśli nie dokona się oceny zgodności przetwarzania z prawem, to można się tego tylko domyślać, nie sposób zaś domysłu w przedmiocie zgodności przetwarzania utożsamiać z tą zgodnością. Podsumowując – trzeba dokonać czegoś na kształt audytu zgodności z prawem przetwarzania danych osobowych.

– Jakie czynności należy podjąć po wykonaniu czynności, która jest przedmiotem namysłu?

Przede wszystkim należy zarchiwizować dokumenty, które są dowodami na to, że administrator dokonał oceny na gruncie art. 24 ust. 1 RODO.

Kolejną czynnością, po wykonaniu czynności oceny ryzyka jest – jak się wydaje – dostosowanie przetwarzania do wymogów stawianych przez przepisy prawa. Czynność ta ma miejsce, jeżeli ocena wykaże, że przetwarzanie danych osobowych w jakimś zakresie odbiega od obowiązków prawnych.

Kolejną czynnością jest też po prostu przetwarzanie danych osobowych, teraz już w sposób zgodny z prawem. Być może i wcześniej odbywało się ono w sposób zgodny z prawem (zwłaszcza jeżeli bierzemy pod rozwagę kolejną ocenę ryzyka, nie zaś pierwszą ocenę ryzyka, pierwszą czyli tę podjętą jeszcze przed przystąpieniem do przetwarzania danych osobowych). Być może tak się odbywało, jednak po wykonaniu oceny, administrator jest pewien, że teraz przetwarzanie danych osobowych jest z prawem zgodne.

Realizacja celów pracy, dotyczących czynności o charakterze ocen (w zakresie analizy oceny ryzyka i zjawisk pochodnych), w odniesieniu do art. 32 RODO

Poniżej odpowiadam na pytania postawione w części pracy zatytułowanej: **Cele pracy w zakresie analizy oceny ryzyka i zjawisk pochodnych.** Dla zachowania jasności wywodu powtarzam kolejne pytania, w kolejności, w jakiej zostały zadane i obok pytania zamieszczam odpowiedzi.

– Jakie czynności należy wykonać w związku z ochroną danych osobowych na gruncie RODO?

– Czy dana czynność jest związana z ochroną danych osobowych na gruncie RODO?

Podobnie jak w przypadku art. 24 RODO, w odniesieniu do czynności, o której mowa w art. 32 RODO, najwygodniej jest na zadane powyżej pytania odpowiedzieć jednocześnie. Z art. 32 ust. 1 RODO wynika obowiązek. Czynność oceny ryzyka naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze jest jedną z czynności, jakie należy wykonać w związku z ochroną danych osobowych na gruncie RODO. O czynności tej mowa jest w art. 24 RODO (piszę o tym w odpowiednim miejscu niniejszej książki) i w art. 32 RODO.

Dana czynność, czyli ocena ryzyka naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze jest związana z ochroną danych osobowych na gruncie RODO.

Należy przy tym dodać, ocena ryzyka, która wynika z art. 32 ust. 1 RODO, jest związana z ochroną danych osobowych na gruncie RODO w większym stopniu niż ocena ryzyka, która wynika z art. 24 RODO. Artykuł 24 RODO poświęcony jest nie tylko ocenie ryzyka, przepis ten nakazuje co prawda dokonanie oceny ryzyka ale jej celem jest zgodność przetwarzania danych osobowych z RODO i możliwość wykazania tej zgodności, podczas gdy celem art. 32 ust. 1 RODO jest zapewnienie stopnia bezpieczeństwa przetwarzania danych odpowiadającego ryzyku. Zakres art. 32 ust. 1 RODO jest węższy, bezpieczeństwo przetwarzania danych osobowych zawiera się w zgodności przetwarzania danych osobowych z prawem, jednak w jej szerokim rozumieniu. Zgodność

przetwarzania danych osobowych z prawem w jej wąskim rozumieniu to zgodność przetwarzania danych z art. 6 RODO.

– Jaki jest związek danej czynności z ochroną danych osobowych?

Po odróżnieniu od siebie obowiązków z art. 24 RODO i z art. 32 RODO – o czym piszę wyżej – widzimy, że związek art. 32 RODO z ochroną danych osobowych jest bezpośredni. Celem art. 32 ust. 1 RODO jest, *aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku […]* Ponadto po art. 32 ust. 1 RODO znajduje się art. 32 ust. 2 RODO, który to przepis zawiera listę parametrów, jakie należy wziąć pod uwagę przy dokonywaniu oceny ryzyka na gruncie art. 32 ust. 1 RODO. Parametry, o których tu piszę, to inaczej ryzyka, które administrator danych osobowych ma obowiązek wziąć pod uwagę przy dokonywaniu oceny ryzyka. Mają one charakter techniczny i organizacyjny i są ściśle, treściowo związane z ochroną danych osobowych. Co więcej, zagrożenia te są powtórzeniem zagrożeń, które zawarte są w definicji naruszenia ochrony danych osobowych, która znajduje się w art. 4 pkt 12 RODO.

Można zatem powiedzieć, że administrator, który dokonuje oceny ryzyka na gruncie art. 32 ust. 1 RODO, dokonuje tym samym oceny ryzyka zaistnienia naruszenia ochrony danych osobowych, które jest zdefiniowane w art. 4 pkt 12 RODO.

– Kiedy należy wykonać czynność?

Czynność należy wykonać przed przystąpieniem do przetwarzania danych osobowych i następnie należy ją powtarzać na tyle często, by zachowana była realizacja celów czynności. Opisuję to częściowo w podrozdziale (*3.11 Art. 32 ust. 1 i 2 i 3 Uwaga 11 Kolejność czynności*). Ocenę ryzyka należy wykonać po sporządzeniu rejestru czynności przetwarzania danych osobowych, za które odpowiada administrator danych osobowych (lub odpowiednio rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, który prowadzi podmiot przetwarzający).

Jeżeli administrator danych osobowych zamierza przystąpić do wykonywania nowej czynności, to uważam, że zanim zacznie tę czynność rzeczywiście wykonywać, powinien on dopisać tę czynność do odpowiedniego rejestru, o ile go prowadzi (zwykle tak właśnie czyni)

i następnie dokonać oceny ryzyka wykonywania tej czynności. Patrząc przez pryzmat RODO, jeżeli administrator nie wykona oceny ryzyka nowej czynności, to administrator nie wie, jak chronić dane przetwarzane tą czynnością. Nie wie, ponieważ właśnie nie wykonał oceny ryzyka. Przetwarzanie danych innymi czynnościami może być bardzo podobne, ryzyka mogą być podobne, środki ochrony mogą być podobne, jednak podkreślenia wymaga, że ochrona danych przetwarzanych jedną czynnością jest czymś odmiennym od ochrony danych przetwarzanych inną czynnością, nawet jeżeli te czynności są podobne. Jest czym innym, bo to są inne czynności.

– Co powinno być przedmiotem czynności? (Jak należy wykonać daną czynność?) (Co należy poddać ocenie?)

Przedmiotem czynności powinno być przeprowadzenie oceny ryzyka naruszenia praw i (sic!) wolności osób fizycznych o różnym prawdopodobieństwie i wadze. Następnie przedmiotem czynności powinno być wdrożenie środków technicznych i środków organizacyjnych odpowiednich do ocenionego ryzyka. Celem wdrożenia środków jest zapewnienie stopnia bezpieczeństwa odpowiadającego temu ryzyku.

