ANALIZA RYZYKA I BEZPIECZEŃSTWO DANYCH W KANCELARIACH PRAWNYCH

redakcja naukowa Dominik Lubasz

Roman Bieda, Edyta Bielak-Jomaa, Witold Chomiczewski
Włodzimierz Chróścik, Marcin Ciemiński, Agnieszka Gajewska-Zabój
Maciej Gawroński, Jarosław Greser, Damian Karwala, Damian Klimas
Maciej Kołodziej, Dominik Lubasz, Michał Magdziak, Iga Małobęcka-Szwast
Arwid Mednis, Dominika Nowak, Robert Pająk, Marcin Rojszczak
Marlena Sakowska-Baryła, Grzegorz Sibiga, Paweł Skuczyński, Monika Susałko
Katarzyna Syska, Adam Szkurłat, Kamil Szpyt, Marcin Wielisiej, Tomasz Zalewski

PRAWO W PRAKTYCE

Wolters Kluwer

ANALIZA RYZYKA I BEZPIECZEŃSTWO DANYCH W KANCELARIACH PRAWNYCH

redakcja naukowa Dominik Lubasz

Roman Bieda, Edyta Bielak-Jomaa, Witold Chomiczewski
Włodzimierz Chróścik, Marcin Ciemiński, Agnieszka Gajewska-Zabój
Maciej Gawroński, Jarosław Greser, Damian Karwala, Damian Klimas
Maciej Kołodziej, Dominik Lubasz, Michał Magdziak, Iga Małobęcka-Szwast
Arwid Mednis, Dominika Nowak, Robert Pająk, Marcin Rojszczak
Marlena Sakowska-Baryła, Grzegorz Sibiga, Paweł Skuczyński, Monika Susałko
Katarzyna Syska, Adam Szkurłat, Kamil Szpyt, Marcin Wielisiej, Tomasz Zalewski

PRAWO W PRAKTYCE

Wolters Kluwer

WARSZAWA 2022

Stan prawny na 1 października 2021 r.

Recenzent
Dr hab. Dariusz Szostek, prof. UO

Wydawca
Monika Pawłowska

Redaktor prowadzący
Kinga Zając

Opracowanie redakcyjne
Anna Kunz

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

ISBN 978-83-8246-657-7 *ISBN PDF-a: 978-83-8246-969-1*

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

Część szczegółowa
Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych – wybrane zagadnienia szczegółowe

WYKAZ NAJWAŻNIEJSZYCH SKRÓTÓW

ENISA – Europejska Agencja Bezpieczeństwa Sieci i Informacji
EROD – Europejska Rada Ochrony Danych
k.c. – ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2020 r. poz. 1740 ze zm.)
k.k. – ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2020 r. poz. 1444 ze zm.)
k.p.c. – ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2021 r. poz. 1805 ze zm.)
k.p.k. – ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2021 r. poz. 534 ze zm.)
KEA – Kodeks Etyki Adwokackiej (obwieszczenie Prezydium Naczelnej Rady Adwokackiej z 27.02.2018 r. w sprawie ogłoszenia jednolitego tekstu Zbioru Zasad Etyki Adwokackiej i Godności Zawodu)
KERP – Kodeks Etyki Radcy Prawnego (załącznik do uchwały nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z 22.11.2014 r.)
pr. adw. – ustawa z 26.05.1982 r. – Prawo o adwokaturze (Dz.U. z 2020 r. poz. 1651 ze zm.)
RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz.Urz. UE L 119, s. 1)
SN – Sąd Najwyższy
TK – Trybunał Konstytucyjny
TSUE – Trybunał Sprawiedliwości Unii Europejskiej
u.r.p. – ustawa z 6.07.1982 r. o radcach prawnych (Dz.U. z 2020 r. poz. 75 ze zm.)
WSA – wojewódzki sąd administracyjny

SŁOWO WSTĘPNE

Konieczność wdrożenia systemu ochrony danych osobowych w kancelariach prawnych nie jest zagadnieniem nowym. Zobowiązania dotyczące tego obszaru wynikały pierwotnie z regulacji ustawy o ochronie danych osobowych z 1997 roku, a obecnie z obowiązującego od 25.05.2018 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, tzw. RODO). Realizacja tego zobowiązania napotyka jednak nadal istotne problemy, zwłaszcza w obszarze analizy ryzyka, przede wszystkim co do poprawności jej przeprowadzenia. Kancelarie prawne nie wykazują w tym zakresie znaczących odmienności niż pozostali uczestnicy obrotu należący do kategorii małych i średnich przedsiębiorców. Równocześnie istotnej modyfikacji ulega rynek usług prawnych, zarówno w obszarze organizacji procesów, jak i narzędzi, w tym wykorzystujących mechanizmy sztucznej inteligencji. Przyspieszenie transformacji cyfrowej w kancelariach prawnych, spowodowane czynnikami wywołanymi m.in. pandemią COVID-19, generuje nowe zagrożenia i zwiększa potencjalne ryzyko wymagające weryfikacji analitycznej i adekwatnego wdrożenia środków technicznych i organizacyjnych łagodzących to ryzyko.

Publikacji składa się z dwóch części. W pierwszej – przeglądowej – przedstawiono poszczególne aspekty analizy ryzyka, począwszy od uwag konstrukcyjnych i o charakterze ogólnym, zagadnień związanych z bezpieczeństwem, w tym w relacji z podmiotami przetwarzającymi, cyberbezpieczeństwem, zgodności ze standardami, perspektywę regulacji wewnątrzkorporacyjnych oraz analizę ryzyka jako element *compliance*

w kancelariach prawnych. W drugiej, szczegółowej części w dwunastu rozdziałach omówione zostały z perspektywy analizy ryzyka i bezpieczeństwa poszczególne sposoby przetwarzania danych w kancelariach i wykorzystywane narzędzia, począwszy od rozwiązań chmurowych, poczty elektronicznej, narzędzi do komunikacji i do obsługi kancelarii, przez platformy do kontraktowania się, narzędzia automatyzujące pracę prawnika, a skończywszy na wykorzystywaniu w pracy prawnika mediów społecznościowych, stron internetowych, IoT i sztucznej inteligencji.

W publikacji uwzględniono najnowsze rozstrzygnięcia Prezesa Urzędu Ochrony Danych Osobowych, w tym w zakresie administracyjnych kar pieniężnych, a także organów nadzorczych w innych państwach członkowskich oraz orzecznictwo sądów administracyjnych i Trybunału Sprawiedliwości UE. Uwzględniono także najnowsze decyzje Komisji Europejskiej dotyczące transferów danych do państw trzecich oraz standardowych klauzul umownych w umowach powierzenia przetwarzania danych. Omówiono również wytyczne Europejskiej Rady Ochrony Danych oraz organów samorządów zawodowych radców prawnych i adwokatów.

Publikacja łączy zagadnienia teoretyczne i konstrukcyjne z kwestiami praktycznymi, które są efektem przemyśleń wielu autorów.

Wkład w opracowanie niniejszej publikacji wniosło 27 autorów o rozległych kompetencjach merytorycznych z zakresu problematyki ochrony danych osobowych, *compliance*, jak również regulacji zawodów zaufania publicznego, będących zarówno praktykami, jak i przedstawicielami nauki.

Dziękuję im za zaangażowanie i podzielenie się z czytelnikami specjalistyczną wiedzą!

Liczę, że niniejsza publikacja *Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych* będzie ciekawą propozycją wydawniczą, dostarczającą czytelnikom, zwłaszcza przedstawicielom zawodów prawniczych wykonującym zawód w kancelariach prawnych, kompleksowej wiedzy dotyczącej analizy ryzyka i bezpieczeństwa danych, oraz ułatwiającą prawidłowe stosowanie przepisów regulujących tę materię.

Dominik Lubasz

Część ogólna

ANALIZA RYZYKA I BEZPIECZEŃSTWO DANYCH W KANCELARIACH PRAWNYCH – ZAGADNIENIA OGÓLNE

Rozdział 1

ANALIZA RYZYKA JAKO ELEMENT SYSTEMU OCHRONY DANYCH OSOBOWYCH W KANCELARIACH PRAWNYCH

1. Wprowadzenie

Konieczność wdrożenia systemu ochrony danych osobowych w kancelariach prawnych nie jest zagadnieniem nowym. Zobowiązania dotyczące tego obszaru wynikały pierwotnie z regulacji ustawy o ochronie danych osobowych z 1997 roku[1], a obecnie z obowiązującego od dnia 25.05.2018 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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), pomijając oczywiście regulacje zawodowe i kodeksy deontologiczne, obejmujące zagadnienie tajemnicy zawodowej, odnoszące się do atrybutu poufności określonych informacji, a zatem częściowo pokrywające się zakresowo z regulacją ochrony danych osobowych[2]. Zagadnienie to nadal jednak napotyka pewne przeszkody. Kancelarie prawne nie są w tym zakresie podmiotami znacząco odmiennymi od pozostałych uczestników obrotu, należąc do kategorii małych i średnich przedsiębiorców.

[1] Ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.).

[2] Na temat regulacji ochrony tajemnicy zawodowej oraz zasad etyki zawodowej zob. odpowiednio część ogólną, rozdziały 7 i 8 w niniejszej publikacji.

Edyta Bielak-Jomaa, Dominik Lubasz

Problemy wdrożeniowe wśród MŚP dostrzegła Komisja Europejska w raporcie podsumowującym 2 lata obowiązywania ogólnego rozporządzenia o ochronie danych[3]. W swym komunikacie Komisja Europejska wskazuje, że stosowanie RODO stanowi wyzwanie zwłaszcza dla małych i średnich przedsiębiorców[4]. Komisja zauważa wprawdzie podjęte przez krajowe organy ochrony danych działania wspierające MŚP w implementacji wymogów prawnych w obszarze ochrony danych osobowych, w tym opracowanie narzędzi ułatwiających wdrożenia przez tę kategorię przedsiębiorców, podkreśla jednak, że wysiłki te powinny zostać zintensyfikowane i rozpowszechnione, najlepiej w ramach wspólnego europejskiego podejścia[5]. Diagnozę tę potwierdzają badania przeprowadzone przez organizacje zrzeszające przedsiębiorców[6]. W raporcie przygotowanego przez D. Barnarda-Willsa, L. Cochrane, K. Matturiego i F. Marchettiego, Report on the SME experience of the GDPR, zaprezentowano diagnozę tego stanu rzeczy[7]. Autorzy badania skatalogowali główne czynniki stanowiące wyzwanie dla MŚP w związku z wdrażaniem ogólnego rozporządzenia danych, wskazując m.in. na:

1) koszty zapewnienia zgodności, zarówno pod względem finansowym, jak i zaangażowania innych zasobów, w tym czasu pracowników;

[3] Raport Komisji Europejskiej podsumowujący 2 lata stosowania ogólnego rozporządzenia o ochronie danych – Komunikat Komisji do Parlamentu Europejskiego i Rady, Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych, 24.06.2020 r. COM(2020) 264 final.

[4] Komunikat Komisji do Parlamentu Europejskiego i Rady, Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych, 24.06.2020 r. COM(2020) 264 final, s. 11.

[5] Komunikat Komisji do Parlamentu Europejskiego i Rady, Ochrona danych jako filar wzmacniania pozycji obywateli oraz podejścia UE do transformacji cyfrowej – dwa lata stosowania ogólnego rozporządzenia o ochronie danych, 24.06.2020 r. COM(2020) 264 final, s. 11.

