DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH ZE WZORAMI

redakcja naukowa Mariusz Jagielski

Artur Cieślik, Magdalena Czaplińska, Paweł Fajgielski, Mariusz Jagielski
Damian Karwala, Paulina Komorowska-Mrozik, Dominik Lubasz, Marta Otto
Katarzyna Palka-Bartoszek, Wojciech Piszewski, Marlena Sakowska-Baryła
Paweł Tobiczyk, Mariola Więckowska

EDYTOWALNE WZORY DOSTĘPNE NA STRONIE INTERNETOWEJ

2

WYDANIE ZAKTUALIZOWANE I UZUPEŁNIONE

Wolters Kluwer

Materiały uzupełniające na stronie
www.dokumentacja-ochrony-danych-osobowych.wolterskluwer.pl
będą dostępne do 30 czerwca 2024 r.

Jeżeli w książce nie ma zdrapki z kodem aktywacyjnym, prosimy o kontakt
tel. 801 04 45 45

PIKTOGRAMY

wskazują ważne elementy
książki i ułatwiają
ich odnalezienie


Ważne

Przykłady


Podstawa prawna
Kontekst prawny


Pytania
Zadania


Rozwiązania
Odpowiedzi


Stanowisko stron
Pogląd


Orzecznictwo


Literatura


Historia

Nowe przepisy

DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH ZE WZORAMI

redakcja naukowa Mariusz Jagielski

Artur Cieślik, Magdalena Czaplińska, Paweł Fajgielski, Mariusz Jagielski
Damian Karwala, Paulina Komorowska-Mrozik, Dominik Lubasz, Marta Otto
Katarzyna Palka-Bartoszek, Wojciech Piszewski, Marlena Sakowska-Baryła
Paweł Tobiczyk, Mariola Więckowska

2

WYDANIE ZAKTUALIZOWANE I UZUPEŁNIONE

Wolters Kluwer

WARSZAWA 2022

Stan prawny na 1 maja 2022 r.

Recenzent
Dr hab. Andrzej Krasuski, prof. UJD

Wydawca
Monika Pawłowska

Redaktor prowadzący
Kinga Zając

Opracowanie redakcyjne
Trzy kropki Joanna Maź

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

Poszczególne części opracowali:
Artur Cieślik – rozdział 5
Magdalena Czaplińska, Marlena Sakowska-Baryła – rozdział 4
Paweł Fajgielski – rozdział 10
Mariusz Jagielski – przedmowa do drugiego wydania, rozdział 1
Damian Karwala – rozdział 13
Paulina Komorowska-Mrozik – rozdział 6
Dominik Lubasz – rozdział 12
Marta Otto – rozdział 9
Katarzyna Palka-Bartoszek – rozdziały 7, 8
Wojciech Piszewski, Paweł Tobiczyk – rozdział 3
Marlena Sakowska-Baryła, Mariola Więckowska – rozdział 11
Paweł Tobiczyk – rozdział 2

ISBN 978-83-8286-382-6
2. wydanie zaktualizowane i uzupełnione

ISBN PDF-a: 978-83-8286-707-7

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 728 313 462
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

Akty prawne

dyrektywa 95/46/WE	–	dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L 281, s. 31, ze zm.)
k.c.	–	ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2020 r. poz. 1740 ze zm.)
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)
k.p.	–	ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2020 r. poz. 1320 ze zm.)
k.p.a.	–	ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2021 r. poz. 735 ze zm.)
k.p.c.	–	ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2021 r. poz. 1805 ze zm.)
KPP	–	Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 398)
k.s.h.	–	ustawa z 15.09.2000 r. – Kodeks spółek handlowych (Dz.U. z 2020 r. poz. 1526 ze zm.)
o.p.	–	ustawa z 29.08.1997 r. – Ordynacja podatkowa (Dz.U. z 2021 r. poz. 1540 ze zm.)
pr. pras.	–	ustawa z 26.01.1984 r. – Prawo prasowe (Dz.U. z 2018 r. poz. 1914)
pr. tel.	–	ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U z 2021 r. poz. 576 ze zm.)
p.u.s.p.	–	ustawa z 27.07.2001 r. – Prawo o ustroju sądów powszechnych (Dz.U. z 2020 r. poz. 2072 ze zm.)
r.d.p.d.o.	–	rozporządzenie 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 (Dz.U. Nr 100, poz. 1024)

RODO, rozporządzenie ogólne	–	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) (Dz.Urz. UE L 119, s. 1, ze sprost.)
rozporządzenie 2019/1020	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z 20.06.2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.Urz. UE L 169, s. 1)
r.p.k.z.p.	–	rozporządzenie Rady Ministrów z 19.12.1992 r. w sprawie pracowniczych kas zapomogowo-pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy (Dz.U. Nr 100, poz. 502)
r.t.s.r.z.	–	rozporządzenie Ministra Administracji i Cyfryzacji z 11.05.2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. poz. 745)
TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47)
u.e.r.FUS	–	ustawa z 17.12.1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U. z 2022 r. poz. 504)
u.KRS	–	ustawa z 20.08.1997 r. o Krajowym Rejestrze Sądowym (Dz.U. z 2021 r. poz. 112 ze zm.)
u.KZP	–	ustawa z 11.08.2021 r. – ustawa o kasach zapomogowo-pożyczkowych (Dz.U. poz. 1666)
u.n.z.a.	–	ustawa z 14.07.1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2020 r. poz. 164 ze zm.)
u.o.d.o.	–	ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
u.o.d.o. z 1997 r.	–	ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.); nie obowiązuje
u.o.p.	–	ustawa z 24.08.1991 r. o ochronie przeciwpożarowej (Dz.U. z 2021 r. poz. 869 ze zm.)
u.PBT	–	ustawa z 15.07.2020 r. o Polskim Bonie Turystycznym (Dz.U. z 2021 r. poz. 839 ze zm.)
u.p.d.o.f.	–	ustawa z 26.07.1991 r. o podatku dochodowym od osób fizycznych (Dz.U. z 2021 r. poz. 1128 ze zm.)
u.s.u.s.	–	ustawa z 13.10.1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2022 r. poz. 1009 ze zm.)
u.ś.u.d.e.	–	ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
u.ZFŚS		ustawa z 4.03.1994 r. o zakładowym funduszu świadczeń socjalnych (Dz.U. z 2022 r. poz. 923)