Wydaje się, że ocena ryzyka na gruncie art. 32 ust. 1 RODO i wdrożenie środków na gruncie art. 32 ust. 2 RODO są elementami oceny z art. 24 RODO, jednak elementami, które dotyczą właśnie ochrony danych osobowych.

Analiza przepisów prowadzi do wniosku, że najpierw należy dokonać oceny na gruncie art. 32 ust. 2 RODO i ocenić ryzyko zaistnienia wymienionych tam okoliczności. Następnie należy przystąpić do oceny ryzyka na gruncie art. 32 ust. 1 RODO i ocenić *ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze*. Następnie należy dokonać wdrożenia odpowiednich środków technicznych i organizacyjnych nadal na gruncie art. 32 ust. 1 RODO. Poza tym należy udokumentować wykonanie wskazanych wyżej czynności, co wynika z art. 5 ust. 2 RODO.

– Jakie czynności należy podjąć po wykonaniu czynności, która jest przedmiotem namysłu?

Przede wszystkim należy zarchiwizować dokumenty, które są dowodami na to, że administrator dokonał oceny i następnie wdrożenia na gruncie art. 32 ust. 1 i 2 RODO.

Należy tu zwrócić uwagę na jeszcze jeden element, otóż, jak piszę wyżej w (*3.11 Art. 32 ust. 1 i 2 i 3 Uwaga 11 Kolejność czynności*):

„– Wdrożenie środków technicznych i organizacyjnych modyfikuje ryzyko. […]
– Wprowadzenie nowych czynności modyfikuje ryzyko.
– Upływ czasu modyfikuje ryzyko".

Z uwagi na powyższe, należy powtarzać zarówno czynność oceny ryzyka, jak i czynność jej dokumentowania, jak i – o ile to zachodzi – czynność wdrożenia środków technicznych i organizacyjnych. Przede wszystkim po wdrożeniu środków technicznych i organizacyjnych należałoby dokonać oceny ryzyka. Ocena taka pozwoliłaby stwierdzić, czy wdrożone środki są odpowiednie.

Jeśli chodzi o powtarzanie czynności oceny ryzyka i wdrożenia środków w związku z wprowadzeniem nowych czynności lub w związku z upływem czasu, to powtarzanie takie – co wiem z własnych obserwacji – się odbywa. Czasem administratorzy zapominają o doniosłości jednego lub drugiego czynnika, jednak czasem też pamiętają. Nie prowadzę tu badań, dysponuję jedynie pewnymi obserwacjami.

Realizacja celów pracy, dotyczących czynności o charakterze ocen (w zakresie analizy oceny ryzyka i zjawisk pochodnych), w odniesieniu do art. 33 i 34 RODO

Poniżej odpowiadam na pytania postawione w części pracy zatytułowanej: **Cele pracy w zakresie analizy oceny ryzyka i zjawisk pochodnych.** Dla zachowania jasności wywodu powtarzam kolejne pytania, w kolejności, w jakiej zostały zadane i obok pytania zamieszczam odpowiedzi.

Realizacja wskazanych celów pracy jest poniżej opisana łącznie dla art. 33 RODO i dla art. 34 RODO w takim zakresie, w jakim je w pracy omawiam. Połączenie (o charakterze nowelizacji) art. 33 RODO z art. 34 RODO postuluję w dwóch postulatach *de lege ferenda* postawionych wyżej w niniejszej pracy (*6.1. Art. 34 ust. 1. Postulat 1. Połączenie przepisów. Wersja minimalistyczna*) i (*6.2. Art. 34 ust. 1. Postulat 2 i 3. Połączenie przepisów. Wersja pełniejsza. Uzupełnienie przepisu o naruszenie praw i wolności*).

– Jakie czynności należy wykonać w związku z ochroną danych osobowych na gruncie RODO?

– Czy dana czynność jest związana z ochroną danych osobowych na gruncie RODO?

Zarówno art. 33 RODO, jak i art. 34 RODO związane są z ochroną danych osobowych. Związek ten jest może na pierwszy rzut oka zaskakujący, jest jednak niewątpliwy. Obydwa przepisy dotyczą sytuacji, w której nastąpiło naruszenie ochrony danych osobowych, zdefiniowane w art. 4 pkt 12 RODO.

Czynności, o których mowa w art. 33 RODO i art. 34 RODO, wymieniam poniżej.

Najpierw zachodzi zdarzenie. Nie opisuję go tu szczegółowo, zostało tak bowiem opisane przez mnie w jednej z poprzednich monografii[362]. Jeżeli zdarzenie to stanowi naruszenie ochrony danych osobowych zdefiniowane w art. 4 pkt 12 RODO, to oznacza to, że admi-

[362] J. Rzymowski, *RODO – GDPR. Przedmiot i cele…*, s. 487–531.

nistrator danych osobowych ma obowiązek zastosować art. 33 RODO i art. 34 RODO. Można się spierać i postawić tu tezę, że jeżeli poziom ryzyka nie jest wysoki, to administrator stosuje jedynie art. 33 RODO, ale należy przy tym pamiętać, że wysoki poziom ryzyka skutkuje obowiązkiem zastosowania art. 34 RODO. Uważam zatem, że po zaistnieniu naruszenia ochrony danych osobowych administrator danych osobowych powinien wziąć pod uwagę zawsze nie tylko art. 33 RODO, ale również art. 34 RODO, po to co najmniej, by ustalić, że poziom ryzyka wysoki nie jest i że w związku z tym nie należy stosować art. 34 RODO, a jedynie art. 33 RODO.

Następnie zatem administrator ocenia poziom ryzyka naruszenia praw i wolności osób fizycznych. Oczywiście administrator ocenia poziom ryzyka, jakie mogło mieć miejsce w związku z zaistniałym zdarzeniem. Zależnie od poziomu ryzyka administrator odpowiednio: nie informuje nikogo, informuje PUODO (organ nadzorczy), informuje PUODO i osoby, których dane dotyczą (art. 33 ust. 1 RODO).

Jeżeli zdarzenie miało miejsce nie w organizacji administratora, ale w organizacji podmiotu przetwarzającego, to podmiot przetwarzający po zaistnieniu zdarzenia informuje o nim administratora (art. 33 ust. 2 RODO).

Jednocześnie administrator dokumentuje szczegóły naruszenia i podjętych działań zaradczych w sposób, który umożliwić może organowi nadzorczemu weryfikację, czy administrator przestrzega art. 33 RODO (art. 33 ust. 5 RODO).

Może się zdarzyć, że administrator danych osobowych poinformuje PUODO, a nie poinformuje jeszcze osób, których dane dotyczą. W takiej sytuacji administrator danych osobowych musi wykonać czynności odpowiednio do tego, co poleci mu wykonać PUODO. PUODO może zatem nakazać poinformowanie osób, których dotyczą dane, których dotyczyło naruszenie; PUODO może też uznać, że zaistniały zjawiska, które opisane są w art. 34 ust. 3 RODO i że w związku z tym administrator nie informuje osób, których dotyczą.

– Jaki jest związek danej czynności z ochroną danych osobowych?

Związek między czynnościami, które są opisane w art. 33 RODO i w art. 34 RODO, jest bezpośredni. Administrator danych osobowych, a następnie również PUODO mają obowiązek wykonać czynności opisane we wskazanych przepisach, kiedy zajdzie naruszenie ochrony

danych osobowych, czyli zdarzenie opisane w art. 4 pkt. 12 RODO. Naruszenie ochrony danych osobowych, co zakrawa na truizm, dotyczy ochrony danych osobowych. Można oczywiście wywodzić, że naruszenie ochrony danych osobowych nie dotyczy samych danych, ale że dotyczy ono właśnie ich ochrony. Jest to logicznie poprawne, jednak wydaje się to być niepotrzebnym dzieleniem włosa na szesnaścioro.