[6] Np. General Data Protection Regulations survey (GDPR), ISME, 12.01.2018 r., https://isme.ie/report-businesses-unprepared-gdpr/; *2019 GDPR Small Business Survey,* https://gdpr.eu/2019-small-business-survey/ (dostęp: 20.08.2012 r.).

[7] Report on the SME experience of the GDPR, STAR II Deliverable D2.2, https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf (dostęp: 20.08.2021 r.), s. 31.

2) brak wiedzy specjalistycznej w zakresie ochrony danych oraz wysokość kosztów pozyskania doradztwa zewnętrznego, a także brak zaufania do kompetencji doradców zewnętrznych;
3) koszty i wyzwania związane z przeglądem istniejących i ustalonych praktyk oraz trudności ze zmianą codziennej rutyny i praktyk biznesowych w celu zachowania zgodności, w tym kultury organizacyjnej;
4) obawy związane z niepewnością oraz nadmierną ostrożność związaną z zagrożeniem wysokimi karami administracyjnymi;
5) błędne informacje na temat wymogów prawnych;
6) ograniczony dostęp do praktycznych wskazówek dotyczących interpretacji przepisów pozwalających na zrozumienie wymogów;
7) konserwatywne stosowanie wymogów dotyczących ochrony danych osobowych przez organy nadzorcze i dostrzegany brak spójności w UE;
8) konieczność zmiany podejścia do stosowania przepisów: z kazuistycznych wymogów prawnych na wymogi oparte na ryzyku, co powoduje trudności ze zrozumieniem, jakich zmian należy dokonać, aby zachować zgodność z przepisami[8].

Powyższe zagadnienia, stanowiące wyzwania dla MŚP przy wdrażaniu ogólnego rozporządzenia o ochronie danych, stanowią analogiczne wyzwania dla przedstawicieli zawodów prawniczych, z tym zastrzeżeniem, że środek ciężkości przesuwany jest w tym przypadku na zagadnienia pozaprawne, w szczególności dotyczące analizy ryzyka i zapewnienia bezpieczeństwa, a zatem przede wszystkim na kwestie wymienione w ostatnim z wymienionych punktów problemowych.

Nie ulega przy tym wątpliwości, że z perspektywy wdrażania wymogów ogólnego rozporządzenia o ochronie danych przedstawiciele zawodów prawniczych prowadzący działalność w formach spółek osobowych lub kancelarii jednoosobowych, o których mowa – odpowiednio – w art. 8 ust. 1 ustawy o radcach prawnych i art. 4a ust. 1

[8] Report on the SME experience of the GDPR, STAR II Deliverable D2.2, https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf (dostęp: 20.08.2021 r.), s. 31.

ustawy – Prawo o adwokaturze, są podmiotami zobowiązanymi, adresatami norm rozporządzenia, i choć adekwatnie do indywidualnego kontekstu związanego z przetwarzaniem przez nich danych osobowych, to jednak nie korzystają, co do zasady, ze zwolnień z obowiązków[9]. Obligatoryjne dostosowanie organizacji do wymogów ogólnego rozporządzenia o ochronie danych, przy założonej przez prawodawcę unijnego ogólnikowości regulacji i pozostawieniu decyzji wdrożeniowych w rękach administratora, pociąga za sobą szereg problemów praktycznych[10]. Zakres zmian prawnych, technologicznych i funkcjonalnych, które bezpośrednio oddziałują na codzienne życie organizacji w związku z ich większą odpowiedzialnością wobec osób, których dane dotyczą, wzmocnioną przez nowe przepisy oraz przeniesieniem odpowiedzialności z organów krajowych na organizacje zobowiązane do udowodnienia pełnej zgodności z przepisami, stanowi niebagatelne wyzwanie[11].

2. Założenia i cele regulacji

Rozporządzenie 2016/679 zastąpiło dotychczas obowiązującą dyrektywę 95/46/WE, a w konsekwencji również ustawę o ochronie danych osobowych z 1997 r., wprowadzając odmienny, proaktywny model ochrony, **oparty na podejściu bazującym na ryzyku** (*risk-based approach*). Odchodzi tym samym od sztywnych ram regulacyjnych i wyabstrahowanych od kategorii administratora, zakresu jego działania, zwłaszcza jego

[9] Poza opisanymi już, wynikającymi z art. 30 ust. 5 RODO i art. 4a u.p.k., art. 16a i 16b pr. adw., art. 5a i 5b u.p.r.

[10] J. Hashim, *Information communication technology (ICT) adoption among SME owners in Malaysia*, „International Journal of Business Information" 2007/2(2), s. 221–240, za: M. Brodin, *A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises*, „European Journal for Security Research" 2019/4, s. 244; H. Schulze, *GDPR compliance report*, https://crowdresearchpartner s.com/portfolio/gdpr-compliance-report/ (dostęp: 20.08.2021 r.).

[11] M. Brodin, *A Framework*…, s. 243–244; zob. także N. Fähnrich, M. Kubach, *Enabling SMEs to comply with the complex new EU data protection regulation* [w:] *Open Identity Summit 2019. Lecture Notes in Informatics (LNI)*, red. H. Roßnagel, Bonn 2019, s. 177.

związku z przetwarzaniem danych osobowych i skali tego przetwarzania, które były charakterystyczne dla polskiej ustawy o ochronie danych osobowych i rozporządzeń wykonawczych do niej, a zwłaszcza rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[12].

Rozwiązanie to miało na celu unowocześnienie regulacji, zapewnienie jej neutralności technologicznej, zniesienie zbędnych z perspektywy ochrony obciążeń administracyjnych, zniwelowanie negatywnych aspektów związanych z dotychczasowym wyborem środka legislacyjnego w postaci dyrektywy o minimalnym charakterze, a wreszcie związane było z dostrzeżeniem wartości danych osobowych w gospodarce i wpływu wykorzystania danych, w szczególności w aspekcie transgranicznym, na budowanie jednolitego rynku cyfrowego w UE.

Zgodnie z zamierzeniami prawodawcy unijnego ogólne rozporządzenie o ochronie danych ma zapewnić z jednej strony **wysoki poziom ochrony praw osób fizycznych**, z drugiej jednak poszerzyć możliwości wykorzystania danych poprzez **ułatwienie swobodnego przepływu danych osobowych na jednolitym rynku cyfrowym**.

Wskazywana neutralność technologiczna i skorelowane z tym podejście oparte na ryzyku przesunęło ciężar oceny adekwatności środków technicznych i organizacyjnych zmierzających do zapewnienia zgodności i bezpieczeństwa przetwarzania z prawodawcy na administratorów, dając im swobodę co do wyboru metod i środków, z wykorzystaniem których będą realizować cele i zadania związane z bezpieczeństwem informacji. Pokreślenia wymaga, że swoboda ta nie oznacza dowolności. Administratorzy muszą bowiem wykazać zgodnie ze sformułowaną w art. 5 ust. 2 RODO zasadą rozliczalności, że wdrażane środki są adekwatne do poziomu ryzyka o różnym prawdopodobieństwie i wadze, wynikającego lub mogącego wnikać dla praw i wolności podmiotów

[12] Dz.U. Nr 100, poz. 1024 ze zm.

danych w związku z przetwarzaniem danych osobowych. Zmieniono w związku z tym optykę rozwiązań, uelastyczniając podejścia i różnicując nakładane obowiązki zależnie od warunków konkretnego przetwarzania danych, różnych podmiotów przetwarzających i różnej jego skali oraz różnego charakteru samych danych. W kontekście przetwarzania danych osobowych w związku ze świadczenie pomocy prawnej istotne znaczenie będą miały m.in. aspekty dotyczące samego charakteru świadczonych usług, zakresu danych, zobowiązań płynących z regulacji zawodowych itp.

3. Podejście oparte na ryzyku

W koncepcji regulacyjnej rozporządzenia *risk-based approach* główną rolę odgrywa **szacowanie ryzyka, którego analiza stanowi istotny element**, a także dokonywany na tej podstawie przez administratora dobór środków technicznych i organizacyjnych mających na celu zapewnienie zgodności z rozporządzeniem. Ocena ta ma uwzględniać z jednej strony naturę, zakres, kontekst i cel przetwarzania danych, a z drugiej wynikające z tego ryzyka dla praw i wolności podmiotów danych. **Kluczowa jest zatem perspektywa podmiotu danych, a nie samego administratora**, o czym należy pamiętać, projektując rozwiązania adekwatne z punktu widzenia rozporządzenia.

Prawodawca unijny, odchodząc od sztywnych, nierelatywizowanych co do zakresu, potrzeb i zagrożeń ram ochrony, zdecydował się zrelatywizować i uelastycznić regulację przez uwzględnienie perspektywy podmiotów zobowiązanych, podkreślając jednocześnie jej **neutralny technologicznie charakter**. W konsekwencji to charakter, kontekst, cel i zakres przetwarzania danych osobowych przez konkretny podmiot jest podstawą oceny zgodności podjętej przez ten podmiot decyzji co do prawidłowego wdrożenia środków organizacyjnych i prawnych w celu zabezpieczenia praw i wolności osób, których dane są przetwarzane. Decyzja ta oparta jest na dokonanej przez te podmioty ocenie ryzyka związanego z przetwarzaniem danych (motyw 74).

Ważne
Pojęcie ryzyka nie zostało zdefiniowane w przepisach rozporządzenia ogólnego. Według ogólnych definicji ryzyko należy natomiast rozumieć jako zagrożenie lub szansę wystąpienia zdarzenia, które może pociągnąć za sobą możliwość wystąpienia zarówno negatywnych, jak i pozytywnych konsekwencji. W obrocie występują również definicje szczegółowe, np. zawarte w normach ISO. Dla przykładu w normie „ISO/IEC 31000. Zarządzanie ryzykiem. Zasady i wytyczne" **ryzyko jest definiowane jako wpływ niepewności na cele, który powoduje pozytywne lub negatywne odchylenie od oczekiwań**. Cele zaś mogą dotyczyć różnych aspektów, np. finansowych lub biznesowych. W doktrynie z kolei definiuje się **ryzyko jako scenariusz opisujący konkretne zdarzenie i jego konsekwencje (dla praw i wolności osób, których dane są przetwarzane), oszacowane pod kątem ich dotkliwości oraz prawdopodobieństwa**[13].

Prawodawca unijny nie tylko nie narzuca w przepisach rozporządzenia ogólnego, ale także nie proponuje metod analizy ryzyka. Tym samym wybór metody należy do administratora i zależny jest m.in. od jego możliwości organizacyjnych i finansowych, kontekstu przetwarzania danych, ekspozycji organizacji na ryzyka oraz związku głównego przedmiotu działalności z przetwarzaniem danych osobowych, a wreszcie osobistych preferencji.