u.z.s.o.	–	ustawa z 10.01.2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją (Dz.U. poz. 357)
u.z.z.	–	ustawa z 23.05.1991 r. o związkach zawodowych (Dz.U. z 2022 r. poz. 854)

Urzędy, instytucje, organizacje

ENISA	–	Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (The European Union Agency for Cybersecurity)
EROD	–	Europejska Rada Ochrony Danych
GIODO	–	Generalny Inspektor Ochrony Danych Osobowych
IOD	–	inspektor ochrony danych
KODO	–	koordynator ochrony danych osobowych
PUODO	–	Prezes Urzędu Ochrony Danych Osobowych
TSUE	–	Trybunał Sprawiedliwości Unii Europejskiej
UODO	–	Urząd Ochrony Danych Osobowych
WSA	–	wojewódzki sąd administracyjny
ZFŚS	–	zakładowy fundusz świadczeń socjalnych
ZUS	–	Zakład Ubezpieczeń Społecznych

Inne

AI	–	sztuczna inteligencja (*artificial intelligence*)
IT	–	technika informatyczna (*information technology*)
KZP	–	kasa zapomogowo-pożyczkowa
M. Prawn.	–	Monitor Prawniczy
PKZP	–	pracownicze kasy zapomogowo-pożyczkowe
PNT	–	Prawo Nowych Technologii
PP	–	podmiot przetwarzania

PRZEDMOWA DO DRUGIEGO WYDANIA

Przedstawiając w 2019 r. Czytelnikom pierwsze wydanie książki, napisałem, że ochrona danych osobowych to jedna z najbardziej dynamicznie zmieniających się dziedzin prawa. Trzy lata, które upłynęły od tego czasu, w pełni potwierdziły powyższą konstatację. Mimo że podstawowy akt prawny w tej dziedzinie – RODO, nie uległ zmianie, pojawiły się liczne nowe regulacje, dokumenty i rozstrzygnięcia precyzujące, rozszerzające, a w pewnym stopniu także modyfikujące wymagania nałożone na podmioty zobowiązane realizować obowiązki z dziedziny ochrony danych osobowych. Przybrały one postać nowych przepisów szczególnych oraz poprawek do dotychczas obowiązujących aktów prawnych, wytycznych interpretacyjnych, wydanych w szczególności przez Europejską Radę Ochrony Danych (EROD) oraz Prezesa Urzędu Ochrony Danych Osobowych (PUODO), orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE) i sądów polskich oraz decyzji PUODO. Konieczność ich uwzględnienia wymaga m.in. przeprowadzenia analizy dotychczas posiadanej dokumentacji ochrony danych osobowych i jej dostosowania do nowych przepisów, wytycznych i rekomendacji.

Oddawane do rąk Czytelników drugie wydanie *Dokumentacji ochrony danych osobowych ze wzorami* stanowi odpowiedź na powyższe wyzwanie. Zawiera ono nie tylko aktualizację treści zawartych w wydaniu pierwszym, lecz także zostało poszerzone o liczne nowe zagadnienia i wzory. Dość powiedzieć, że w aktualnej wersji książki Czytelnik znajdzie trzy całkowicie nowe rozdziały, a niemal każdy dotychczasowy rozdział jest uzupełniony o nowe formatki, tabele i szablony. Nowe wydanie liczy o 218 stron tekstu więcej niż wydanie pierwsze. Śmiało można powiedzieć, że przedstawiana Czytelnikom publikacja stanowi nowe opracowanie problematyki dokumentacji ochrony danych osobowych.

Przygotowane na potrzeby Czytelników pierwszego wydania zestawienie najważniejszych aktualizacji, zmian i uzupełnień, jakie znajdują się w niniejszym opracowaniu, prezentuje się następująco.

Dodano nowy rozdział odnoszący się do dokumentacji serwisu internetowego. Rozdział zawiera wytyczne dotyczące zakresu i funkcji poszczególnych dokumentów stosowanych powszechnie przez administratorów serwisów WWW, w tym tzw. skróconych klauzul informacyjnych i klauzul zgód, polityki prywatności oraz polityki cookie. W rozdziale

zamieszczone zostały wzory poszczególnych dokumentów wraz z ich omówieniem i instrukcją stosowania przez administratorów serwisów internetowych.

Dodano nowy rozdział omawiający prawne i etyczne zagadnienia, które powinny być uwzględnione w przypadku zastosowania rozwiązań informatycznych z zastosowaniem sztucznej inteligencji. Zgodnie z profilem książki zastosowano w tym względzie podejście praktyczne: prezentowane zagadnienia zostały opracowane w postaci wzorów, tabel i zestawów ułatwiających sprawdzenie stopnia realizacji wymogów. Rozdział zawiera też użyteczne rekomendacje.