– Kiedy należy wykonać czynność?

Czynności opisane w art. 33 RODO i w art. 34 RODO należy wykonać po zaistnieniu naruszenia ochrony danych, czyli zdarzenia opisanego w art. 4 pkt 12 RODO.

– Co powinno być przedmiotem czynności? (Jak należy wykonać daną czynność?) (Co należy poddać ocenie?)

Najpierw ma miejsce zdarzenie, przedmiotem czynności musi być zatem ustalenie, czy zdarzenie, które zaszło, jest zdarzeniem, którego cechy opisane są w art. 4 pkt 12 RODO. Administrator danych osobowych musi więc zdarzenie takie poddać ocenie pod kątem realizacji warunków, które znajdują się w art. 4 pkt 12 RODO. W przepisie tym są zawarte trzy grupy warunków, by zdarzenie było naruszeniem musi ono realizować co najmniej po jednym warunku z każdej z grup. Nie opisuję tu tego bardziej szczegółowo, zostało to bowiem szczegółowo omówione na kartach niniejszej książki (*3.11. Art. 33 Uwaga 11. Naruszenie ochrony danych osobowych – metoda ustalenia*), (*3.14. Art. 33 Uwaga 14. Naruszenie ochrony danych osobowych. Kolejność działań*.), (*3.10. Art. 33 ust. 1 Uwaga 10. Naruszenie ochrony danych osobowych – zestawienie*).

Jeżeli naruszenie opisane w art. 4 pkt 12 RODO ma miejsce, to administrator ma obowiązek je udokumentować. Dokumentacja ta powinna obejmować „okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu (sic!) weryfikowanie przestrzegania niniejszego artykułu".

Następnie należy dokonać oceny ryzyka naruszenia praw i wolności osób fizycznych w związku z naruszeniem. Tu również nie opisuję zagadnienia bardziej szczegółowo, tak właśnie bowiem opisałem je wyżej w książce (*3.2. Art. 33 ust. 1 Uwaga 2. Prawa i wolności przy ocenie skutków naruszenia*), (*3.3. Art. 33 ust. 1 Uwaga 3. Prawa*

i wolności w RODO. Zarys zagadnień), (*3.4. Art. 33 ust. 1 Uwaga 4. Prawa i wolności w RODO. Naruszenie łącznie z naruszeniem innych praw i wolności*) (*3.5. Art. 33 ust. 1 Uwaga 5. Prawa i wolności. Źródła inne niż RODO*), (*3.6 Art. 33 ust. 1 Uwaga 6. Prawa i wolności w EKPC*), (*3.7. Art. 33 ust. 1 Uwaga 7. Prawa i wolności w KPP UE*).

W końcu – zależnie od poziomu ryzyka naruszenia praw i wolności osób fizycznych – należy podjąć decyzję, czy nie informować nikogo, czy poinformować PUODO, czy poinformować PUODO i osoby, których dane dotyczą i oczywiście decyzję tę zrealizować.

Administrator powinien również wdrożyć odpowiednie środki techniczne i organizacyjne tak, by zapobiec pogłębianiu się skutków naruszenia i by zapobiec kolejnym analogicznym naruszeniom (Art. 33 ust. 3 lit. d RODO, art. 34 ust. 3 RODO).

– Jakie czynności należy podjąć po wykonaniu czynności, która jest przedmiotem namysłu?

I tu również, podobnie jak w odniesieniu do art. 32 RODO, należy archiwizować wszystkie dokumenty. Administrator musi mieć dowody, że dokonał odpowiednich ocen na gruncie art. 33 i art. 34 RODO. Administrator musi również zarchiwizować dokumentację naruszenia, o której mowa w art. 33 ust. 5 RODO.

Wdrożenie odpowiednich środków technicznych i organizacyjnych, które mają na celu zapobieżenie dalszym skutkom naruszenia i zapobieżenie analogicznym naruszeniom to czynności, o których jest mowa na gruncie art. 33 RODO i art. 34 RODO.

Należy jednocześnie zastanowić się nad tym, co administrator danych osobowych powinien uczynić po wykonaniu czynności, których obowiązek wykonania wynika z art. 33 RODO i z art. 34 RODO.

Nie wydaje się, by z przepisów wynikały tu jakieś konkretne czynności do wykonania. Jednocześnie wydaje się, że jeżeli zaszło naruszenie, to administrator danych osobowych powinien poważnie zastanowić się nad wykonanymi ocenami ryzyka i nad stosowanymi środkami ochrony. Oceny wykonano, środki wdrożono i jednocześnie naruszenie zaszło. Może to o czymś świadczyć. Może świadczyć o niewłaściwie wykonanej ocenie ryzyka, może świadczyć o niewłaściwych, nieodpowiednich do oceny ryzyka albo niewłaściwie wdro-

żonych środkach zabezpieczających, może wreszcie świadczyć o niedostatecznym przeszkoleniu pracowników lub o niewydajnej pracy IODa. O czymkolwiek by świadczyło, problem należy przemyśleć i podjąć odpowiednie do wyniku przemyśleń kroki.

Realizacja pozostałych celów pracy

Realizacja celu:

„Poczynienie ustaleń szczegółowych, dotyczących ocen ryzyka”

Cel ten realizowany jest w rozdziale pierwszym i w rozdziale drugim pracy, zatytułowanych: *Ocena ryzyka na gruncie art. 24 RODO* i *Ocena ryzyka na gruncie art. 32 RODO*. Rozdziały te liczą w sumie około 210 stron. Zgodnie z przyjętą konstrukcją pracy, w rozdziałach tych najpierw szczegółowo analizuję przepis. Czynię to z wykorzystaniem etapowej analizy semantycznej. Wyniki analizy prezentuję w podrozdziałach warstwy „Analiza”, wnioski z analizy, miejscami w wersji skróconej, prezentuję w podrozdziałach warstwy „Wnioski z analizy”. Ustalenia tam prezentowane są bardzo szczegółowe, co zapewnia zastosowanie etapowej analizy semantycznej. Ustalenia czynione na poziomie wykładni są, w miarę potrzeby, rozwijane w podrozdziałach warstwy „Uwagi”. Podrozdziałów warstwy tej, w odniesieniu do art. 24 RODO powstało 31. W odniesieniu do art. 32 RODO, podrozdziałów tej warstwy powstało 13. Elementami podrozdziałów warstwy „Uwagi” są elementy podsumowujące kolejne rozważania w duchu konceptualizmu prawniczego, czyli teorii, która pozwala przełożyć język przepisów na język uprawnień i obowiązków. Realizuję w ten sposób jeden z dalszych celów pracy, ale i podnoszę poziom szczegółowości rozważań. Rozważania warstwy „Analiza” prowadzone są za pomocą klasycznej metody logiczno-językowej i następnie uzupełnione są przez rozważania powstałe na gruncie konceptualizmu prawniczego. Rozważania na gruncie konceptualizmu prawniczego stanowią niejako ponowną analizę kolejnych fragmentów przepisów, jednak analiza ta pozwala na uchwycenie oraz – co ważne – zaprezentowanie czytelnikom, miejsc, w których przepis skutkuje uprawnieniem i obowiązkiem.