[13] Zob. np. D. Lubasz [w:] *Meritum. Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020, s. 101, ale także na temat identyfikacji ryzyk M. Gumularz, T. Izydorczyk, *Ochrona danych osobowych. Ocena ryzyka i skutków. Metody i praktyczne przykłady*, Warszawa 2021; L. Kępa, *Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku*, Warszawa 2019; P. Litwinski, *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz,* Warszawa 2021, komentarz do art. 32, P. Mielniczek, *Ochrona danych osobowych od A do Z w 16 krokach*, Warszawa 2021; J. Młotkiewicz, *Analiza ryzyka przy udostępnianiu danych – wybrane zagadnienia*, „Informacja w administracji Publicznej" 2019/2; D. Nowak, *Podejście oparte na ryzyku w RODO w praktyce – wnioski po dwóch latach stosowania RODO,* dodatek MoP 2020/23; A. Rapcewicz, *Oddalenie skargi na decyzję PUODO, nakładającą pierwszą karę pieniężną w sektorze publicznym*, „Informacja w administracji Publicznej" 2020/4.

Ważne
Metody analizy ryzyka można podzielić na:
– jakościowe,
– ilościowe i
– mieszane[14].
Metoda jakościowa jest prostsza, tańsza i mniej sformalizowana, jednakże mniej precyzyjna. **Metody ilościowe** charakteryzują się większą szczegółowością i precyzją, dlatego częściej stosuje się je w przypadku poważnych typów ryzyka.

Wybór metody analitycznej zależy od administratora i powinien być dostosowany do potrzeb organizacji i wymogów, m.in. zapewnienia rozliczalności. Wsparcia przy wyborze metody analitycznej można szukać m.in. w:

1) wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych oraz pomagających ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, WP 248 rev.1;
2) opracowaniach polskiego organu nadzorczego: *Poradniki – Jak rozumieć podejście oparte na ryzyku* i *Jak stosować podejście oparte na ryzyku*;
3) normach ISO z rzędu 27000, w szczególności w normie ISO/IEC 27005. Technika Informatyczna. Technika bezpieczeństwa. Zarzadzanie ryzykiem w bezpieczeństwie informacji, stanowiącej rozszerzenie normy ISO/IEC 27001 – w zakresie dotyczącym bezpieczeństwa opartego na analizie ryzyka, z tym zastrzeżeniem, że na podstawie tych norm badane jest ryzyko związane z zapewnieniem bezpieczeństwa informacji, a nie ryzyko przetwarzania dla praw i wolności podmiotów danych;
4) normie ISO/IEC 27701:2019 Techniki bezpieczeństwa – Rozszerzenie do ISO/IEC 27001 i ISO/IEC 27002 – Zarządzanie informacjami o prywatności – wytyczne i wymagania;

[14] Polska norma PN-ISO/EIC 27005. Technika informatyczna. Technika bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji, s. 25.

5) normie ISO/IEC 29134:2017 Technika informatyczna, Techniki bezpieczeństwa, Wytyczne dotyczące oceny skutków dla prywatności, wraz z normami skorelowanymi 27000 – systemy zarządzania bezpieczeństwem informacji, 29100 – ramy prywatności;
6) opracowaniach ENISA: *Reinforcing trust and security in the area of electronic communications and online services. Sketching the notion of „state-of-the-art" for SMEs in security of personal data processings*, s. 31;
7) metodologii PIA (*privacy impact assessment*) opracowanej przez francuski organ nadzorczu CNIL, https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment[15] (dostęp: 20.08.2021 r.).

Istota szacowania ryzyka, którego elementem jest analiza ryzyka, została ujęta w motywie 83 rozporządzenia ogólnego, który stanowi, że w celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej i koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie.

Ważne
Na szacowanie ryzyka składa się:
– identyfikowanie ryzyka,
– analiza ryzyka,
– ocena poziomu ryzyka.

Zasadniczym celem szacowania jest określenie wartości aktywów informacyjnych, zidentyfikowanie zagrożeń, podatności, a także zabezpieczeń i ich wpływu na zidentyfikowane ryzyko, jak również możliwe następstwa, priorytety i kolejność uzyskanych typów ryzyka[16]. Szacowanie

[15] Szerzej zob. w części ogólnej rozdziały 2 i 6.

[16] Polska norma PN-ISO/EIC 27005. Technika informatyczna. Technika bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji, s. 20.

ryzyka powinno być przeprowadzone w oparciu o **jedną, z góry przyjętą przez administratora metodę, uwzględniającą wszystkie kryteria**, które powinny zostać wzięte pod uwagę przy ocenie ryzyka, oraz perspektywę podmiotów danych jako wymóg wyraźnie wynikający z przepisów ogólnego rozporządzenia o ochronie danych. Szacowanie ryzyka powinno mieć charakter **obiektywny**. Co więcej, zastosowana metoda analizy ryzyka i jej szacunkowe wyniki powinny zostać udokumentowane w taki sposób, aby podmiot niezależny, w szczególności organ nadzoru, mógł odtworzyć proces analityczny administratora oraz ocenić, czy dokonując analizy, administrator wziął pod uwagę niezbędne kryteria i okoliczności, w jaki sposób je ocenił i z jakiej przyczyny doszedł do określonych wniosków. **Dokumentowanie lub raportowanie** przeprowadzanej analizy powinno obejmować każdy jej etap, co umożliwia ocenę przeprowadzonej analizy pod kątem jej rzetelności i miarodajności. Tego rodzaju dokumentowanie pozwala także na wykazanie zgodności działania administratora z obowiązującą na podstawie art. 5 ust. 2 zasadą rozliczalności.

Podkreślenia wymaga, że analiza ryzyka zgodna z wymogami ogólnego rozporządzenia o ochronie danych powinna być przeprowadzana nie z perspektywy kancelarii, a z punktu widzenia praw i wolności osób, których dane dotyczą, oraz potencjału naruszenia tychże praw i wolności (motyw 75). Niemożliwe jest oderwanie oceny ryzyka od ustalenia potencjalnych skutków **wystąpienia ryzyka dla praw i wolności podmiotów danych**. Co więcej, na ryzyko o różnym prawdopodobieństwie i wagę wpływać może szereg okoliczności. W szczególności należy tu wskazać na:

- **rodzaj i ilość przetwarzanych danych**, jak również
- **kategorię osób, do których dane należą,** i
- **czynności podejmowane na danych**.

Do wzrostu ryzyka przyczynia się przetwarzanie szczególnych kategorii, zwanych danymi wrażliwymi, oraz danych dotyczących wyroków skazujących i czynów zabronionych, tj. danych, o których mowa w art. 9 ust. 1 i art. 10 RODO. Istotna wartość tych danych, wynikająca z faktu dotykania sfer o podwyższonej wrażliwości z perspektywy prywatności, wpływać będzie na wynikowy poziom ryzyka poprzez zwiększenie wagi

danych, co zwłaszcza w działaniu przedstawicieli zawodów prawniczych ma bardzo istotne znaczenie.

Np. Ryzyko naruszenia praw lub wolności osób może wynikać z przetwarzania danych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych (motyw 75), w szczególności:

1) jeżeli przetwarzanie może skutkować:
   - dyskryminacją,
   - kradzieżą tożsamości lub oszustwem dotyczącym tożsamości,
   - stratą finansową,
   - naruszeniem dobrego imienia,
   - naruszeniem poufności danych osobowych chronionych tajemnicą zawodową,
   - nieuprawnionym odwróceniem pseudonimizacji,
   - wszelką inną znaczną szkodą gospodarczą lub społeczną;
2) jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
3) jeżeli przetwarzane są dane osobowe ujawniające pochodzenia rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa;
4) jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych;
5) jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, zwłaszcza dzieci;
6) jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

Te ryzyka dla praw lub wolności podmiotów danych mogą wynikać z różnych czynników, w tym np. z umożliwienia nieuprawnionego dostępu do danych, nieuprawnionego odwrócenia pseudonimizacji, kradzieży tożsamości, naruszenia integralności danych. Identyfikacja samego

ryzyka oraz ocena prawdopodobieństwa jego wystąpienia i ustalenie, jaki w związku z tym jest wpływ przetwarzania na prywatność osoby, której dane dotyczą, należą do administratora. Powinny być one prowadzone na podstawie obiektywnej oceny i – co wynika z konstrukcji przepisów dotyczących obowiązków administratora – z perspektywy wyodrębnionych przez administratora procesów przetwarzania.

4. Obowiązki oparte na analizie ryzyka

Podejście oparte na ryzyku jest przede wszystkim istotnym elementem:
- ogólnego obowiązku zapewnienia zgodności z rozporządzeniem, o którym mowa w art. 24 RODO;
- uwzględniania ochrony danych już w fazie projektowania (*data protection by design*) w myśl art. 25 ust. 1 RODO oraz realizacji zasady domyślnej ochrony danych (*data protection by default*) zgodnie z art. 25 ust. 2 RODO;
- sporządzania określonej przepisami dokumentacji przetwarzania ujętej w ramy art. 30 RODO;
- zapewnienia bezpieczeństwa przetwarzania, w szczególności wskazanego w art. 32 RODO;
- oceny skutków planowanych operacji przetwarzania dla ochrony danych (*data protection impact assessment*) oraz uprzednich konsultacji z organem nadzoru, o których mowa odpowiednio w art. 35 i 36;
- oceny powagi naruszenia i obowiązków notyfikacyjnych z art. 33 i 34[17].

Przepis art. 24 ust. 1 RODO **ma charakter klauzuli generalnej**, określającej podstawowy i główny obowiązek podmiotu zobowiązanego, tj. administratora, czyli obowiązek zapewnienia zgodności z rozporządzeniem. Konstrukcja regulacji art. 24 jest przejawem przyjętej w RODO koncepcji neutralności technologicznej i oddania w ręce administratora decyzji co do adekwatności wdrażanych środków, bazującej na przeprowadzanej przez niego ocenie ryzyka.

[17] Odnośnie do tiret drugiego, czwartego, piątego i szóstego zob. część ogólną, rozdział 2.

Zgodnie z art. 24 RODO administrator zobowiązany jest – uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze – wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

Ocena adekwatności środków technicznych i organizacyjnych, które administrator powinien wdrożyć, musi uwzględniać **charakter, zakres, kontekst i cele przetwarzania** oraz **ryzyko naruszenia praw lub wolności osób fizycznych** o różnym prawdopodobieństwie i różnej wadze zagrożenia.

Np.

Charakter przetwarzania jest związany z oceną planowanych operacji przetwarzania. Uwzględnia zatem np. to, czy będą przetwarzane szczególne kategorie danych, w jaki sposób będzie przebiegał proces przetwarzania, jakie podmioty będą w nim zaangażowane, istotność procesu itp.

Zakres przetwarzania odnosi się z kolei przede wszystkim do aspektów ilościowych przetwarzania, tj. skali przetwarzania. Bierze się zatem pod uwagę zakres przetwarzanych danych osobowych, ilość przetwarzanych danych oraz podmiotów danych, których danych przetwarzanie dotyczy.

Kontekst przetwarzania nakazuje oceniać wszelkie okoliczności prawne i faktyczne przetwarzania. Przede wszystkim należy oceniać intensywność ingerencji w prywatność danego procesu przetwarzania danych, np. związanego z monitoringiem, przyjęte rozwiązania techniczne i dostępną technologię, okoliczności i sposób wykorzystywania założonego rozwiązania i relacji do pozostałych elementów ocennych, w tym celu przetwarzania, a także przesłanek legalizacyjnych. Relewantny może być również czas i długość przetwarzania.

Cel przetwarzania jest związany z realizacją zasady ograniczenia celu (art. 5 ust. 1 lit. b), zgodnie z którą dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Przez pryzmat celu przetwarzania następuje też prawidłowe wydzielenie ocenianych procesów przetwarzania.