Dodano nowy rozdział dotyczący współadministrowania danymi osobowymi oraz statusu współadministratorów. Rozdział uwzględnia treść najnowszych wyroków TSUE dotyczących współadministrowania w przypadku wykorzystywania narzędzi informatycznych, jak również Wytyczne w sprawie koncepcji administratora i procesora nr 7/2020 przyjęte przez EROD w lipcu 2021 r. Kluczowym elementem tej części opracowania jest wzór umowy o współadministrowanie danymi osobowymi.

Rozdział poświęcony audytom wewnętrznym został zmodyfikowany tak poważnie, że wymagał zmiany tytułu na „Dokumentacja monitorowania zgodności z RODO – audyty wewnętrzne i weryfikacja powierzenia przetwarzania". Zawiera on liczne nowe tabele audytów wraz z ich omówieniem, w tym obejmujące takie obszary, jak: działania zarządcze w organizacji, inwentaryzacja danych osobowych, prowadzenie rejestru czynności przetwarzania oraz mapa przepływu danych w organizacji, wdrożenie zasad ochrony danych osobowych wewnątrz organizacji, oddziaływanie systemu ochrony danych na działania organizacji, zarządzanie procesem szkoleń oraz działaniami zwiększającymi świadomość, zarządzanie ryzykiem związanym z bezpieczeństwem przetwarzania danych osobowych, zarządzanie ryzykiem związanym z przekazywaniem danych osobowych podmiotom zewnętrznym, w tym umowy powierzenia przetwarzania danych i standardowe klauzule umowne, zarządzanie komunikacją z podmiotami danych, realizacja praw podmiotów danych, w tym odpowiadanie na ich żądania oraz obsługa ich skarg, ocena skutków dla ochrony danych oraz stosowanie podejścia opartego na ryzyku, w tym ochrona danych w fazie projektowania i domyślna ochrona danych, proces zarządzania incydentami bezpieczeństwa i naruszeniami ochrony danych wraz z ich zgłoszeniem do organu nadzorczego, monitorowanie sposobu postępowania z danymi, monitorowanie przez IOD lub inne wyznaczone do tego osoby przestrzegania RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych, audyt podmiotu przetwarzającego, audyt umów powierzenia przetwarzania, audyt cyberbezpieczeństwa w IT według ENISA i audyt obszaru przetwarzania danych osobowych.

Rozdział na temat polityki ochrony danych osobowych został uzupełniony o praktyczne wytyczne dotyczące przygotowania szczegółowych procedur w ramach polityki. Nowe

zagadnienia obejmują m.in. procedurę retencji danych osobowych, procedurę wyboru dostawcy oraz procedurę obsługi żądań podmiotów danych.

Rozdział dotyczący oceny (szacowania) ryzyka uzupełniono o nowe szablony, w szczególności wykaz aktywów wspomagających, klasyfikację informacji – czynności przetwarzania danych osobowych, opis rodzaju źródeł ryzyka na potrzeby analizy ryzyka, rejestr ryzyka, raport z szacowania ryzyka. Przedstawiono liczne nowe przykłady, w tym wykaz zawierający 73 przykłady zagrożeń dla bezpieczeństwa danych. W ramach prezentacji sposobów postępowania uwzględniono organizacje o mniejszej skali działalności.

W rozdziale omawiającym problematykę oceny skutków dla ochrony danych osobowych uwzględniono nowy, zmieniony wykaz rodzajów operacji wymagających przeprowadzenia oceny skutków dla ochrony danych (PUODO *8 lipca 2019*). Zaktualizowano też wzór oceny skutków dla ochrony danych oraz uzupełniono rozdział o nowe przykłady praktyczne, kiedy ocena skutków dla ochrony danych jest wymagana.

W rozdziale poświęconym rejestrom czynności przetwarzania i kategorii czynności przetwarzania poszerzono liczbę przykładów uzupełnienia rejestrów. W ten sposób wzory rejestrów zostały dostosowane do potrzeb większej liczby adresatów.

Rozdział odnoszący się do dokumentacji pracowniczej został uzupełniony o wzory dotyczące innego niż wizyjny monitoringu pracowniczego oraz ankiety kontrolnej. Zawarto w nim też liczne nowe wskazówki praktyczne, przygotowane na podstawie stosownych wytycznych i interpretacji EROD i PUODO oraz tzw. dobrych praktyk.

W rozdziale prezentującym wzory zgód i klauzul informacyjnych uwzględniono najnowsze decyzje PUODO i orzecznictwo sądów administracyjnych, a także przepisy implementujące RODO z 2019 r., w tym przepisy Kodeksu pracy w zakresie dotyczącym zgody pracowników.

W rozdziale poświęconym międzynarodowym transferom danych uwzględniono nowe standardowe klauzule umowne opublikowane przez Komisję Europejską w czerwcu 2021 r., które zastąpiły dotychczasowe klauzule modelowe, uznane za niezapewniające zgodności z RODO. Rozdział prezentuje cztery odrębne wzory umów, bazując na modułach (wariantach) uwzględnionych w nowych klauzulach Komisji. Dodatkowo omówiono kluczowe zmiany w podejściu do stosowania klauzul modelowych i innych instrumentów transferowych będących skutkiem orzeczenia TSUE w sprawie Schrems II.