Nie chcę tu powtarzać tez, które zostały postawione i wniosków, które zostały wywiedzione na gruncie pracy na art. 24 RODO i art. 32 RODO, jednak z uwagi na ich szczegółowość uważam, że omawiany tu cel pracy został zrealizowany. Warto dodać, że uważam tak nie tylko z uwagi na sam fakt przeprowadzenia rozważań, ale też z uwagi na to, że poprowadzenie analizy przepisów metodą warstwo-

wą pozwoliło na przyjrzenie się przepisom pod różnym kątem i – co nie mniej ważne – na zrozumiałą prezentację wyników tej lustracji.

Stawiając ten cel, zakładałem, że dobrze byłoby, gdyby rozważania naukowe – czy to dogmatyczne czy to teoretyczne – miały też walor dla praktyki. Uważam, że cel pracy również w tym zakresie udało mi się osiągnąć. Szczególne znaczenie dla praktyki może mieć wskazanie, jakie prawa i wolności należy brać pod uwagę przy dokonywaniu ocen ryzyka oraz jakie zagrożenia techniczne i organizacyjne należy przy wykonywaniu tych ocen pod uwagę brać. Z uwagi na potrzeby praktyki zestawienia poczynione na gruncie wniosków w podrozdziałach warstwy „Uwagi" zamieszczam na końcu niniejszej książki, tak by mogły służyć w codziennej pracy osób dokonujących ocen.

Ustalenia powyższe dotyczą ryzyka naruszenia praw i wolności, które jest brane pod uwagę na etapie dokonywania ocen ryzyka. Ryzyko naruszenia praw i wolności jest również brane pod uwagę przy okazji dokonywania ocen skutków naruszenia. Odnoszę się do tego niżej, ponieważ rozważania dotyczące ocen skutków naruszenia dotyczą realizacji raczej kolejnego celu pracy. Zwracam tu jedynie uwagę na fakt, który może umknąć przy lekturze kolejnych rozważań szczegółowych, że ryzyko które jest brane pod uwagę na etapie dokonywania ocen ryzyka i ryzyko, które jest brane pod uwagę na etapie dokonywania ocen skutków naruszenia to ryzyko, będące ryzykiem, które można określić jako takie same rodzajowo.

Realizacja celu:

„Poczynienie ustaleń szczegółowych, dotyczących ocen skutków naruszenia"

Cel ten realizowany jest w rozdziale trzecim pracy, zatytułowanym: *Naruszenie ochrony danych osobowych i jego zgłaszanie*. W rozdziale tym analizuję głównie dwa przepisy, a to art. 33 RODO i art. 34 RODO. Rozdział ten liczy sobie około 230 stron. Również w tym rozdziale, konsekwentnie trzymając się konstrukcji pracy, najpierw szczegółowo analizuję przepis, z wykorzystaniem etapowej analizy semantycznej. Oczywiście również tu wyniki analizy prezentuję w podrozdziałach warstwy „Analiza", wnioski z analizy zaś prezentuję w podrozdziałach warstwy „Wnioski z analizy".

Ustalenia czynione na poziomie wykładni są rozwijane w podrozdziałach warstwy „Uwagi". Podrozdziałów warstwy tej, w odniesieniu do art. 33 RODO powstało 24. W odniesieniu do art. 34 RODO, podrozdziałów tej warstwy powstało 19. Elementy podsumowujące kolejne rozważania w duchu konceptualizmu prawniczego zostały umieszczone w osobnych podrozdziałach.

Jeśli chodzi o realizację tego elementu celu pracy, jakim jest ustalenie, jakie prawa i wolności osób fizycznych należy koniecznie na gruncie RODO chronić, to cel ten został zrealizowany zarówno poprzez pryzmat tego, jakie prawa i wolności chronić, jak i poprzez pryzmat tego, jak to czynić. O tym, jakie prawa chronić, piszę w wielu miejscach tej pracy, ale zwłaszcza wskazuję to w podrozdziale (*3.1. Art. 24 Uwaga 1 Prawa i wolności*), gdzie rzecz omawiam ogólnie. Nieco bardziej szczegółowo, ale nadal na gruncie RODO rzecz omawiam w dwóch podrozdziałach, a to w: (*3.2. Art. 24 Uwaga 2. Przykładowe prawa i wolności zasadnicze*) i (*3.3. Art. 24 Uwaga 3. Przykładowe prawa i wolności szczegółowe*). Zjawisku praw i wolności poza RODO poświęcony jest między innymi podrozdział (*3.4. Art. 24 Uwaga 4. Inne prawa i wolności*).

O tym, jak chronić prawa i wolności, piszę również w wielu miejscach niniejszej pracy, pewne podrozdziały można jednak wskazać jako te, w których cel realizowany jest najdokładniej. Zrazu zatem rozważam poziomy ryzyka naruszenia praw i wolności (3.*14. Art. 24. Uwaga 14 Poziomy ryzyka*) i prezentuję je w sposób, który łączy tabelę z ryciną. Dalej wskazuję na konieczny związek między przepisem a prawem, obowiązkiem i wolnością (*3.23. Art. 24. Uwaga 23 Przepis jako zapis prawa, obowiązku i wolności*), w kolejnych uwagach wskazuję argumenty, które potwierdzają ten związek. Wskazuję również na zjawisko stałej zależności między zdarzeniami z art. 32 ust 2 RODO a zasadami z art. 5 RODO (*3.30. Art. 24. Uwaga 30 Ryzyko. Pojęcie na gruncie art. 32. Stałość zależności*). Ryzykiem naruszenia praw i wolności zajmuje się w uwadze (*3.5 Art. 32 ust. 1 i 2 i 3 Uwaga 5 Prawa i wolności*). Zagadnieniem praw i wolności zajmuję się również dalej (*3.3. Art. 33 ust. 1 Uwaga 3 Prawa i wolności w RODO Zarys zagadnień*) i w uwagach kolejnych. Dalej zajmuję się tym w uwadze (*3.2. Art. 34 ust. 1 Uwaga 2 Ocena ryzyka naruszenia praw i wolności*) i kolejnych, w jednej, z których prezentuję rozwiniętą wersję wymienionej wyżej tabeloryciny, w której wskazuję nie tylko kiedy,

ale i kogo informować o naruszeniach. Na końcu książki wracam do zjawiska związku między zdarzeniami z art. 32 ust. 2 RODO lub art. 4 pkt 12 RODO a zasadami z art. 5 RODO poprzez zestawienie tychże w tabelach.

Realizacja celu:

„Prezentacja etapowej analizy semantycznej"

Cel ten realizowany jest w rozdziale pierwszym i w rozdziale drugim i w rozdziale trzecim pracy w podrozdziałach warstwy „Analiza". Etapowa analiza semantyczna, to metoda, która posłużyła do przeprowadzenia analizy przepisów prezentowanej na kartach niniejszej książki. Rozważania prowadzone za pomocą etapowej analizy semantycznej prowadzone są w podrozdziałach warstwy „Analiza". Na bazie analiz wykonanych z wykorzystaniem etapowej analizy semantycznej prowadzone są dalsze prace w niniejszej książce. Etapowa analiza semantyczna została w niniejszej książce zaprezentowana niejako w działaniu. Na początku książki (*Pozostałe cele pracy*) omówione zostały kolejne etapy, które składają się na etapową analizę semantyczną, mam jednak poczucie, że metodę tę prawdziwie udało mi się zaprezentować nie tam gdzie ją omawiam, ale tam gdzie ją stosuję.