Z generalnym obowiązkiem wynikającym z art. 24 ust. 1 **skorelowane zostały obowiązki szczegółowe** dotyczące m.in. uwzględniania ochrony danych już w fazie projektowania (*data protection by design*) – art. 25 ust. 1, domyślnej ochrony danych (*data protection by default*) – art. 25 ust. 2, dokumentacji przetwarzania – art. 30, a także bezpieczeństwa przetwarzania opartego na analizie ryzyka – art. 32, oceny skutków dla ochrony danych (*data protection impact assessment*) – art. 35 czy wreszcie uprzednich konsultacji z organem nadzoru – art. 36[18].

Warto również zwrócić uwagę, że zgodna z rozporządzeniem 2016/679 ochrona praw i wolności podmiotów danych w zakresie przetwarzania ich danych osobowych wymaga podjęcia odpowiednich środków nie tylko przy projektowaniu rozwiązań wymagających przetwarzania danych osobowych, ale i podczas całego procesu przetwarzania, aż do jego zakończenia. Jest to odzwierciedleniem woli zapewnienia wysokiego standardu ochrony w toku całego życia informacji o charakterze osobowym. Przeprowadzoną analizę ryzyka należy zatem ponawiać nie tylko w przypadkach zmian organizacyjnych w istniejących procesach czy wdrażania nowych czynności przetwarzania danych, ale również z góry zaplanować regularne testowanie i weryfikowanie poziomu adekwatność wdrożonych środków technicznych i organizacyjnych, by zachować ich aktualność.

Znaczenie podejścia opartego na ryzyku, a także adekwatności środków technicznych i organizacyjnych ocenianej z perspektywy ryzyk dla praw i wolności osób, jako podstawowych elementów obowiązków wdrożeniowych administratorów, podkreślone zostało przez Prezesa UODO w kolejnych decyzjach nakładających administracyjne kary pieniężne[19]. Prezes UODO zwrócił w nich uwagę m.in. na:

1) konieczność zapewnienia kompleksowości analizy ryzyka, tj. zmapowania wszystkich aspektów kluczowych wpływających na ryzyko naruszenia praw i wolności podmiotów danych,

[18] Szerzej zob. część ogólna, rozdział 2.

[19] Zob. decyzje: z 10.09.2019 r., ZSPR.421.2.2019; z 18.10.2019 r., ZSPU.421.3.2019; z 21.08.2020 r., ZSOŚS.421.25.2019; z 3.12.2020 r., DKN.5112.1.2020; z 11.02.2021 r., DKN.5130.2024.2020.

2) prawidłowość oceny adekwatności wdrażanych środków technicznych i organizacyjnych zarówno w stosunku do ryzyka o niskim poziomie, jak i do ryzyka o poziomie wysokim,
3) regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania,
4) rolę inspektora ochrony danych w kontekście przeprowadzania analizy ryzyka i oceny skutków dla ochrony danych,
5) powtarzające się uchybienia w zakresie prawidłowego dokumentowanie analizy ryzyka.

Ważne
Obowiązek prawny wykonywania analizy ryzyka w oparciu o przepisy art. 24, 25 i 32 RODO był również przedmiotem wykładni w orzecznictwie sądów administracyjnych. Zob. przykładowo:
– wyrok WSA w Warszawie z 26.08.2020 r., II SA/Wa 2826/19, LEX nr 3067899, w którym w kontekście art. 32 RODO wskazane zostało, że „(…) nie wymaga od administratora danych wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych. Taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różną wysokością", a także że „przyjęte środki mają mieć charakter skuteczny, w konkretnych przypadkach niektóre środki będą musiały być środkami o charakterze niwelującym niskie ryzyko, inne – muszą niwelować ryzyko wysokie, ważne jednak jest, aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka";
– wyrok WSA z 3.09.2020 r., II SA/Wa 2559/19, LEX nr 3077973, w którym wskazano, że „rozporządzenie 2016/679 wprowadziło podejście, w którym zarządzanie ryzykiem jest fundamentem działań związanych z ochroną danych osobowych i ma charakter ciągłego procesu. Podmioty przetwarzające dane osobowe zobligowane są nie tylko do zapewnienia zgodności z wytycznymi

ww. rozporządzenia poprzez jednorazowe wdrożenie organizacyjnych i technicznych środków bezpieczeństwa, ale również do zapewnienia ciągłości monitorowania poziomu zagrożeń oraz zapewnienia rozliczalności w zakresie poziomu oraz adekwatności wprowadzonych zabezpieczeń. Oznacza to, że koniecznością staje się możliwość udowodnienia przed organem nadzorczym, że wprowadzone rozwiązania, mające na celu zapewnienie bezpieczeństwa danych osobowych, są adekwatne do poziomu ryzyka, jak również uwzględniają charakter danej organizacji oraz wykorzystywanych mechanizmów przetwarzania danych osobowych. Administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka".

5. Przeprowadzanie i dokumentowanie analizy ryzyka

Dokumentacja ogólnej analizy ryzyka powinna ponadto obejmować wszystkie jej etapy, tj.:

1) identyfikowanie ryzyka,
2) analiza ryzyka,
3) ocenę poziomu ryzyka.

Dokumentowanie procesu analizy ma pozwolić na ocenę prawidłowości podjętej przez administratora (również wymagającej udokumentowania) **decyzji co do dalszego postępowania z ryzykiem**, a zatem tego, czy z uwagi na poziom ryzyka wymaga ono podjęcia decyzji co do jego **zmniejszenia, przeniesienia, uniknięcia** czy też **postawienia na określonym poziomie** jako akceptowalne, co jest związane z poziomem tzw. **apetytu na ryzyko, czyli poziomu akceptowalnego przez administratora**. W konsekwencji przekłada się to bowiem na ocenę i dobór adekwatnych środków technicznych czy organizacyjnych uwzględniających naturę, zakres, kontekst i cel przetwarzania danych oraz wynikające z tego ryzyka dla praw i wolności podmiotów danych (art. 24, 25, 32 RODO).

Europejska Rada Ochrony Danych w wytycznych 4/2019 dotyczących zastosowania wynikającej z art. 25 zasady *data protection by design* wskazuje ponadto, że centralnym elementem koncepcji wdrożeniowej RODO jest skuteczność. Wymóg skutecznego wdrożenia oznacza, że każdy środek powinien przynieść zamierzone rezultaty w zakresie przetwarzania projektowanego przez administratora z perspektywy podmiotu danych. Skuteczność konkretnych środków zależeć będzie zatem od kontekstu danego przetwarzania oraz oceny jego relewantnych elementów, które należy uwzględnić przy określaniu sposobów przetwarzania. Takie podejście powoduje jednak, że administratorzy powinni być w stanie wykazać, że zapewnili adekwatność, a wdrożone środki i zabezpieczenia przynoszą pożądany skutek w zakresie ochrony danych osobowych, minimalizując ryzyko dla podmiotów danych związane z planowanymi formami przetwarzania. W tym celu, jak podkreśla Europejska Rada Ochrony Danych, administrator może określić odpowiednie kluczowe wskaźniki efektywności lub przedstawić uzasadnienie swojej oceny skuteczności wybranych środków i zabezpieczeń, aby wykazać ich skuteczność, zgodnie z zasadą rozliczalności (art. 5 ust. 2)[20].

Ważne
Wdrożenie systemu ochrony danych osobowych z uwzględnieniem podejścia opartego na ryzyku wymaga zatem projektu opartego na cyklu Deminga ujmującego działania implementacyjne w logiczny porządek następujących po sobie czynności P-D-S-A (*Plan-Do-Study-Act*), z uwzględnieniem zasady rozliczalności poszczególnych etapów analizy ryzyka[21].

Kluczem do prawidłowej realizacji projektu wdrożeniowego jest pierwotne ustalenie pełnego kontekstu działania kancelarii, co pozwoli – poprzez mapowanie procesów – określić czynności przetwarzania danych

[20] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, przyjęte 20.10.2020 r. przez Europejską Radę Ochrony Danych, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (dostęp: 20.08.2021 r.), s. 7.

[21] Szerzej zob. część ogólną, rozdział 6.

osobowych według kryterium celu przetwarzania, np. czynności przetwarzania w HR, rekrutacji, świadczenia pomocy prawnej, obsługi dostawców itp.

Ważne
Czynności przetwarzania w rozumieniu art. 30 ust. 1 RODO to zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w **związku z celem, w jakim te czynności są podejmowane**. W przypadku rekrutacji pracowników jeden **cel będzie obejmował wiele cząstkowych operacji niewymagających szczegółowego ich opisywania w rejestrze, takich jak:** pozyskiwanie informacji o kandydatach z ofert nadesłanych w wyniku ogłoszenia, dokonywanie ich selekcji, uzyskiwanie dodatkowych informacji w ramach przeprowadzania wywiadów z wybranymi osobami, usunięcie danych osób, które nie zostały wskazane do zatrudnienia, itp. Przy wyodrębnianiu poszczególnych procesów (zespołów czynności) **zasadne jest uwzględnienie rzeczywistego podziału zadań pomiędzy poszczególnymi komórkami organizacyjnymi lub osobami w danej jednostce**. W dużych podmiotach, o złożonej strukturze organizacyjnej często wydziela się oddzielny zespół do spraw kadr i oddzielny do spraw płac[22].

[22] Prezes Urzędu Ochrony Danych Osobowych, Wskazówki i wyjaśnienia dotyczące rejestrowania czynności i kategorii przetwarzania określonego w art. 30 ust. 1 i 2 RODO, https://uodo.gov.pl/pl/123/214 (dostęp: 3.11.2021 r.).

Np.

Przykłady rejestrów

Rejestr czynności przetwarzania – przykład podstawowy

Rejestr czynności przetwarzania		
Dane administratora: [nazwa, adres siedziby]		
Dane Inspektora ochrony danych osobowych: [imię, nazwisko; adres siedziby] [jeżeli został wyznaczony]		
Osoba odpowiedzialna za aktualizację rejestru: [imię, nazwisko]		
1	Numer wpisu	
2	Nazwa procesu – czynności przetwarzania	
3	Cel przetwarzania danych w ramach procesu	
4	Opis procesu, w tym sposób pozyskiwania danych	
5	Podstawa prawna przetwarzania danych	
6	Kategorie osób, których dane dotyczą	
7	Opis kategorii danych osobowych	
8	Źródło danych	
9	Informacja o współ-administrowaniu w ramach procesu oraz dane kontraktowe współadministratora	
10	Informacja o podziale obowiązków między współ-administatorami	
11	Informacja o powierzeniu przetwarzania w ramach procesu i podmiotach przetwarzających	
12	Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane, niebędący podmiotami przetwarzającymi	

13	Terminy usunięcia danych w ramach procesu przetwarzanych	
14	Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego lub organizacji międzynarodowej oraz dokumentacji zabezpieczeń	
15	Ocena skutków dla ochrony danych, o ile została przeprowadzona wraz z odesłaniem do lokalizacji	
16	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (do weryfikacji po analizie ryzyka)	
17	Informacja na temat wykorzystywanych systemów teleinformatycznych	
18	Informacje dodatkowe, np. proces uprzednich konsultacji, zastosowanie kodeksu dobrych praktyk, certyfikacja	
19	Data wpisu / modyfikacji wpisu	
20	Data wykreślenia z rejestru	

Źródło: opracowanie własne.