Mariusz Jagielski

Mariusz Jagielski

Rozdział 1

DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH ZGODNA Z RODO

1.1. Wprowadzenie

Dzień 25.05.2018 r., czyli dzień, w którym zaczęło być stosowane 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 (ogólne rozporządzenie o ochronie danych), zwane RODO, nie stanowi daty początkowej prawnej ochrony danych osobowych. W Europie Zachodniej pierwsze przepisy chroniące dane osobowe pojawiły się już w latach 70. XX w. Ochrona danych na poziomie europejskim funkcjonuje od lat 90. XX w. – kluczową rolę w tym względzie odegrało przyjęcie poprzedniczki RODO – dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[1]. Natomiast w Polsce odpowiednia ustawa o ochronie danych osobowych została uchwalona 29.08.1997 r. (weszła w życie 30.04.1998 r.).

Przez cały ten czas twórcom regulacji prawnych przyświecała idea wypracowania rozwiązań jak najskuteczniej chroniących osoby, których dane są przetwarzane. Zadanie to było o tyle trudne, że w interesie tych ostatnich wcale nie leży wyłącznie ograniczanie wykorzystywania dotyczących ich informacji. Wręcz odwrotnie, zazwyczaj przynosi im to korzyści. Chodzi zarówno o korzyści indywidualne – dostarczenie im potrzebnych usług i świadczeń, jak i o te o charakterze zbiorowym – rozwój ekonomiczny i społeczny dobrobyt, jak również właściwe funkcjonowanie instytucji publicznych. W konsekwencji ochronę danych osobowych należy widzieć w kategoriach próby poszukiwania kompromisu pomiędzy gospodarczymi i administracyjnymi potrzebami przetwarzania informacji o człowieku a koniecznością zagwarantowania mu ochrony jego praw. Ochrona danych osobowych stanowi zatem próbę znalezienia złotego środka

[1] Por. M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 10–12.

i wyważenia interesów na rynku (w ramach relacji przedsiębiorcy – klienci) i w państwie (w ramach relacji organy państwowe – obywatele). Przy tym przyjmowane w zajmującej nas dziedzinie regulacje podlegały i podlegają nieustannej ewolucji. Dzieje się tak dlatego, że metody ochrony trzeba na bieżąco dostosowywać do nowych wyzwań, zwłaszcza przemian technologicznych[2]. Te zaś następowały w ostatnich dziesięcioleciach z niezwykłą intensywnością. W konsekwencji prawna ochrona danych osobowych to jedna z najbardziej dynamicznie zmieniających się dziedzin prawa.

Częsta zmiana przepisów nie jest korzystna – ani dla tych, którzy mają je stosować, ani dla tych, którzy mają być przez nie chronieni. Stąd zamysł, by spróbować odnaleźć takie rozwiązania, które będą w stanie przetrwać próbę czasu. Takie właśnie było założenie reformy ochrony danych osobowych, której ostatecznym efektem stało się RODO. Skoro przemiany technologiczne są tak szybkie, że unormowania prawne nie potrafią za nimi nadążyć – jak założyli twórcy reformy – trzeba wypracować na tyle elastyczne metody podejścia, by umożliwiły one reagowanie na bieżąco na pojawiające się zagrożenia, bez konieczności zmiany przepisów. To zaś jest możliwe jedynie w przypadku, gdy ciężar reakcji przeniesiemy z poziomu legislacyjnego na poziom zarządzania bezpieczeństwem. Oznacza to, że trzeba pozostawić swobodę podmiotom odpowiedzialnym za realizację ochrony – administratorom, podmiotom przetwarzającym. Tylko one mogą na bieżąco analizować zagrożenia i dostosowywać metody ochrony do najnowszych wyzwań. Podejście takie nazwano podejściem opartym na ocenie ryzyka (*risk-based approach*) i wokół niego zorganizowano system ochrony danych osobowych w RODO[3].

Przewidziane reformą nowe rozwiązania ochronne są więc znacznie bardziej elastyczne niż te, które obowiązywały pod rządami wcześniejszych przepisów. Powyższą konstatację można odnieść do większości obszarów ochrony danych osobowych. Jednym z nich – gdzie powyższa zmiana rysuje się najbardziej spektakularnie – jest problematyka dokumentacji ochrony danych osobowych.

1.2. Podstawy prawne i zasady prowadzenia dokumentacji ochrony danych osobowych

Przed 25.05.2018 r. przepisy w miarę precyzyjnie wskazywały dokumenty, które powinni posiadać wszyscy administratorzy oraz podmioty przetwarzające, nierzadko determinując w sposób szczegółowy ich treść. Zasadnicze elementy tej dokumentacji stanowiły:

[2] A. Grzelak, *Główne cele ogólnego rozporządzenia o ochronie danych* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017, s. 21–22; A. Krasuski, *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018, s. 17.

[3] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2017, s. 341. O ryzyku w kontekście RODO por. też A. Krasuski, *Ochrona...*, s. 295 i n.