Etapowa analiza semantyczna pozwala nie tylko właśnie na analizę przepisów, ale umożliwia również prace dalsze. Prace te zostały zaprezentowane w podrozdziałach kolejnych warstw. Faktem jest, że rozważania prowadzone w podrozdziałach kolejnych warstw, nie są prowadzone z wykorzystaniem przedmiotowej metody, jednak uważam, że jej zastosowanie w podrozdziałach warstwy „Analiza" i tym samym szczegółowe przeanalizowanie przepisów, pozwoliło na dokonanie rozważań w rozdziałach kolejnych warstw. Poza tym etapowa analiza semantyczna jest metodą właśnie analizy przepisów, nie zaś metodą prowadzenia dalszych wobec analizy, rozważań dogmatycznych lub teoretycznych. Drobiazgowa analiza wykonana z użyciem tej metody pozwala na prowadzenie rozważań szczegółowych, ujętych w podrozdziałach warstwy „Uwagi".

Realizacja celu:

„Prezentacja konceptualizmu prawniczego – ogólnej teorii prawa”

Cel ten realizowany jest we wszystkich rozdziałach książki. W rozdziale pierwszym i drugim, poświęconym art. 24 RODO i art. 32 RODO. W rozdziałach tych podsumowania sporządzone na gruncie konceptualizmu prawniczego wprowadzone zostały między do podrozdziałów warstwy „Analiza” i przeplecione zostały z tradycyjnymi, dogmatycznymi, rozważaniami prowadzonymi za pomocą metody logiczno-językowej. Efektem takiego podejścia jest dokładniejsza (niż tradycyjna) analiza przepisu. Przepis jest analizowany w sposób tradycyjny, a następnie analizowane jest, jakie uprawnienie przysługuje osobie, której dane dotyczą, na podstawie danego fragmentu przepisu i jednocześnie, jaki obowiązek na podstawie tego fragmentu przepisu spoczywa na administratorze. Następnie, pod koniec - rozdziału poświęconego art. 24 RODO i pod koniec rozdziału poświęconego art. 32 RODO, zamieszczone są podrozdziały zatytułowane „**Podsumowanie w duchu Konceptualizmu Prawniczego – Ogólnej Teorii Prawa**”. W podrozdziałach tych powtórzone i odpowiednio połączone są rozważania dotyczące obowiązków administratora danych osobowych i uprawnień (praw) osób, których dane dotyczą. Podrozdziały te stanowią swojego rodzaju osobny komentarz do kolejnych przepisów RODO. Komentarz ten pozwala spojrzeć na przepisy RODO nie tylko w sposób, który nazwałbym tradycyjnie dogmatycznym, ale daje on też inne spojrzenie. Czytelnik wskazanych podrozdziałów może potraktować je po prostu jako źródło wiedzy o prawach i obowiązkach, Czytelnik może też zauważyć, że każdy z analizowanych przepisów ustanawia uprawnienie i obowiązek. Daje to – jak uważam – właściwy wgląd w istotę przepisów i głębiej – w istotę prawa. Nieważne, czy ktoś hołduje wizji prawa jako systemu uprawnień, czy prawa jako systemu obowiązków, niezależnie od tego, tak prawa, jak obowiązki są w książce zapisane, widać więc, że prawo je ustanawia, czy też – inaczej patrząc – że składają się one na prawo.

Prowadzenie rozważań z wykorzystaniem konceptualizmu prawniczego – ogólnej teorii prawa pozwala nie tylko zaprezentować tę teorię w praktyce, co jest omawianym tu celem pracy, ale pozwala ono również na prezentację możliwości, jakie ta teoria daje.

Realizacja celu:

„Postawienie postulatów *de lege ferenda*"

Cel ten realizowany jest we wszystkich rozdziałach książki. W rozdziale pierwszym postawiono 4 postulaty, w rozdziale drugim postawiono 2 postulaty, w rozdziale trzecim postawiono 13 postulatów. Postulaty *de lege ferenda* są niejako ubocznym efektem prac, których wyniki prezentowane są w książce.

Przy omawianiu realizacji tego celu, podobnie jak pozostałych, nie powtarzam odpowiednich fragmentów pracy. Postulaty są umieszczone w miejscach do tego w pracy przeznaczonych. Celu tego nie uważam za istotny cel pracy, został on jednak zrealizowany niejako na uboczu realizacji celów podstawowych.

Realizacja celu:

„Drobiazgowa analiza

tekstu prawnego wybranych przepisów RODO"

Cel ten realizowany jest we wszystkich rozdziałach książki. Cel ten uważam za istotny cel książki, uważam bowiem, że analiza przepisów powinna być dokonywana w sposób, który mogę nazwać uczciwym. Uczciwa analiza przepisu – to moim zdaniem – właśnie analiza drobiazgowa. Cel ten – jak sądzę – został zrealizowany i to w trzech odsłonach.

Po pierwsze, przepisy zostały przeanalizowane z wykorzystaniem etapowej analizy semantycznej, która w swoją istotę ma wpisaną szczegółowość analizowania, będącego podstawą metody. Zastosowanie etapowej analizy semantycznej zagwarantowało realizację tego celu na poziomie niejako podstawowym.

Po drugie, tam gdzie dostrzegłem takie potrzeby, tam przeprowadziłem rozważania szczegółowe. Miejscami uzupełniają one wywody podstawowe, prowadzone w warstwie „Analiza", jednak głównie składają się one na kolejne podrozdziały warstwy „Uwagi".

Po trzecie, kolejne przepisy zostały przeze mnie niejako przetłumaczone na język praw i obowiązków. W ten sposób przyglądam się przepisom przez ten właśnie konkretny pryzmat oraz pozwalam, by i czytelnicy w ten sposób spojrzeli. Uważam, że ten właśnie sposób spojrzenia na przepis jest szczególnie wartościowy przy analizowaniu

RODO. Patrzymy na przepis i widzimy obowiązki administratora i prawa osób, których dane dotyczą. Na marginesie zwracam uwagę, że system składający się z praw i obowiązków służy ochronie odpowiadających tym prawom i tym obowiązkom, wolności. Szerzej zajmuję się tym w publikacji „*RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*”[363].

Realizacja celu:
„Prezentacja warstwowej metody tworzenia prac naukowych”

Cel ten realizowany jest w obydwu rozdziałach książki. Warstwowa metoda tworzenia prac naukowych ma na celu przede wszystkim wewnętrzne uporządkowanie pracy. Niniejsza praca jest piątą, (ewentualnie szóstą, tyle, że jednej z prac jeszcze nie wydano), a na pewno trzecią moją pracą, w której stosuję tę metodę. Na pewno trzecią, ponieważ jest to trzecia praca jednoautorska, w której metodę tę stosuję w sposób świadomy i konsekwentny. Stosowałem ją w jednej jeszcze książce, a mianowicie w książce poświęconej dokumentacji administratora na gruncie RODO[364].

W pracach prawniczych zjawiskiem normalnym jest prowadzenie rozważań po kolei. Rozważań dogmatycznych, analitycznych, teoretycznych, prawodawczych, historycznych, różnych. Różnych, zależnie od celu pracy, na pewno też zależnie od kompetencji autora lub autorów. Mimo prowadzenia rozważań w pewnej – każdorazowo przyjętej przez autora – kolejności bywa, że rozważania różnej natury przeplatają się ze sobą. Tekst taki wygląda atrakcyjnie, świadczy czasem o wielkiej wiedzy i naukowej erudycji autora, bywa jednak trudny w lekturze, zwłaszcza dla mniej kompetentnych czytelników. Rozdzielenie poszczególnych dziedzin rozważań pozwala nie tylko uporządkować wywód, ale nadaje mu pewną jasność oraz – co uważam za szczególnie doniosłe – ułatwia lekturę tak skomponowanej publikacji.