Rejestr czynności przetwarzania – przykład rozbudowany

Nazwa procesu (czynność przetwarzania):	**Rekrutacja pracowników**	
Cel przetwarzania danych	*Opisać cel przetwarzania w procesie, np. wyłonienie spośród kandydatów na określone stanowisko osoby, która możliwie najdokładniej spełni oczekiwania administratora wobec przyszłego pracownika – pod kątem zarówno umiejętności, kompetencji miękkich, nastawienia do firmy, jak i oczekiwań finansowych.*	
Charakter przetwarzania danych	*Opisać planowane lub realizowane operacje przetwarzania, rodzaje danych osobowych, które mają być przetwarzane, w tym to, czy będą przetwarzane dane wrażliwe.*	
Podstawa przetwarzania	*Opisać podstawę przetwarzania, na której oparto proces.*	
Kategorie osób, których dane dotyczą	*Opisać zaangażowane w proces podmioty*, np.: • pracownicy obsługujący proces, • kontrahenci obsługujący proces oraz ich pracownicy, • kandydaci do pracy	
Zakres przetwarzanych danych według kategorii danych (*wskazano przykładowy zakres*)	Dane identyfikacyjne	• imię (imiona) i nazwisko; • imiona rodziców kandydata do pracy; • data urodzenia kandydata do pracy; • obywatelstwo kandydata do pracy
	Dane kontaktowe	• e-mail; • telefon kontaktowy; • adres zameldowania; • adres do korespondencji
	Dane dotyczące przebiegu kariery i wykształcenia, oczekiwań wobec pracodawcy	• wykształcenie (nazwa szkoły, rok ukończenia szkoły, zawód, specjalność, stopień naukowy, tytuł zawodowy, tytuł naukowy); • wykształcenie uzupełniające (kursy, studia podyplomowe, data ukończenia nauki); • przebieg dotychczasowego zatrudnienia (nazwa pracodawcy, stanowisko pracy, okres zatrudnienia od – do); • oczekiwania finansowe; • wyniki przeprowadzonych testów kompetencji

Nazwa procesu (czynność przetwarzania):	**Rekrutacja pracowników**	
	Dane dotyczące dodatkowych uprawnień i zainteresowań	dodatkowe uprawnienia, umiejętności, zainteresowania (np. stopień znajomości języków obcych, prawo jazdy, obsługa komputera)
	Dane dotyczące stanu zdrowia	stopień niezdolności do pracy (zdolny, grupa inwalidzka, niezdolność do pracy na czas określony, niezdolność do pracy na czas nieokreślony)
Kontekst przetwarzanych danych	*Opisać wszelkie okoliczności prawne i faktyczne przetwarzania. Przede wszystkim należy ocenić intensywność ingerencji w prywatność danego procesu przetwarzania danych, używanych narzędzi i dostępnej technologii, okoliczności i sposób wykorzystywania założonego rozwiązania i relacji do pozostałych elementów ocennych, w tym celu przetwarzania, a także przesłanek legalizacyjnych. Relewantne mogą również być czas i długość przetwarzania.*	
Kategorie odbiorców/ Odbiorcy danych	*Kategorie odbiorców ewentualnie konkretne podmioty, którym ujawniono lub zostaną ujawnione dane, w tym z państw trzecich.*	
Transfery danych	*Przekazanie danych do państw trzecich, ze wskazaniem podstawy oraz jeśli jest to przypadek, o którym mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń.*	
Retencja	*Opisać proces usuwania danych po osiągnięciu celu oraz procedurę ewentualnej zmiany celu.*	
Opis środków technicznych i organizacyjnych	*Opisać zabezpieczenia procesu, fizyczne, organizacyjne, osobowe, techniczne przez pryzmat poufności, integralności i dostępności.*	

Źródło: opracowanie własne.

Wydzielone czynności przetwarzania są podstawą konstrukcji rejestru czynności przetwarzania, który jest podstawowym obowiązkiem dokumentacyjnym nałożonym na administratorów przepisem art. 30 ust. 1 RODO. Zgodnie ze stanowiskiem Grupy Roboczej Art. 29 rejestr czynności jest **narzędziem mającym na celu zapewnienie realizacji zasad rozliczalności i przejrzystości** przetwarzania danych[23].

Ważne
Wydzielenie czynności przetwarzania jest istotne z perspektywy analizy ryzyka z uwagi na to, że analiza ryzyka i analiza zgodności są przeprowadzane właśnie dla poszczególnych czynności przetwarzania i to w ramach czynności przetwarzania administrator ocenia adekwatność wdrażanych środków technicznych i organizacyjnych, co ostatecznie odzwierciedla w rejestrze czynności przetwarzania, wskazując wdrożone środki (art. 30 ust. 1 lit. g RODO).

Ustalenie poszczególnych czynności przetwarzania umożliwi określenie i opisanie pełnego tła przetwarzania, w tym celu, zakresu, charakteru i kontekstu, jako czynników relewantnych dla analizy ryzyka w rozumieniu art. 24, 25, 32, 35 RODO. Do takich czynników należy określenie zapotrzebowania na dane, począwszy od zakresu, kategorii podmiotów danych, oznaczenia użytkownika i właściciela, a także dalszych podmiotów zaangażowanych w proces przetwarzania, tj. podmiotów przetwarzających i innych odbiorców. Z perspektywy funkcjonowania kancelarii prawnych ustalenia będą dotyczyć np. obiegu dokumentów, sposobu świadczenia pomocy prawnej, pracy zdalnej, wyboru narzędzi do obsługi kancelarii, zasad działania sekretariatu, wykorzystywanej infrastruktury IT itd.[24] Ustalenia kontekstowe muszą obejmować zarówno aspekty wewnątrzkancelaryjne, jak i relacje zewnętrzne, w których dochodzi do powierzenia przetwarzania danych osobowych (art. 28 RODO). Poczynione ustalenia mogą, ale nie muszą znaleźć to odzwierciedlenie

[23] Grupa Robocza Art. 29, *Kluczowe tematy z perspektywy trilogu*, http://www.giodo.gov.pl/pl/file/9537 (dostęp: 3.11.2021 r.).

[24] Poszczególne najistotniejsze elementy omówione zostały w części szczegółowej niniejszej publikacji.

w rejestrze czynności przetwarzania. Dokumentowanie ustaleń kontekstowych może następować również w dokumentacji analizy ryzyka. Prowadzenie rejestru w rozbudowanej formie, a zatem zawierającej elementy szersze niż tylko wynikające z art. 30 ust. 1 RODO, jest jednak operacyjnie korzystniejsze, pozwala bowiem na zaimplementowanie tego narzędzia do procesów analitycznych i na większą przejrzystość systemu.

Ważne
Dla wydzielonych i opisanych w powyższy sposób poszczególnych czynności przetwarzania (procesów przetwarzania) powinno nastąpić w dalszej kolejności **określenie wymagań** dotyczących ochrony danych i bezpieczeństwa informacji, zarówno przepisów ogólnych, jak i sektorowych, wytycznych, mających zastosowanie kodeksów postępowania, norm, w tym norm etycznych, oraz standardów.

Z perspektywy ogólnego rozporządzenia o ochronie danych osobowych na pierwszym planie znajduje się zapewnienie zgodności procesu przetwarzania danych osobowych ze sformułowanymi w art. 5 zasadami przetwarzania danych osobowych, tj. zasadą legalności, rzetelności i przejrzystości, zasadą ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności. Już na tym etapie analizy administrator swoją ocenę i decyzję co do sposobów zapewnienia zgodności będzie musiał zademonstrować zgodnie z zasadą rozliczalności, co powinien uwzględnić w procedurze zapewnienia zgodności poprzez tworzenie stosownej dokumentacji[25].

Równie istotne z perspektywy wymagań prawnych jest zagadnienie takiego zaprojektowania procesów przetwarzania, by zapewnić respektowanie praw podmiotów danych ujętych w art. 12–22 RODO[26]. Obejmuje to zarówno odpowiednie zaprojektowanie polityki

[25] Zob. szerzej P. Drobek [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, komentarz do art. 5, nb 5 i n., s. 325 i n.

[26] M. Susałko [w:] *Meritum. Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020, s. 230.

informacyjnej, co związane jest z koniecznością umożliwienia podmiotom danych zachowania kontroli nad ich danymi i możliwość reakcji, gdy ingerencja w prywatność jest przez nich nieakceptowana, jak i przygotowanie do wykonania wynikających z rozporządzenia szczegółowych uprawnień, tj. prawa dostępu do danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia, sprzeciwu.

Analiza zgodności w oparciu o wymogi z art. 24 RODO, w kontekście ryzyka dla praw i wolności podmiotów danych, obejmuje w szczególności zagadnienia sposobu udostępniania informacji z art. 13 i 14 RODO, używanego języka, pod kątem recepcji informacji w myśl art. 12 ust. 1 RODO, ułatwiania realizacji praw podmiotów danych (art. 12 ust. 2 RODO). Jest też elementem ocenianym przy legalizacji procesu przetwarzania przy ocenie np. świadomego wyrażania zgody czy też uzasadnionego oczekiwania określonych form przetwarzania w związku z wykonywaniem testu równowagi, będącego elementem przesłanki przetwarzania z art. 6 ust. 1 lit. f RODO.

Ważne
Prezes UODO w **decyzji** z 16.10.2019 r., ZSPR.421.7.2019, podkreślił, że naruszenie **art. 12 RODO** i sformułowanych w nim wymogów przejrzystości należy rozpatrywać w kontekście art. 24 RODO, co w konsekwencji prowadzić może do stwierdzania **niewdrożenia odpowiednich środków technicznych i organizacyjnych, które umożliwiałyby osobie, której dane dotyczą, skuteczne skorzystanie z jej praw**.

Niezbędnym elementem analizy ryzyka jest także ocena wpływu oraz ryzyka wynikającego z przetwarzania danych nie tylko pod kątem zgodności oddziałującej na prawa podmiotów danych, ale i bezpieczeństwa przetwarzania. Jest to związane z prawidłowym wdrożeniem zasady poufności i integralności uszczegółowianej przepisami art. 25 i 32 RODO[27].

[27] Szerzej o analizie ryzyka z perspektywy bezpieczeństwa przetwarzania zob. część ogólną, rozdział 2.

W zakresie bezpieczeństwa przetwarzania celem analizy ryzyka jest znalezienie adekwatnie dobranych środków mających na celu, aby dane osobowe były przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Ważne
Adekwatnie dobranymi środkami w rozumieniu art. 32 ust. 1 RODO są, jak wynika z wyroku WSA w Warszawie z 26.08.2020 r., II SA/Wa 2826/19, LEX nr 3067899, takie, które korespondują z poszczególnymi poziomami ryzyka, bowiem „niektóre środki będą musiały być środkami o charakterze niwelującym niskie ryzyko, inne – muszą niwelować ryzyko wysokie, ważne jednak jest, aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka".