1) polityka bezpieczeństwa informacji (§ 4 r.d.p.d.o.),
2) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (§ 5 r.d.p.d.o.),
3) indywidualne upoważnienia do przetwarzania danych osobowych nadane każdej osobie, która bierze udział w procesie przetwarzania danych osobowych (art. 37 u.o.d.o. z 1997 r.),
4) indywidualne zobowiązanie do zachowania danych oraz sposobu ich zabezpieczenia w tajemnicy (art. 39 ust. 2 u.o.d.o. z 1997 r.),
5) ewidencja osób upoważnionych do przetwarzania danych osobowych (art. 39 u.o.d.o. z 1997 r.),
6) dokumentacja sprawdzeń (art. 36b u.o.d.o. z 1997 r. oraz § 3 ust. 3 i § 5 ust. 2 r.t.s.r.z.).

N! Reforma ochrony danych osobowych z 2018 r. doprowadziła do tego, że wszystkie akty normatywne, które wymagały opracowania i wdrożenia powyższych dokumentów, przestały obowiązywać[4]. Zaowocowało to istotnymi zmianami w interesującej nas dziedzinie[5]. Zgodnie z nowym podejściem RODO nie zawiera generalnych wytycznych ani co do struktury dokumentacji, ani co do sposobu jej prowadzenia, ani – w końcu – co do jej merytorycznej treści. Swoboda, jaką pozostawiono administratorom i podmiotom przetwarzającym w zakresie zapewnienia ochrony danych osobowych, przejawia się między innymi w tym, że mogą one nie tylko samodzielnie kształtować, ale także opisywać stosowane metody przetwarzania danych osobowych, związane z nimi procedury, jak również zastosowane zabezpieczenia techniczne i organizacyjne. Chodzi o to, by opracowywane dokumenty mogły być jak najbardziej praktyczne, dostosowane do potrzeb konkretnego podmiotu, a także by ograniczyć przypadki tworzenia dokumentów zbędnych, takich, które w kontekście skali i sposobu przetwarzania danych przez dany podmiot nie są użyteczne.

[4] Nastąpiło to na podstawie art. 175 u.o.d.o. zasadniczo z dniem 25.05.2018 r. Wyjątkiem jest sektor zapobiegania i zwalczania przestępczości, w którym to przedłużono obowiązywanie niektórych regulacji u.o.d.o. z 1997 r., w tym tych będących podstawą opracowania dokumentacji ochrony danych osobowych, do dnia wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89, ze sprost.). Przepisy te przybrały ostatecznie postać ustawy z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), która weszła w życie 6.02.2019 r. W tym dniu przepisy u.o.d.o. z 1997 r. oraz przepisy wykonawcze nakazujące opracowanie i wdrożenie wskazanych dokumentów przestały ostatecznie obowiązywać.

[5] Praktyczne porównanie rozwiązań z ustawy o ochronie danych osobowych funkcjonujących przed 25.05.2018 r. oraz z RODO obowiązujących po 25.05.2018 r. zob. D. Lubasz, *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi*, Warszawa 2018, s. 16 i n.

Za ilustrację powyższego problemu mogą posłużyć dotychczasowe dokumenty: polityka bezpieczeństwa informacji oraz instrukcja zarządzania systemem informatycznym. Były to dokumenty, które w poprzednim stanie prawnym obowiązkowo musieli przygotować i wdrożyć niemal wszyscy administratorzy[6], bez względu na skalę, zakres i sposób działania. Treść obydwu dokumentów wynikała z r.d.p.d.o. i była zasadniczo taka sama dla wszystkich adresatów tego aktu prawnego. Jej opracowanie było uciążliwe, a w niektórych przypadkach, zwłaszcza tzw. mikroprzedsiębiorców, praktyczna przydatność wątpliwa.

Powyższe nie oznacza, że po 25.05.2018 r. administratorzy i przetwarzający dane osobowe mogą zrezygnować z dokumentacji w ogóle[7]. Wymagania nakładane na nich przez RODO są tak ukształtowane, że w pewnych przypadkach prowadzenie odpowiedniej dokumentacji stanie się celowe. Z tego punktu widzenia zawarte w RODO regulacje można podzielić na dwa rodzaje. Pierwsze to takie, w których wskazano obowiązki, z których wprost wynika konieczność opracowania pewnych konkretnych dokumentów. Prezes Urzędu Ochrony Danych Osobowych wskazuje następujące takie przypadki:

1) prowadzenie rejestru czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;
2) zgłaszanie naruszenia ochrony danych do organu nadzorczego (UODO) – art. 33 ust. 3 RODO;
3) prowadzenie wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO;
4) zawartość raportu dokumentującego wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7 RODO[8].

Cechą charakterystyczną powyższych rozwiązań jest to, że RODO wskazuje przy ich pomocy wprost konkretne treści, które adresat jest zobowiązany opracować. W tym zakresie sporządzenie dokumentu staje się więc koniecznością, gdyż w przeciwnym wypadku administrator lub podmiot przetwarzający nie zrealizowałby nałożonego nań konkretnego obowiązku.

Przypadek drugi to sytuacja, gdy RODO, określając w sposób ogólny zasady i wymogi, którym musi odpowiadać przetwarzanie danych osobowych, tak je formułuje, że ich wykonanie nie będzie możliwe albo bardzo utrudnione, jeśli nie obejmie opracowania stosownych dokumentów. Kluczową rolę w tym względzie odgrywa wyrażona w art. 5 ust. 2 RODO zasada rozliczalności. Wymaga ona, by administratorzy nie tylko prze-

[6] W drugim przypadku pod warunkiem, że przetwarzali dane osobowe w systemie informatycznym.

[7] M. Cwener, *Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017, s. 100.