Publikacja jest na pewno autorskim zajęciem stanowiska w sprawach, którym jest ona poświęcona, mam jednak pełną świa-

[363] J. Rzymowski, *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje*, Łódź 2020.

[364] J. Rzymowski, *RODO – GDPR. Obowiązkowa dokumentacja…*

domość, że niedobrze byłoby, gdyby publikacja była pisana przez autora dla niego samego. Publikacja, przynajmniej niniejsza i inne z tej serii, pisana jest z myślą o Czytelnikach. Zajmuję tu stanowisko w konkretnych sprawach, jednak staram się czynić to w sposób zrozumiały i łatwo przyswajalny dla Czytelników.

Uważam że warstwowa budowa pracy czyni ją, między innymi, zrozumiałą dla różnych grup czytelników.

Czytelnik, zajmujący się praktyką ochrony danych, może być zainteresowany jedynie warstwą „Wnioski z analizy", ewentualnie również warstwą „Uwagi". Wielce kształcąca dla takiego czytelnika może być też lektura podrozdziałów warstwy „Podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa", ponieważ może uświadomić mu, że RODO dla administratora oznacza obowiązki. Warstwa oparta na konceptualizmie może być też interesującą lekturą dla teoretyka prawa. Warstwa „Analiza" może się okazać użyteczna dla administratora broniącego się przez zarzutami organu kontroli. Pewne rozważania zawarte w warstwie „Uwagi" również mogą być tu pomocne. Rozważania zawarte w podrozdziałach warstwy „Konkretyzacja zasad" mogą być zwłaszcza przydatne dla kogoś, kto przygotowuje dokumentację administratora na gruncie RODO. Dokumentacji poświęciłem osobną książkę[365] niniejszego cyklu, jednak właśnie z punktu widzenia tworzenia dokumentacji istotne jest, jakie zasady realizuje który przepis. Rozważanie niejako w przeciwnym kierunku przeprowadzone jest innej książce[366] z niniejszego cyklu, w której wskazuję, które przepisy którą zasadę realizują.

[365] Ibidem.

[366] J. Rzymowski, *RODO – GDPR. Zasady dotyczące...*

Cele pracy

Uwagi uzupełniające

Na początku pracy poczynione zostało kilka jeszcze uwag, które odnoszą się do celów pracy. Uwagi te poczyniłem we fragmencie, który znajduje się pod nagłówkiem: *Pozostając przy celach pracy, należy poczynić kilka jeszcze uwag***.**

Jeśli chodzi o realizację celu pracy rozumianego jako: „analiza przepisów RODO dotyczących bezpieczeństwa danych osobowych", to cel ten został w pracy zrealizowany, a na pewno został zrealizowany w takim zakresie, w jakim go założono na początku pracy. Przeanalizowane zostały art. 24, 32, 33 i 34 RODO. Analiza wskazanych przepisów przeprowadzona została w sposób możliwie dokładny przy zachowaniu spojrzenia analitycznego, dogmatycznego, teoretycznego i prawotwórczego. Zgodnie z założeniami poczynionymi na początku pracy, odniesienia do zasad mają charakter ograniczony, ponieważ zasadom została poświęcona inna książka[367] z niniejszego cyklu.

Jeśli chodzi o realizację celu rozumianego jako „stosowanie rygorów języka prawnego do języka prawniczego", to zgodnie z założeniami przyjętymi na początku pracy rozważania prowadzone w języku prawniczym głównie w warstwie „uwagi" prowadzone są przy zachowaniu pewnej dyscypliny, przejawiającej się we wprowadzaniu fragmentów tekstu prawnego między rozważania prowadzone w języku prawniczym, unikanie stosowania synonimów i innych rozwiązań stylistycznych, które może czynią tekst piękniejszym, ale na pewno czynią go mniej zrozumiałym.

Na początku pracy przyjąłem, że cel analityczno-badawczy realizowany jest w podrozdziałach warstwy „analiza". Cel ten został zrealizowany. Element analityczny celu pozwolił na sformułowanie podrozdziałów warstwy „komentarz", jak również na przeprowadzenie szczegółowych rozważań w podrozdziałach składających się na warstwę „uwagi", a w końcu nawet na postawienie postulatów nowelizacyjnych. Element badawczy najmocniej przejawia się w podrozdziałach warstwy „uwagi".

---

[367] Ibidem.

Na początku pracy przyjąłem, że cel porządkujący realizowany jest w podrozdziałach warstwy „komentarz" i warstwy „uwagi" oraz warstwy „podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa". Patrząc na wykonaną pracę, mogę stwierdzić, że cel ten zrealizowany został, zwłaszcza w podrozdziałach warstwy „komentarz" i w podrozdziałach warstwy „podsumowanie w duchu konceptualizmu prawniczego – ogólnej teorii prawa". Zwłaszcza w drugiej ze wskazanych warstw udało mi się – dzięki sprowadzeniu treści regulacji do wspólnego mianownika uprawnień i obowiązków – uzyskać wysoki stopień uporządkowania analizowanej materii. Cel porządkujący realizowany jest do pewnego stopnia również w warstwie „uwagi", a mianowicie tam, gdzie wśród uwag szczegółowych zamieszczam rozmaite, merytorycznie wynikające z danego przepisu, zestawienia. Dla ułatwienia korzystania z tych zestawień zostały one wypreparowane z podrozdziałów, których są fragmentami, a następnie zostały zamieszczone na końcu książki, przed częścią poświęconą realizacji celów pracy.

Cel projektujący zrealizowany został w podrozdziałach warstwy Postulaty *de lege ferenda*, Postulaty zostały postawione, w ograniczonym uznanym przeze mnie za konieczny zakresie. Więcej postulatów nowelizacyjnych stawiam w dwóch poprzednich książkach.

Zakończenie

Książka niniejsza poświęcona jest zjawisku ryzyka, a przez to i bezpieczeństwa w RODO. Nie chcę tu powtarzać i w związku z tym nie powtarzam wniosków cząstkowych, które postawiłem w toku książki, głównie w podrozdziałach warstwy „uwagi", oraz jako wnioski *de lege ferenda*. Myślę, że jest jednak jeden podstawowy wniosek, który wynika nie tyle z analizy poszczególnych przepisów, ile z kilku już lat kontaktu z przepisami, z ich interpretacjami i z praktyką. Otóż zarówno kwestie związane z oceną ryzyka na gruncie RODO, jak i kwestie związane z oceną skutków naruszenia na gruncie RODO są uregulowane niejasno. Nie jest to wniosek odkrywczy, uważam jednak, że daje on możliwość sformułowania pewnej konstatacji, wręcz wniosku z wniosku. Niejasność przepisów powoduje różne ich stosowanie, kiedy na to nałożymy kontrolną rolę organu ochrony danych, to okazuje się, że niejasność przepisów RODO godzi poważnie w pewność prawa i w zaufanie do prawa. Administratorzy (danych osobowych), którzy nie rozumieją przepisów RODO, mogą po prostu nie wiedzieć, czego się od nich oczekuje. Nie jestem socjologiem prawa, badań ilościowych nie prowadzę, ale obecność na rynku publikacji, takich jak ta, w których autorzy zastanawiają się na setkach stron, czym jest ryzyko, jak przeprowadzić ocenę ryzyka, jakie prawa i wolności brać pod uwagę, kiedy ma miejsce naruszenie ochrony danych osobowych oraz kiedy i komu je zgłaszać, jest dowodem, że wymienione tu zagadnienia nie są w przepisach opisane w sposób jasny.