Wymagania bezpieczeństwa będą określane poprzez identyfikację zagrożeń, które w poszczególnych procesach przetwarzania mogą wystąpić, oraz ryzyka dla podmiotów danych, jakie z tego mogą wynikać. Czynniki te wpływają na parametry wyboru odpowiednich i właściwych środków zabezpieczeniowych. W tym kontekście analiza ryzyka polega na zidentyfikowaniu potencjalnych konsekwencji różnych zdarzeń lub scenariuszy oraz na ocenie, jak prawdopodobne jest wystąpienie niepożądanego zdarzenia. Ocena ta dokonywana jest z perspektywy wpływu ryzyka na podmioty danych. Ponadto uwzględniać musi stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oddziaływujące na ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, a wynikające z przetwarzania z użyciem danego systemu. Elastyczność doboru danych środków limitowana jest zatem ich adekwatnością do potencjalnych ryzyk związanych z procesami przetwarzania, a zwłaszcza ich bezpieczeństwem. Poziom tolerancji powinien być zaś definiowany indywidualnie dla różnych scenariuszy bezpieczeństwa, procesów przetwarzania i kategorii obejmujących przypadkowe lub niezgodne z prawem zniszczenie, utratę, modyfikację, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych

osobowych[28]. Ma to istotne znaczenie zwłaszcza w procesach głównych związanych ze świadczeniem pomocy prawnej z uwagi na wrażliwości przetwarzanych danych, a ponadto standardy wynikające z regulacji korporacyjnych związanych z zapewnieniem tajemnicy zawodowej w kontekście poufności jako jednego z atrybutów bezpieczeństwa informacji.

Znaczenie adekwatności środków technicznych i organizacyjnych ocenianej z perspektywy ryzyk dla praw i wolności osób, podkreślone zostało przez Prezesa UODO w powołanych wyżej kolejnych decyzjach nakładających administracyjne kary pieniężne.

Niezależnie od powyższego, biorąc pod uwagę szczególnych zakres danych przetwarzanych w kancelariach prawnych oraz uwzględniając wymogi z art. 35 ust. 1, 3 i 4 RODO, w części przypadków obligatoryjne, a w pozostałych zalecane będzie przeprowadzenie oceny skutków dla ochrony danych (*data protection impact assessment*). Polega ona na oszacowanie wpływu, jaki przewidywana operacja przetwarzania może mieć na prawa i wolności osób fizycznych, których dane są lub będą wykorzystywane. Pogłębienie analizy w tym trybie jest jednym z elementów, które mogą być kluczem do udowodnienia spełniania zasady rzetelności, która – o czym była mowa – wymaga ograniczenia negatywnego wpływu przetwarzania na podmioty danych[29].

6. Rola inspektora ochrony danych w procesie analizy ryzyka

W przypadkach wyznaczenia inspektora ochrony danych, czy to z uwagi na zaistnienie w kancelarii przesłanki obligatoryjnego wyznaczenia na podstawie art. 37 ust. 1 RODO (przede wszystkim z art. 37 ust. 1 lit. c RODO), czy też fakultatywnego wyznaczenia, zwrócić należy uwagę na rolę inspektora w procesie analizy ryzyka, a w szczególności oceny

[28] Opracowanie norweskiego organu nadzorczego ds. ochrony danych osobowych, *Software development with Data Protection by Design and by Default*, https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true (dostęp: 20.08.2021 r.).

[29] Szerzej zob. część ogólną, rozdział 2.

skutków dla ochrony danych. W art. 39 ust. 1 RODO wyliczone zostały bowiem zadania inspektora ochrony danych obejmujące informowanie o obowiązkach dotyczących ochrony danych i doradzania w tym zakresie; monitorowanie przestrzegania przepisów o ochronie danych i polityk ochrony danych, podziału obowiązków, działań edukacyjne i audytów; udzielanie zaleceń co do oceny skutków dla ochrony danych i monitorowania jej wykonania; współpracę z organem nadzorczym; pełnienie funkcji punktu kontaktowego dla organu nadzorczego i prowadzenie konsultacji z organem nadzorczym. Wprawdzie przepis nie odnosi się wprost do analizy ryzyka, jednak zobowiązuje inspektora do wydawania na żądanie administratora zaleceń co do oceny skutków ochrony danych, która musi uwzględniać szacowanie ryzyka, elementem którego jest analiza ryzyka.

Inspektor, wykonując swoje zadania (art. 39 ust. 2 RODO), powinien stosować rozwiązania dostosowane do potrzeb podmiotów, w których pełni swoją funkcję, a także cech konkretnego przetwarzania danych i związanego z tym przetwarzaniem ryzyka. Konieczność realizacji obowiązków w powyższy sposób ma w konsekwencji prowadzić do skuteczniejszej ochrony danych. IOD musi zatem wykonywać swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Oznacza to konieczność indywidualnego i samodzielnego określania przez inspektora środków i metod działania oraz dostosowywania ich do specyfiki konkretnego administratora lub podmiotu przetwarzającego. Ułatwia to także doradzenie administratorowi wyboru metodologii stosowanej przy przeprowadzeniu analizy ryzyka i oceny skutków dla ochrony danych, jak również tego, które obszary powinny zostać poddane wewnętrznemu albo zewnętrznemu audytowi, jakie szkolenia wewnętrzne zaplanować i przeprowadzić dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych i na które operacje przetwarzania przeznaczyć więcej czasu i zasobów. Rzecz jasna, nie może to powodować zaniedbywania kontroli zgodności operacji przetwarzania danych o niższym ryzyku[30].

[30] Wytyczne dotyczące inspektorów ochrony danych (DPO), przyjęte 13.12.2016 r., zmienione i przyjęte 5.04.2017 r., https://uodo.gov.pl/pl/10/7 (dostęp: 20.08.2021 r.), s. 18.

Obowiązkiem inspektora ochrony danych jest informowanie administratora, podmiotu przetwarzającego i pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia 2016/679 oraz innych przepisów Unii lub państw członkowskich o ochronie danych oraz doradzanie im w tej sprawie (art. 39 ust. 1 lit. a). Realizacja tego zadania musi uwzględniać odrębności i specyfikę każdej kategorii podmiotów przetwarzających dane, bowiem na każdym z nich spoczywają inne obowiązki, z którymi może się wiązać inny zakres wymaganej w tej dziedzinie wiedzy.

Z punktu widzenia roli, jaką IOD odgrywa w procesie analizy ryzyka, powinien on wesprzeć administratora w dokonaniu takiej analizy oraz wskazać środki, których zastosowanie wpłynie na jego minimalizację. Inspektor może także pomóc administratorowi w doborze środków ochrony danych, adekwatnych do poziomu ryzyka. Rolę inspektora w przeprowadzaniu analizy ryzyka podkreślił Prezes UODO w decyzji w sprawie SGGW[31], w której stwierdził wprost, że obowiązkiem inspektora ochrony danych jest przeprowadzenie analizy ryzyka związanej z przetwarzaniem danych oraz wskazanie administratorowi konieczności jej przeprowadzenia. W powyższej sprawie Prezes UODO podkreślił, że kontrola przestrzegania przepisów o ochronie danych oraz procedur zawartych w politykach, w tym prowadzenie audytów związanych z operacjami przetwarzania, jest działaniem kilkuetapowym, obejmującym zbieranie informacji, analizowanie i sprawdzanie zgodności przetwarzania, informowanie, doradzanie i rekomendowanie określonych rozwiązań. W związku z tym, po pierwsze, istotne jest zbieranie informacji o podmiocie i stosowanych w nim procesach przetwarzania danych, w tym identyfikacja czynności przetwarzania danych, ustalenie aktywów wykorzystywanych do przetwarzania danych i zakresów danych, które są przetwarzane, wraz z ich kategoryzacją. Po drugie, konieczna jest analiza i ocena czynności przetwarzania w zakresie zgodności z przepisami RODO zarówno pod względem formalnoprawnym, jak i zgodności systemów informatycznych, po trzecie natomiast, opracowanie raportu i rekomendacji. Nie wyczerpuje wszystkich elementów audytu organizowanie szkoleń, formułowanie zaleceń, odbywanie spotkań

[31] ZSOŚS.421.25.2019.

z pracownikami czy przygotowywanie dokumentacji (w tym umów powierzenia, klauzul informacyjnych czy zgód podmiotów danych). Inspektorzy ochrony danych nie prowadzili także analiz i przeglądów w kontekście procesu przetwarzania danych osobowych kandydatów na studia w systemie informatycznym.

Dla rzetelnej analizy ryzyka dla ochrony danych wymagane jest jej przeprowadzenie z perspektywy całej organizacji i wszystkich okoliczności. Wydanie rzetelnego zalecenia wymaga bowiem zaangażowania nie tylko wiedzy IOD, ale również personelu oraz administratora. Inspektor przed wydaniem zalecenia może więc wykorzystać wszelkie dostępne kanały komunikacji i formy uzyskania wiedzy o zasobach danych i potencjalnych ryzykach. IOD na podstawie swojej wiedzy o organizacji, audytów, informacji pozyskiwanych w kontaktach z pracownikami biorącymi udział w procesie przetwarzania danych osobowych i współpracy z administratorem powinien móc wskazać metodę szacowania ryzyka, przedstawić ją i wnioski z tego procesu zebrać w formalną analizę ryzyka, dla wyników której opracuje zalecenia minimalizujące ryzyko.

Ważne
Realizując obowiązki informacyjne, inspektor powinien informować administratora o tym, czym jest analiza ryzyka, kiedy administrator powinien ja przeprowadzać, jakie są metody analizy ryzyka, gdzie może szukać wsparcia przy wyborze metody analitycznej, które obowiązki administratora oparte są na analizie ryzyka, jak również o konieczności udokumentowania procesu analizy ryzyka.

Dopełnieniem obowiązku informowania jest **obowiązek doradczy**, skoro zgodnie z art. 39 ust. 1 lit. a RODO na IOD ciąży zobowiązanie do doradzania w sprawie obowiązków wynikających z przepisów o ochronie danych osobowych. Oznacza to, że zarówno administrator, podmiot przetwarzający, jak i pracownicy mogą zwrócić się do inspektora o jego opinię w sprawach związanych z realizowaniem obowiązków ciążących na nich i wynikających z przepisów prawa, obejmujących swą materią regulacyjną ochronę danych. W motywie 77 wyjaśnione zostało,

że sugestie IOD dotyczące sposobu wdrożenia odpowiednich środków oraz sposobu wykazania przestrzegania prawa mogą w szczególności odnosić się do identyfikacji i oceny ryzyka.

Nierozerwalnie związany z powyższym jest obowiązek **monitorowania przestrzegania RODO**, innych przepisów unijnych lub krajowych o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty. Grupa Robocza Art. 29 wskazuje, że w ramach monitorowania IOD może podejmować szereg działań (m.in. zbierać informacje w celu identyfikacji procesów przetwarzania, analizować i sprawdzać zgodność tego przetwarzania, informować, doradzać i rekomendować określone działania administratorowi albo podmiotowi przetwarzającemu), których celem jest, po pierwsze, najpełniejsza wiedza o procesach przetwarzania danych, zagrożeniach, ryzykach z przetwarzaniem związanych, a po drugie, analiza sytuacji, i po trzecie, przedstawianie rekomendacji i opinii administratorowi lub podmiotowi przetwarzającemu[32].

Szczególnym zadaniem w kontekście analizy ryzyka jest udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania, zgodnie z art. 39 ust. 1 lit. c RODO.