[8] UODO, *Dokumentacja przetwarzania danych osobowych zgodnie z RODO*, https://uodo.gov.pl/pl/138/273 (dostęp: 15.04.2022 r.).

strzegali zasad przetwarzania określonych w RODO, ale by byli w stanie to wykazać[9]. Jak widać, konieczność udokumentowania konkretnych treści nie jest w tym przepisie wyrażona wprost, jednak wymóg umiejętności wykazania, że przestrzega się postanowień rozporządzenia, najprościej zrealizować, dokumentując podejmowane działania i stosowane procedury.

Idea powyższa została rozwinięta i doprecyzowana w art. 24 ust. 1 RODO[10]. Przepis ten nakłada na administratorów obowiązek wdrożenia takich środków technicznych i organizacyjnych, które zapewnią, że przetwarzanie będzie odbywało się zgodnie z rozporządzeniem i administratorzy będą w stanie to wykazać. Realizując wskazany obowiązek, administratorzy powinni uwzględnić charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, a także mają obowiązek poddawania przeglądom i uaktualniania zastosowanych środków, jeśli tylko zajdzie taka potrzeba.

Powyższy przepis, analogicznie do art. 5 ust. 2 RODO, nie nakłada wprost obowiązku przygotowania konkretnych dokumentacji, jednak nie ulega wątpliwości, że nie można zrealizować wskazanych w nim zaleceń, unikając tworzenia dokumentów. Wręcz przeciwnie, opracowanie i wdrożenie właściwych dokumentów można potraktować jako wspomniany w tym przepisie „środek organizacyjny", którego zastosowanie umożliwi realizację zawartych w nim wymogów. W świetle zasady rozliczalności przygotowanie dokumentacji ochrony danych osobowych nie jest zatem celem samym w sobie. Stanowi metodę realizacji wskazanych we wspomnianym przepisie obowiązków – zapewnienia, by przetwarzanie odbywało się zgodnie z przepisami, i wymogu, by być w stanie to wykazać.

Z powyższego wynika, że do dokumentacji ochrony danych osobowych należy podchodzić funkcjonalnie. Nie ma znaczenia forma i struktura prowadzonej dokumentacji, czyli nazwy poszczególnych dokumentów oraz podział materii między nimi. W tym zakresie administratorzy i podmioty przetwarzające dysponują daleko idącą swobodą. Ważne, by zrealizować cele wskazane w RODO – zagwarantować, że przetwarzanie będzie odbywało się zgodnie z rozporządzeniem, oraz zapewnić, że będzie się umiało to wykazać.

Cel powyższy rozpada się na liczne bardziej konkretne wymagania zawarte w znacznie szczegółowszych przepisach RODO. Przepisy te stają się w ten sposób bardziej precyzyjnymi podstawami opracowania dokumentacji niż zasada rozliczalności. Prezes Urzędu

[9] Szerzej: P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022, s. 167–168; *RODO. Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D. Lubasz, s. 342–343.

[10] Por. też P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych*, Warszawa 2018, s. 268.

Ochrony Danych Osobowych wymienia w wytycznych siedem rodzajów wymogów, których realizacja będzie wiązać się ze sporządzeniem stosownych dokumentów. Zgodnie z wymogami zawartymi w wytycznych administrator:

a) stosuje się do ogólnych zasad przetwarzania określonych w art. 5 RODO,
b) zapewnia, aby dane przetwarzane były zgodnie z prawem (art. 6–11 RODO),
c) zapewnia, aby przestrzegane były prawa osób, których dane są przetwarzane (art. 12–23 RODO),
d) zapewnia wypełnianie ogólnych obowiązków w zakresie przetwarzania danych ciążących na administratorze i podmiocie przetwarzającym (art. 24–31 RODO),
e) zapewnia bezpieczeństwo przetwarzania danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania danych (art. 32–36 RODO),
f) zapewnia kontrolę nad przetwarzaniem danych w postaci monitorowania przestrzegania przepisów i przyjętych procedur przetwarzania przez Inspektora Ochrony Danych lub podmioty certyfikujące czy monitorujące przestrzeganie przyjętych kodeksów postępowania (art. 27–43 RODO),
g) stosuje się do wymagań w zakresie przekazywania danych do państw trzecich i instytucji międzynarodowych (art. 44–49 RODO)[11].

Prezes Urzędu wskazuje, że realizacja każdego ze wskazanych powyżej typów obowiązków będzie w praktyce wymagała opracowania stosownej dokumentacji. Jednak raz jeszcze trzeba podkreślić, że nie chodzi tu o podstawienie typu: jeden do jednego, czyli że do każdego z wymogów należy przygotować osobny dokument, który będzie opisywać jego realizację. Chodzi o to, żeby wszystkie wskazane obowiązki zostały zrealizowane. Dokumentacja ma to „wykazywać". Natomiast to, jak to będzie „wykazane", czyli ile dokumentów zostanie opracowanych i jaką formę przybiorą (np. czy będą opisowe, czy w postaci tabel, papierowe, czy elektroniczne, odręczne, czy drukowane), jest zasadniczo decyzją samego administratora.

1.3. Podmioty zobowiązane do opracowania dokumentacji ochrony danych osobowych

RODO dzieli podmioty zobowiązane do realizacji wymogów z dziedziny ochrony danych osobowych na dwa zasadnicze[12] typy: administratorów danych oraz podmioty przetwarzające.

[11] UODO, *Dokumentacja przetwarzania danych osobowych zgodnie z RODO*.