I jeden jeszcze wniosek: otóż analiza przepisów, które dotyczą wymienionych tu zagadnień, po części postulaty nowelizacyjne, tabele mające ułatwić przeprowadzanie niektórych czynności, wskazują, że sprawy wyżej wymienione można uregulować prościej, a na pewno w sposób bardziej zrozumiały i tak właśnie powinno się to uczynić. Nieco wbrew sobie formułuję też pewną konstatację merytoryczną: otóż uważam, że w analizowanych przepisach RODO nie wybrzmiewa w sposób przekonujący, że ocena ryzyka i ocena skutków naruszenia powinny być przeprowadzane z wykorzystaniem analogicznych narzędzi. Że w obydwu przypadkach należy wziąć pod uwagę naruszenie tych samych praw i wolności, bo w przeciwnym przypadku, z punktu widzenia naruszenia ochrony danych osobowych, ocena ryzyka nie ma sensu. Że prawa i wolności, które należy brać pod uwagę przy ocenach prawodawca zapisał w art. 5 RODO i ewentualnie w prze-

pisach szczegółowych RODO, bo skoro one tak zapisane są, to nie służą dla ozdoby, są po to, by je brać pod uwagę. Że zarówno przy ocenie ryzyka, jak i przy ocenie skutków naruszenia ochrony danych osobowych należy brać pod uwagę zagrożenia wskazane w RODO, a to odpowiednio w art. 32 ust. 2 RODO i art. 4 pkt. 12 RODO. Uzasadnienie jest takie samo, jak poprzednie. Przepisy nie są dla ozdoby!

Wniosek o praktycznych trudnościach podejścia opartego na ryzyku formułuje D. Nowak[368]. Z wnioskiem tym się oczywiście zgadzam, jednak o ile oboje widzimy symptomy schorzenia, o tyle nie zgadzam się z sugestiami terapii tegoż, wysuniętymi przez wskazaną autorkę. Dominika Nowak postuluje *aktualizacje i doprecyzowanie wytycznych EROD*, rozwój kodeksów postępowania i wprowadzenie mechanizmów certyfikacji oraz znaków jakości i oznaczeń mających świadczyć o zgodności z RODO[369]. Zdaniem wskazanej autorki, kroki te powinny pomóc małym i średnimi przedsiębiorstwom[370]. W podobnym zrazu kierunku idzie myśl Ch. Poszwińskiego. Autor ten w nieostrym ujęciu *przez prawodawcę unijnego poszczególnych uprawnień osób, których dane dotyczą, oraz obowiązków administratorów i podmiotów przetwarzających* widzi narażenie podmiotu *danych na ryzyko naruszenia jego praw i wolności*[371]. Dalej autor wskazuje, które elementy RODO powinny zostać znowelizowane, po czym precyzuje, w jakich kierunkach poszczególne nowelizacje powinny zostać skierowane. Chrystian Poszwiński nie posuwa się do proponowania znowelizowanej treści odpowiednich przepisów RODO, choć miejscami wskazuje, co konkretnie powinno – jego zdaniem – zostać zmienione, jego wystąpienie nie pozostawia jednak wątpliwości, że intencją wskazanego autora jest, by przepisy RODO zostały znowelizowane.

O ile – jak piszę wyżej – z postawioną przez D. Nowak diagnozą się zgadzam, o tyle racjonalną terapię widzę w czym innym, tu bliższe jest mi stanowisko Ch. Poszwińskiego. Wytyczne EROD, kodeksy, certyfikaty, znaki – te rozwiązania oznaczają dalszą komplikację i rosnące koszty dla administratorów (danych osobowych).

---

[368] D. Nowak, op. cit., s. 40.

[369] Ibidem.

[370] Ibidem.

[371] Ch. Poszwiński, op. cit., s. 343–344.

Lekarstwo na chorobę niejasności, którą jest dotknięte RODO, jest inne. Przepisy RODO powinny zostać poprawione.

Bibliografia

Article 29 Data Protection Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679*. Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018. 18/EN. WP250. rev.01.

Barfield W., Pagallo U., *Advanced Introduction to Law and Artifficial Intelligence*. Cheltenham i Northampton Massachusetts 2020.

Barta P., Kawecki M., Litwiński P., [w:] P. Barta, D. Dörre-Kolasa, M. Kawecki, A. Krzyżak, P. Litwiński (red.). *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021.

Bielak-Jomaa E., Lubasz D., [w:] D. Lubasz (red.), *Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych*, Warszawa 2022.

Błahut M., *Pojęcie prawa podmiotowego we współczesnej liberalnej filozofii prawa.* „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2002, Rok LXIV, z. 1.

Bochenek M., *Ochrona danych osobowych w pomocy społecznej w pytaniach i odpowiedziach*, Lex, Warszawa 2019.

Bondy E., *Když jsem všecko napsal, zůstala mi kategorie procesu; ale co to je, ne-li prázdné slovo?*, [w:] E. Bondy. *Příběh o příběhu,* Praha 2009.

Bondy E., *Potíže z identitou protikladů: cesty k poznání však bývají nejen křivolaké, ale leckdy i pro smích; kdybych chtěl být učencem, byl bych toto líčeni raději přeskočil a předložil elegantni výsledek; zatím se jen ukázalo, že s dialektikou to bylo nějak vágní, [w:]* E. Bondy, *Příběh o příběhu,* Praha 2009.

Burton C., [w:] *The EU General Data Protection Regulation (GDPR). A Commentary.* Edited by Ch. Kuner, L.A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020.

Chomiczewski W., [w:] *RODO Ogólne rozporządzenie o ochronie danych. Komentarz,* red. n. E. Bielak-Jomaa, D. Lubasz. E. Bielak-Jomaa, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka, Warszawa 2018.

Ciemiński M., Magdziak M., [w:] D. Lubasz (red.), *Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych*, Warszawa 2022.

Cieślik A., *Ocena (szacowanie) ryzyka*, [w:] M. Jagielski (red.), *Dokumentacja ochrony danych osobowych ze wzorami*, Warszawa 2022.

Cook W.W., *Hohfeld's Contributions to the Science of Law*. "The Yale Law Journal", Jun., 1919, Vol. 28, No. 8 (Jun., 1919).
Stable URL: https://www.jstor.org/stable/787275

Docksey Ch., [w:] *The EU General Data Protection Regulation (GDPR). A Commentary.* Edited by Ch. Kuner, L.A. Bygrave, Ch. Docksey, and Assistant Editor L. Drechsler, Oxford 2020.

Dworkin R., *Biorąc prawa poważnie,* Warszawa 1998.

European Data Protection Board. Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021. Version 1.0.

Fajgielski P., *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*. WKP 2018 – Komentarz. Kom. do art. 24.

Fajgielski P., *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa 2019.

Gałęzowska K.., *Zgłaszanie naruszeń – omówienie nowych wytycznych EROD i problemów praktycznych*, [w:] *Działania instytucji i organów Unii Europejskiej w ochronie danych osobowych. Aktualne problemy ochrony danych osobowych 2021*, pod red. G. Sibigi. Dodatek specjalny do „Monitora Prawniczego" 2020, nr 23.