Ważne
- Dokonywanie oceny skutków jest obowiązkiem administratora.
- Administrator, zgodnie z art. 35 ust. 2 RODO, ma obowiązek konsultowania się z IOD przy dokonywaniu oceny skutków dla ochrony danych.
- Obowiązkiem IOD jest udzielanie zaleceń na żądanie administratora.

[32] Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, przyjęte 4.04.2017 r., zmienione i przyjęte 4.10.2017 r., https://uodo.gov.pl/pl/10/9 (dostęp: 20.08.2021 r.), s. 17–18.

Grupa Robocza Art. 29 zaleca administratorowi konsultowanie z inspektorem m.in. kwestii dotyczących:
- konieczności przeprowadzenia oceny skutków dla ochrony danych;
- metodologii przeprowadzenia oceny skutków dla ochrony danych;
- decyzji, czy przeprowadzić wewnętrzną ocenę, czy też zlecić ją podmiotowi zewnętrznemu;
- zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
- prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z rozporządzeniem ogólnym (czy należy kontynuować przetwarzanie, czy też nie, oraz jakie zabezpieczenia należy zastosować).

Każdy z wykonywanych przez inspektora obowiązków powinien być działaniem podejmowanym we współpracy i na podstawie uzyskanych od administratora informacji, bowiem ostateczną decyzję dotyczącą postępowania z ryzykiem podejmuje administrator. Grupa Robocza Art. 29 rekomenduje, aby w sytuacji gdy administrator nie zgadza się z zaleceniami, dokumentacja oceny skutków dla ochrony danych zawierała pisemne uzasadnienie nieuwzględnienia tych zaleceń.

Rolę IOD w kontekście oceny skutków (w tym analizy ryzyka) podkreślił także Europejski Inspektor Ochrony Danych. W swojej opinii wskazał, że chociaż IOD jest zwykle najbardziej kompetentną osobą w organizacji w kontekście definiowania wymogów ochrony danych osobowych, to jednak jego rola w ramach oceny skutków może być wyłącznie konsultacyjna.

Inspektor ochrony danych nie może przeprowadzać oceny ryzyka (w tym oceny skutków). W szczególności nie on może podejmować wiążących decyzji w zakresie tego, jak należy postąpić ze zidentyfikowanym ryzykiem. IOD może natomiast pełnić rolę koordynatora procesu oceny skutków.

EIOD przypisał administratorowi rolę w zakresie m.in.:
- projektowania oceny skutków,
- weryfikacji, czy należy przeprowadzić uprzednie konsultacje.

Inspektorowi ochrony danych zaś rolę w zakresie m.in.:
- informowania administratora o jego obowiązkach w zakresie oceny skutków,
- konsultowania zakres procedur i projektu dokumentacji,
- doradzania administratorowi w procesie oceny skutków,
- koordynowania działań administratora w zakresie przeprowadzenia oceny skutków[33].

Ważne
Inspektorowi nie można narzucać sposobu interpretacji przepisów RODO. W ramach wypełniania zadań określonych w art. 39 nie może otrzymywać instrukcji dotyczących m.in. sposobu, w jaki określona spraw ma być rozpatrzona, środków, jakie mają zostać podjęte, celu, jaki powinien zostać osiągnięty, decyzji o współpracy z organem nadzorczym w konkretnej sprawie czy istnienia konieczności przeprowadzenia oceny skutków dla ochrony danych, metodologii przeprowadzenia oceny skutków dla ochrony danych, propozycji zabezpieczeń stosowanych do łagodzenia wszelkich zagrożeń, prawidłowości przeprowadzonej oceny skutków dla ochrony danych.

Podejmowana wyżej problematyka ma bardzo duży walor praktyczny, czego dowodem jest decyzja Prezesa Urzędu Ochrony Danych Osobowych w sprawie SGGW[34]. Postępowanie zakończone nałożeniem kary w wysokości 50 tys. zł. dotyczyło zgłoszenia naruszenia ochrony danych osobowych kandydatów na studia w Szkole Głównej Gospodarstwa Wiejskiego w Warszawie i związane było z kradzieżą przenośnego prywatnego komputera pracownika uczelni, który używał go również do celów służbowych, w tym do przetwarzania danych osobowych kandydatów na studia w SGGW na potrzeby czynności rekrutacyjnych w ramach pełnionej funkcji sekretarza Uczelnianej Komisji Rekrutacyjnej.

[33] *Accountability on the ground,* Part II: *Data Protection Impact Assessments & Prior Consultation*, s. 4–5, https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_2_en.pdf (dostęp: 20.08.2021 r.).

[34] ZSOŚS.421.25.2019.

Prezes Urzędu zarzucił uczelni, że nie wdrożyła odpowiednich środków organizacyjnych i technicznych, które zapewniałyby bezpieczeństwo przetwarzania danych osobowych kandydatów na studia, nie wykonała analizy ryzyka oraz że inspektor ochrony danych wypełniał swoje zadania bez należytego uwzględnienia ryzyka związanego z operacjami przetwarzania. IOD nie był angażowany przez uczelnię w proces rekrutacji na studia obejmujący funkcjonowanie systemu informatycznego przeznaczonego do tego działania. Prezes UODO stwierdził w tym kontekście, że inspektor ochrony danych nie przeprowadzał analizy ryzyka związanej z przetwarzaniem danych osobowych kandydatów na studia w SGGW. Nie informował on też o konieczności jej sporządzenia przez rektora SGGW czy kierownika Biura Spraw Studenckich, który zgodnie ze strukturą organizacyjną uczelni odpowiada proces rekrutacji na studia w SGGW.

Jak podkreślił Prezes UODO, wszelkie działania administratora mają na celu zapewnienie ochrony danych osobowych na płaszczyźnie nie tylko formalnej, ale i praktycznej. Oznacza to, że procedury muszą zostać nie tylko wprowadzone, ale także stosowane, gdyż w przeciwnym razie powoduje to niezgodność z rozporządzeniem 2016/679. Z materiału zgromadzonego w toku kontroli, jak również wyjaśnień złożonych w toku postępowania administracyjnego, nie wynikało, by administrator wdrożył te procedury. A choć RODO nie precyzuje, jak należy prowadzić ocenę ryzyka i dokumentować proces zarządzania ryzykiem, to administrator ma obowiązek wykazać, że ryzyko to zostało oszacowane w sposób rzetelny i obiektywny oraz że wprowadzono odpowiednie środki ochrony. Służyć temu może dokumentowanie przeprowadzonej analizy ryzyka i innych działań podjętych w celu zapewnienia zgodności z przepisami rozporządzenia.

Konkludując, należy stwierdzić, że obowiązkiem administratora danych jest wdrożenie środków technicznych i organizacyjnych, które uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, jak również ryzyko naruszenia praw lub wolności osób fizycznych, zapewnią stopień bezpieczeństwa odpowiadający temu ryzyku. Oznacza to, że musi także uwzględniać rolę wyznaczonego inspektora ochrony danych w minimalizowaniu tych ryzyk.

Powinien więc nie tylko wyznaczyć do pełnienia tej funkcji osobę kompetentną o fachowej wiedzy, odpowiednich, z punktu widzenia charakteru i sytuacji oraz potrzeb administratora, kwalifikacjach oraz doświadczeniu i wspierać ją w pełnieniu zadań, ale także włączyć ją w sposób prawidłowy i niezwłocznie we wszystkie sprawy dotyczące ochrony danych, w tym w proces szacowania ryzyka. Jest to zadanie administratora i nie może być przeniesione przez IOD, jednak administrator, realizując je, ma obowiązek konsultowania się z inspektorem ochrony danych, jeżeli został on wyznaczony. Jest to przejaw realizacji faktycznego realizowania m.in. funkcji doradczej inspektora.

7. Podsumowanie

Rzetelnie przeprowadzona analiza ryzyka może w zasadniczy sposób przyczynić się do ograniczenia naruszeń w procesach przetwarzania danych osobowych. RODO daje administratorowi lub podmiotowi przetwarzającemu pewną swobodę co do wyboru środków i metod ochrony danych. Jednym z takich mechanizmów jest szacowanie ryzyka właściwego dla przetwarzania oraz dostosowania do niego i wdrożenia środków minimalizujących to ryzyko. Złożoność procesów zarządzania informacjami, implementacja metodyk szacowania ryzyka dla ochrony danych osobowych do istniejących systemów zarządzania ryzykiem jest niezbędna. Wymaga ona pogłębionej refleksji i wiedzy administratora co do celów, sposobów, możliwości technicznych i organizacyjnych przetwarzania danych oraz woli i uwagi w zakresie wyboru adekwatnego i odpowiedzialnego modelu zarzadzania ryzykiem w organizacji. Przeprowadzenie analizy ryzyka pozwala na identyfikację potencjalnych zagrożeń oraz podjęcie racjonalnej decyzji co do postępowania w przypadku jego wystąpienia. Jedną z kluczowych ról w tym procesie odgrywa inspektor ochrony danych. Administrator co prawda nie może scedować odpowiedzialności za realizację tego zadania na wyznaczonego inspektora ochrony danych, jednak zobowiązany jest zasięgać jego opinii, zwłaszcza w zakresie DPIA, co znajduje wyraz w treści art. 35 ust. 2 RODO, który wskazuje, że „dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony". Obowiązek przeprowadzenie oceny

skutków może jednak występować niezależnie od konieczności wyznaczenia inspektora.

Literatura

Andrzejewska-Czernek I., *Wykładnia prawa podatkowego Unii Europejskiej*, Warszawa 2013

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Kraków 2004

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016

Bielak-Jomaa E., Lubasz D. (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016

Bielak-Jomaa E., Lubasz D. (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018

Bierć A., *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce – aspekty cywilnoprawne* [w:] *Ochrona danych osobowych (zbiór referatów wygłoszonych na poświęconej problematyce ochrony danych osobowych konferencji naukowej w dniach 27–28 II 1998 r.)*, red. M. Wyrzykowski, Warszawa 1999

Biernat S., *Źródła prawa Unii Europejskiej* [w:] *Prawo Unii Europejskiej*, red. J. Barcz, Warszawa 2004

Brodin M., *A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises*, „European Journal for Security Research" 2019/4

Buchner B., Kühling J. (red.), *DS-GVO. Datenschutz-Grundverordnung. Kommentar*, München 2017

Buchner B., Küchling J. (red.), *Datenschutz-Grundverordnung. Bundesdatenschutzgesetz: DS-GVO BDSG. Kommentar*, München 2018

Cisek R., Jezioro J., Wiebe A., *Dobra i usługi informacyjne w obrocie gospodarczym*, Warszawa 2005

Dörre-Kolasa D. (red.), *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu i Rady (UE) 2016/679*, Warszawa 2017

Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2007

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych. Komentarz,* Warszawa 2018

Fähnrich N., Kubach M., *Enabling SMEs to comply with the complex new EU data protection regulation* [w:] *Open Identity Summit 2019. Lecture Notes in Informatics (LNI)*, red. H. Roßnagel, Bonn 2019

Flaga-Gieruszyńska K., Gołaczyński J., Szostek D. (red.), *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane,* Warszawa 2019

Flaga-Gieruszyńska K., Gołaczyński J., Szostek D. (red.), *Media elektroniczne. Współczesne problemy prawne*, Warszawa 2016