[12] Są też inne – przedstawiciel administratora oraz podmiotu przetwarzającego (art. 27 RODO), osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego (art. 29 RODO), odbiorca (art. 4 pkt 9 RODO), strona trzecia (art. 4 pkt 10 RODO). Ze względu na zawężenie omawianej tu problematyki do dokumentacji ochrony danych osobowych kwestia statusu tych podmiotów zostanie jednak w tym miejscu pominięta.

Administratorem jest ten, kto posiada uprawnienia decyzyjne w stosunku do danych osobowych. Podmiot taki może przybrać dowolną postać organizacyjną – może to być osoba fizyczna, osoba prawna, organ publiczny albo każda inna jednostka organizacyjna, byleby tylko samodzielnie lub wspólnie z innymi ustalała cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO). Administratorami będą więc osoby fizyczne samodzielnie prowadzące działalność gospodarczą, spółki prawa handlowego, organizacje pozarządowe, np. stowarzyszenia czy fundacje, spółdzielnie, organy państwowe i samorządowe, jak też wszelkiego typu państwowe i komunalne jednostki organizacyjne, niezależnie od tego, czy posiadają osobowość prawną, czy nie, byleby tylko posiadały uprawnienia decyzyjne w stosunku do danych[13].

Np.

Samodzielność decyzyjna może wynikać z gwarantowanych konstytucyjnie swobód obywatelskich, w tym z wolności prowadzenia działalności gospodarczej. Tak będzie przykładowo, gdy przedsiębiorca podejmie decyzję, że będzie prowadzić sprzedaż wysyłkową towarów klientom, albo gdy zadecyduje o wysyłaniu newslettera. Każde z tych działań będzie wymagało przetworzenia danych osobowych odbiorcy. Jeśli jednak cele i sposoby przetwarzania są określone w przepisach prawa, to te właśnie przepisy mogą określić kryteria pozwalające ustalić, kto jest administratorem, albo nawet wskazywać administratora wprost. Przykładem takiej sytuacji może być przetwarzanie danych osobowych pracowników przez pracodawcę w celu realizacji obowiązków wynikających z przepisów prawa albo działalność organów i jednostek państwowych i samorządowych, których większość zadań stanowi realizację kompetencji określonych ustawami.

RODO pozwala, by dwóch lub kilku administratorów wspólnie ustalało cele i sposoby przetwarzania. Są oni wtedy określani mianem współadministratorów. By działać w ten sposób, administratorzy muszą zawrzeć porozumienie, w którym wspólnie uzgodnią zakresy swoich obowiązków oraz odpowiedzialność (art. 26 RODO). Tacy działający wspólnie współadministratorzy muszą więc realizować wymagania, które RODO przewidziało dla administratorów14.

Od wskazanego powyżej rozwiązania należy odróżnić sytuację prawną podmiotu przetwarzającego, czyli takiego, któremu administrator powierza przetworzenie danych osobowych. Z przypadkiem takim będziemy mieli do czynienia, gdy administrator zamiast samodzielnie wykonać jakąś czynność przetwarzania, posłużył się w celu jej realizacji jakimś podmiotem zewnętrznym. To właśnie ten ostatni podmiot będzie nazywany przetwarzającym. Jako przykład takiej sytuacji można podać zlecenie specjalistycznej firmie zniszczenia dokumentów zawierających dane osobowe. Podmiot przyjmujący zlecenie nie uzyska statusu administratora, gdyż nie ma uprawnień decyzyjnych w stosunku do danych – może zrobić z nimi tylko to, co nakazał mu administrator.

[13] P. Fajgielski, *Ogólne...*, s. 122–123; *RODO. Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D. Lubasz, s. 211 i n.

[14] P. Fajgielski, *Ogólne...*, s. 327 i n.; *RODO. Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D. Lubasz, s. 613 i n.

Nie uzyska też statusu współadministratora, gdyż nie bierze udziału w ustalaniu celów i sposobów przetwarzania wspólnie z administratorem. Wręcz przeciwnie, będzie związany ustaleniami w tym względzie powziętymi przez administratora, np. co do czasu, miejsca i sposobu zniszczenia danych.

Przy tym, żebyśmy mieli do czynienia z podmiotem przetwarzającym, musi być to podmiot posiadający status prawny niezależny od administratora – musi to być odrębna osoba fizyczna, osoba prawna, organ publiczny lub inna jednostka organizacyjna niepowiązana strukturalnie z administratorem. Tym, co łączy podmiot przetwarzający z administratorem, jest umowa lub inny instrument prawny, na podstawie którego administrator zleca przetwarzającemu realizację zadania, które wiążą się z przetworzeniem danych osobowych „należących" do administratora. Oznacza to, że podmiot przetwarzający będzie przetwarzać takie dane, które powierzył mu administrator, w celu, jaki wyznaczył administrator, oraz w sposób, jaki on określił. Podmiot przetwarzający nie jest więc samodzielny w zakresie podejmowanych czynności – działa w imieniu administratora (art. 4 pkt 8 RODO)[15].