Gawroński M., Czarnowski A.P., Dominiak M., Gawron A., Gawroński M., Kibil M., Kloc K., Kunda K., Naklicka P., Piotrowska Z., Punda P., Sztąberek M., Wojtas M. (red.), *RODO przewodnik ze wzorami*, Warszawa 2018.

Gerloch A., *Teorie práva*, 8 vyd. Plzeň 2021.

Grupa Robocza art. 29, *Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679*. Przyjęte w dniu 3 października 2017 r. Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r. 18/PL WP250 rev.01.

Gumularz M., Izydorczyk T., [w:] M. Gumularz, T. Izydorczyk (red.). *Ochrona danych osobowych. Ocena ryzyka i skutków. Metody i praktyczne przykłady*, Warszawa 2021.

Hart H.L.A., *Pojęcie prawa*, Warszawa 1998.

Hohfeld W.N., *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, "The Yale Law Journal", Jun., 1917, Vol. 26, No. 8 (Jun., 1917).
Stable URL: https://www.jstor.org/stable/786270

Hohfeld W.N., *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, "The Yale Law Journal", Nov., 1913, Vol. 23, No. 1 (Nov., 1913). Stable URL: https://www.jstor.org/stable/785533

Izydorczyk T., [w:] *Ochrona danych osobowych. Ocena ryzyka i skutków. Metody i praktyczne przykłady*, red. M. Gumularz, T. Izydorczyk, Warszawa 2021.

Janowski J., *Informatyka prawa*, Lublin 2011.

Kaczmarek A., Młotkiewicz M., Łapińska A., Miłocha A., Mazur M., *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1.* Warszawa 2018.

Kaczmarek T., *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Warszawa 2008.

Kaczmarek A., Łapińska A., Miłocha A., Młotkiewicz M., *Nowa optyka w ocenie ryzyka*, „ABI Expert" 2017 4(5).

Kania R., *Ryzyko, czas i cudze prawa – proces ochrony danych*. „ABIEXPERT" 2018 nr 2(7), s. 34–36.

Kloza A., Calvi S., Casiraghi S., Vazquez Maymir, Ioannidis N., Tanas A. , Van Dijk N., Uściński P., Otmianowski M. (TRANS. 2021). *Szablon raportu z procesu oceny skutków dla ochrony danych w Unii Europejskiej: propozycja. d.pia.lab Policy Brief*. (1/2020).

Kasl F., *Porušení bezpečnosti osobních údajů w kontextu Internetu věcí*, Masarykova univerzita 2021.

Kokot‑Stępień P., *Identyfikacja ryzyka jako kluczowy element zarządzania ryzykiem w przedsiębiorstwie*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" nr 855, „Finanse, Rynki Finansowe, Ubezpieczenia" 2015/74, t. 1.

Kołodziej M., *Pseudonimizacja w RODO – kiedy i jak stosować*, „ABI Expert" 2018, nr 2(7).

Král Š., [w:] J. Pattynová, L. Suchánková, J. Černy, M. Růžička a kolektiv. Obecné nařizeni o ochraně osobnich údajů (GDPR) Zákon o zpracováni osobnich údajů. Komentář, Praha 2019.

Krasuski A., [w:] A. Krasuski, P. Siembida, *Analiza ryzyka w ochronie danych osobowych*, Warszawa 2022.

Litwiński P., Barta P., Kawecki M., [w:] P. Litwiński (red.) P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, s. 285.

Lubasz D., [w:] *RODO Ogólne rozporządzenie o ochronie danych. Komentarz*, red. nacz. E. Bielak-Jomaa, D. Lubasz, E. Bielak-Jomaa, W. Chomiczewski, M. Czerniawski, P. Drobek, U. Góral, M. Kuba, D. Lubasz, J. Łuczak, P. Makowski, K. Witkowska-Nowakowska, N. Zawadzka, Warszawa 2018, s. 105.

Malinowski A., *Polski tekst prawny. Opracowanie treściowe i redakcyjne,* Warszawa 2012.

Mazur M., *Zgłaszanie naruszeń ochrony danych*, „ABI Expert" 2018, nr 3(8).

Mednis A., *Pierwsza ocena i przegląd RODO – stanowiska zainteresowanych i główne elementy sprawozdania Komisji Europejskiej*, [w:] *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, pod. red. G. Sibigi. Dodatek specjalny do „Monitora Prawniczego" 2020, nr 23.

Morawski L., *Zasady wykładni prawa*, Toruń 2006.

Nowak D , *Podejście oparte na ryzyku w RODO w praktyce – wnioski po dwóch latach stosowania RODO*, [w:] *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*. pod. red. G. Sibigi. Dodatek specjalny do „Monitora Prawniczego" 2020, nr 23, s. 35.

Nuliček M., Donát J., Nonnemann F., Lichnovský B., Tomíšek. J., *GDPR / Obecné nařízení o ochraně osobních údajů. Prakticky komentař,* Praha 2017.

Nerka A., [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Nyquist C., *Teaching Wesley Hohfeld's Theory of Legal Relations*, „Journal of Legal Education", March/June 2002, Vol. 52, No. 1/2 (March/June 2002). Stable URL: https://www.jstor.org/stable/42893752.

Opałek K., Wróblewski J., *Zagadnienia teorii prawa*, Warszawa 1969.

PN-ISO/IEC 27005:2014-01. Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji.

Poszwiński Ch., *Podejście oparte na ryzyku w procesie przetwarzania danych osobowych*, Wrocław 2021.

Rzymowski J., *RODO – GDPR. Przedmiot i cele, zakresy, prawa i wolności, definicje,* Łódź 2020.

Rzymowski J., *RODO – GDPR. Zasady dotyczące przetwarzania danych osobowych. Zgodność przetwarzania danych osobowych z prawem*, Łódź 2020.

Rzymowski J., *RODO – GDPR. Obowiązkowa dokumentacja przetwarzania danych osobowych z punktu widzenia administratora*, Kraków 2019.

Rzymowski J. (red.), D. Spałek. *RODO – GDPR. Ochrona danych medycznych*, Łódź 2022.

Sakowska-Baryła M., [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Sibiga G., Małobęcka-Szwast I., Nowak D., Syska K., [w:] D. Lubasz (red.), *Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych*, Warszawa 2022.

Siembida P., [w:] A. Krasuski, P. Siembida, *Analiza ryzyka w ochronie danych osobowych*, Warszawa 2022.

Sobczyk A., *RODO. Rozproszona władza publiczna*, Kraków 2019.

Terelak Tymczyna A., *Zarządzanie bezpieczeństwem*, Szczecin 2014.

Twardowski K., *O filozofii średniowiecznej wykładów sześć,* Warszawa 1910.

Welenc P., [w:] B. Makowicz, B. Jagura (red.), *Systemy zarządzania zgodnością. Compliance w praktyce*, Warszawa 2020.

Wygoda K., [w:] M. Sakowska-Baryła (red.), B. Fischer, M. Górski, A. Nerka, K. Wygoda, M. de Bazelaire de Rupierre. *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz,* Warszawa 2018.

Wygoda K., [w:] M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej,* Wrocław 2018.

Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679. Przyjęte w dniu 4 kwietnia 2017 r. Ostatnio zmienione i przyjęte w dniu 4 października 2017 r. Grupa Robocza Art. 29. 17/PL WP 248 rev.01.

Ziembiński Z., *Logika praktyczna*, Warszawa 1995.

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

wydawnictwo.uni.lodz.pl
ksiegarnia@uni.lodz.pl
(42) 665 58 63

Książka dostępna również
jako e-book

ISBN 978-83-8331-244-6