Gawroński M. (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa 2018

Gawroński M., Gnatowska A., *Duża skala według estońskiego DPA* [w:] *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, red. M. Gawroński, Warszawa 2018

Gołaczyński J. (red.), *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2009

Gudowski J. (red.), *Kodeks cywilny. Komentarz. Księga pierwsza. Część ogólna*, LEX 2014

Gumularz M., Izydorczyk T., *Ochrona danych osobowych. Ocena ryzyka i skutków. Metody i praktyczne przykłady*, Warszawa 2021

Gumularz M., Kozik P., *Ochrona danych osobowych. Kontrola i postępowanie w sprawie naruszenia przepisów. Poradnik ze wzorami*, Warszawa 2019

Gumularz M., Kozieł K., Kozik P. (red.), *Ustawa o ochronie danych osobowych. Przepisy wdrażające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). Komentarz*, Warszawa 2018

Hashim J., *Information communication technology (ICT) adoption among SME owners in Malaysia*, „International Journal of Business Information" 2007/2(2)

Jagielski M. (red.), *Dokumentacja ochrony danych osobowych ze wzorami,* Warszawa 2019

Jagiełło-Jaroszewska E., Jarmużek D., Zawadzka-Filipczyk P., *RODO. Ochrona danych osobowych w stosunkach pracy*, Warszawa 2018

Kępa L., *Bezpieczeństwo danych osobowych. Podejście oparte na ryzyku*, Warszawa 2019

Kępa L., *Ochrona danych osobowych. Praktyczny przewodnik dla przedsiębiorców*, Warszawa 2018

Ehmann E., Selmayrred M. (red.), *Datenschutzgrundverordnung. Kommentar*, München 2017

Kluska M., Koszewicz K., Leśniewski G., Wanio G., *Ochrona danych osobowych w działaniach kadr. Odpowiedzi na 370 najtrudniejszych pytań,* Wrocław 2014

Kołyszko A., Dyrberg P., *Zasada autonomii proceduralnej w prawie Unii Europejskiej i jej ograniczenia w praktyce*, http://www.temidium.pl/artykul/zasada_autonomii_proceduralnej_w_prawie_unii_europejskiej_i_jej_ograniczenia_w_praktyce-957.html#_ftnref23 (dostęp: 20.08.2021 r.)

Konarski X., *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004

Kot D., *Dyrektywa Unii Europejskiej o handlu elektronicznym i jej implikacje dla prawa cywilnego*, „Kwartalnik Prawa Prywatnego" 2001/1

Kowalik-Bańczyk K., *Procedural Autonomy of Member States and the EU Rights of Defence in Antitrust Proceedings*, „Yearbook of Antitrust and Regulatory Studies" 2012/5(6)

Krasulski A., *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018

Kuner Ch., Bygrave L.A., Docksey Ch., *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford 2020

Litwiński P., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Legalis

Litwiński P. (red.), *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2018

Litwinski P., *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021

Litwiński P. (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018

Lubasz D., *Charakter prawny polecenia i upoważnienia*, „ABI Expert", lipiec–wrzesień 2019, nr 3

Lubasz D., *Handel elektroniczny. Bariery prawne*, Warszawa 2013

Lubasz D. (red.), *Meritum. Ochrona danych osobowych*, Warszawa 2020

Lubasz D. (red.), *RODO dla małych i średnich przedsiębiorstw,* Warszawa 2018

Lubasz D. (red.), *RODO w e-commerce*, Warszawa 2018

Lubasz D., Namysłowska M. (red.), *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, Warszawa 2011

Lubasz D., Sęczkowski D., *Nowe europejskie przepisy o ochronie danych osobowych – przygotowania do wdrożenia czas zacząć*, „Compliance. Magazyn fachowy Instytutu Compliance" 2016/3

Marcinkowski B., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018

Materna G., *Pojęcie przedsiębiorcy w polskim i europejskim prawie ochrony konkurencji*, Warszawa 2009

Mednis A., *Cechy zgody na przetwarzanie danych osobowych w opinii Grupy Roboczej Art. 29 dyrektywy 95/46 Nr 15/2011 (WP 187)* [w:] *Aktualne problemy prawnej ochrony danych osobowych*, red. G. Sibiga, „Monitor Prawniczy" 2012/7 – dodatek

Mednis A., *Ochrona prawna danych osobowych a zagrożenia prywatności – rozwiązania polskie* [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999

Mednis A., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2001

Mędrala M., *RODO. Ochrona danych osobowych w zatrudnieniu. Ze wzorami*, Warszawa 2018

Miąsik D., *Zasada efektywności prawa wspólnotowego* [w:] *Stosowanie prawa Unii Europejskiej przez sądy*, red. A. Wróbel, Kraków 2005

Miąsik D., *Zasada pierwszeństwa prawa wspólnotowego przed prawem krajowym*, EPS 2005, nr 1;

Młotkiewicz J., *Analiza ryzyka przy udostępnianiu danych – wybrane zagadnienia*, „Informacja w administracji Publicznej" 2019/2

Nowak D., *Podejście oparte na ryzyku w RODO w praktyce – wnioski po dwóch latach stosowania RODO*, dodatek MoP 2020/23

Paal B.P., Pauly D.A., *Datenschutz-Grundverordnung. Bundesdatenschutzgesetz: DS--GVO BDSG. Kommentar*, München 2018

Podrecki P. (red.), *Prawo Internetu*, Warszawa 2007

Rapcewicz A., *Oddalenie skargi na decyzję PUODO, nakładającą pierwszą karę pieniężną w sektorze publicznym*, „Informacja w administracji Publicznej" 2020/4

Schulze H., *GDPR compliance report*, https://crowdresearchpartner s.com/portfolio/gdpr-compliance-report/ (dostęp: 20.08.2021 r.)

Sibiga G., *Przetwarzanie i ochrona danych osoby ubiegającej się o zatrudnienie w świetle przepisów prawa pracy*, „Radca Prawny" 2005/2

Sibiga G., Syska K., *Ogólne rozporządzenie o ochronie danych. Podręczny zbiór przepisów o ochronie danych osobowych, zestawień, schematów oraz wzorów rejestru czynności przetwarzania*, Warszawa 2017

Szymielewicz K., *Nowa filozofia w ochronie danych osobowych: od oceny ryzyka do spójnej strategii w organizacji*, https://panoptykon.org/sites/default/files/publikacje/panoptykon_rodo_praktyczny_poradnik_22.01.2018.pdf (dostęp: 20.08.2021 r.)

Wróbel A., *Autonomia proceduralna państw członkowskich. Zasada efektywności i zasada efektywnej ochrony sądowej w prawie Unii Europejskiej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2005/1

Żołyński J., *RODO. Prawo do zapomnienia w sferze zatrudnienia*, Warszawa 2018

Rozdział 2

ANALIZA RYZYKA JAKO ELEMENT BEZPIECZEŃSTWA PRZETWARZANIA DANYCH W KANCELARIACH PRAWNYCH

1. Wprowadzenie

Przeprowadzanie analizy ryzyka w kancelarii prawnej stanowi nieodłączny element zapewnienia bezpieczeństwa danych osobowych. Bezpieczeństwo informacji, w tym danych osobowych, należy rozumieć jako zachowanie następujących atrybutów informacji:

- poufności, czyli zapewnienia, że informacja jest dostępna wyłącznie dla uprawnionych osób,
- integralności, czyli zapewnienia kompletności i dokładności informacji oraz metod przetwarzania,
- dostępności, czyli zapewnienia, że osoby upoważnione mają dostęp do potrzebnych im informacji i aktywów zawsze wówczas, gdy te informacje lub aktywa są im niezbędne.

W oparciu o tę definicję zapewnienie bezpieczeństwa danych osobowych przez kancelarię prawną sprowadza się do zapewnienia poufności, integralności i dostępności danych osobowych – zarówno tych związanych z prowadzonymi sprawami (w szczególności danych klientów), jak i danych osobowych dotyczących pracowników i współpracowników kancelarii.

Grzegorz Sibiga, Iga Małobęcka-Szwast, Dominika Nowak, Katarzyna Syska

W niniejszym rozdziale analiza ryzyka jako element bezpieczeństwa przetwarzania danych osobowych została przedstawiona w oparciu o obowiązki administratora określone w następujących przepisach: art. 24–25 oraz art. 32–36 RODO.

2. Podejście oparte na ryzyku

Zanim zostanie omówiona analiza ryzyka jako element bezpieczeństwa, należy określić, czym jest zasada podejścia opartego na ryzyku i czemu ma służyć. Zasada podejścia opartego na ryzyku została wprowadzona w art. 24 ust. 1 zdanie pierwsze RODO. Zgodnie z tym przepisem administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Szczegółowo kwestia podejścia opartego na ryzyku oraz cel jej wprowadzenia zostały szczegółowo omówione w rozdziale 1 części ogólnej niniejszej publikacji.

3. Rozwinięcie zasady podejścia opartego na ryzyku i jej wpływ na bezpieczeństwo danych osobowych

Zasada podejścia opartego na ryzyku z art. 24 RODO znajduje rozwinięcie w obowiązkach administratora, które są elementami zapewniania bezpieczeństwa danych osobowych. Do obowiązków tych należą:

1) uwzględnianie ochrony danych w fazie projektowania z art. 25 ust. 1 RODO, czyli tzw. zasada *privacy by design*;
2) domyślna ochrona danych z art. 25 ust. 2 RODO, czyli tzw. zasada *privacy by default*;
3) zapewnianie bezpieczeństwa danych w oparciu o analizę ryzyka z art. 32 RODO;
4) przeprowadzenie oceny skutków dla ochrony danych z art. 35 RODO;
5) przeprowadzenie uprzednich konsultacji z organem nadzorczym z art. 36 RODO;
6) zgłoszenie przez administratora wystąpienia naruszenia ochrony danych do organu nadzorczego (art. 33 RODO) oraz

7) powiadomienie osoby, której dane dotyczą, o wystąpieniu naruszenia ochrony danych (art. 34 RODO).

W dalszej części zostaną rozwinięte poszczególne obowiązki z perspektywy zapewnienia bezpieczeństwa danych osobowych w kancelarii prawnej. Obowiązki te należy podzielić na takie, które należy realizować w celu zapewnienia bezpieczeństwa danych (pkt 1–5 powyższego wyliczenia), oraz takie, które są realizowane w przypadku wystąpienia naruszenia ochrony danych (pkt 6–7 powyższego wyliczenia).

4. Zasada ochrony danych w fazie projektowania oraz zasada domyślnej ochrony danych a bezpieczeństwo w kancelarii prawnej

Dla zapewnienia bezpieczeństwa danych osobowych w kancelarii prawnej istotne znaczenie mają dwie zasady:
1) zasada ochrony danych osobowych w fazie projektowania oraz
2) zasada domyślnej ochrony danych.

Zasada ochrony danych w fazie projektowania (art. 25 ust. 1 RODO) oznacza, że administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja. Środki te są projektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO, w tym chronić prawa osób, których dane dotyczą. Przy określaniu środków technicznych i organizacyjnych administrator bierze pod uwagę takie czynniki, jak stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, jak również wynikające z przetwarzania ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i różnej wadze.

Dla prowadzenia kancelarii prawnej zasada ochrony danych oznacza przede wszystkim konieczność wdrożenia odpowiednich środków technicznych i organizacyjnych już na etapie podejmowania decyzji