Np. Innymi wskazanymi przez Prezesa Urzędu Ochrony Danych Osobowych przykładami powierzenia danych osobowych będą:

1) przechowywanie danych klienta (administratora) rozumiane jako udostępnienie zamawiającemu określonej przestrzeni dyskowej w infrastrukturze przetwarzającego na przechowywanie danych, którymi zlecający (administrator) sam zarządza i decyduje o tym, jakie dane tam przechowuje – np. wykonuje kopie zapasowe danych elektronicznych;
2) udostępnianie klientowi (administratorowi) mocy obliczeniowej procesorów, przestrzeni pamięci operacyjnej i dyskowej lub innych usług na potrzeby instalacji i eksploatacji usług przetwarzania, którymi zamawiający w pełni zarządza – dostarczanie infrastruktury informatycznej;
3) udostępnienie klientowi (administratorowi) określonej platformy programistycznej (np. serwera WWW wraz z odpowiednim oprogramowaniem do prowadzenia własnej strony internetowej);
4) wykonywanie na zamówienie klienta (zamawiającego) określonych usług w zakresie konfiguracji sprzętowej, programowej, w tym zabezpieczeń udostępnionych mu serwerów, innych urządzeń komputerowych oraz oprogramowania – usługi administracyjne i konserwacyjne;
5) wykonywanie na zamówienie klienta (zamawiającego) usług programistycznych, w tym aktualizacji oprogramowania na okoliczność zmieniających się przepisów prawnych lub wymagań klienta – usługi programistyczne itp.;
6) samo przechowywanie dokumentacji podatkowej, księgowej, kadrowej i medycznej;
7) prowadzenie dokumentacji podatkowej, księgowej, kadrowej;
8) archiwizacja danych elektronicznych;

[15] A. Krasuski, *Ochrona...*, s. 147 i n.; P. Fajgielski, *Ogólne...*, s. 123–124; *RODO. Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D. Lubasz, s. 222 i n.

9) skanowanie i digitalizacja danych;
10) niszczenie nośników informacji[16].

Jeśli chodzi o zakres obowiązków, jakie na administratorów i podmioty przetwarzające nakładają przepisy RODO[17], to możliwe są trzy sytuacje. Po pierwsze, są to obowiązki, które muszą spełnić zarówno administratorzy, jak i podmioty przetwarzające. Druga kategoria to obowiązki, które zostały nałożone wyłącznie na administratorów danych. W końcu przypadek trzeci to sytuacja, gdy dany typ obowiązku dotyczy wyłącznie podmiotów przetwarzających. Powyższa konstatacja odnosi się rzecz jasna także do obowiązków dokumentacyjnych. Podział ten zostanie przedstawiony szczegółowo w dalszej części opracowania (zob. pkt 1.4).

W tym miejscu zauważmy jeszcze, że konkretny podmiot zobowiązany do realizacji postanowień RODO może występować jednocześnie w obydwu wskazanych rolach – jako administrator i jako podmiot przetwarzający. Stanie się tak, gdy pewne dane będzie przetwarzać jako swoje (czyli takie, których będzie administratorem), a inne na zlecenie jakiegoś podmiotu zewnętrznego. Dobrym przykładem takiej sytuacji będzie przypadek wskazanego wcześniej przedsiębiorcy zajmującego się niszczeniem dokumentów. W zakresie danych powierzonych mu do zniszczenia przez kontrahentów będzie ich przetwarzającym. Jednak w stosunku do własnych danych (np. własnych danych księgowych lub własnych danych pracowniczych) będzie ich administratorem. Będzie on administratorem tych ostatnich danych także wtedy, gdy zdecyduje się je zniszczyć. A zatem dokonując tej samej czynności przetwarzania – niszczenia danych – może występować w dwóch różnych rolach. O zniszczeniu własnych (np. niepotrzebnych już) dokumentów księgowych lub pracowniczych zadecyduje samodzielnie – wystąpi więc w roli administratora. Dokumenty dostarczone mu przez jego kontrahentów będzie niszczyć na ich zlecenie – czyli wystąpi jako podmiot przetwarzający. Fakt, że występuje w takiej podwójnej roli, będzie musiał uwzględnić w prowadzonej dokumentacji.

1.4. Zakres przedmiotowy dokumentacji ochrony danych osobowych

Uwzględniając podstawy prawne i zasady określone w pkt 1.2 oraz wskazany w pkt 1.3 podział podmiotów zobowiązanych do stosowania RODO na administratorów i przetwarzających, należy zauważyć, że nie można przedstawić jednego, uniwersalnego modelu dokumentacji, który będzie pasował do wszystkich podmio-

[16] UODO, *Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO*, s. 10, https://www.uodo.gov.pl/data/filemanager_pl/708.pdf (dostęp: 15.04.2022 r.).

[17] Skrupulatne wyliczenie tych obowiązków można znaleźć w: *RODO. Przewodnik ze wzorami*, red. M. Gawroński, Warszawa 2018, s. 119–121 i 123–124.

tów zobowiązanych do jej prowadzenia. Musi ona bowiem być dostosowana do typu podmiotu oraz zakresu i sposobu przetwarzanych przezeń danych osobowych. Można natomiast wskazać dokumenty, których opracowanie każdy taki podmiot powinien rozważyć. Oto wykaz tych dokumentów ze wskazaniem, czy są one obowiązkowe, czy zalecane, w zależności od rodzaju prowadzonej działalności oraz tego, czy mamy do czynienia z administratorem, czy podmiotem przetwarzającym.

1. Polityka ochrony danych osobowych. Jest to najbardziej ogólny element dokumentacji. Jego opracowanie i wdrożenie nie jest obowiązkowe, jest jednak zalecane jako „środek organizacyjny" zapewniający zgodność przetwarzania z RODO. Zalecenie to zostało wyrażone wprost w stosunku do administratorów (art. 24 ust. 2 RODO). W przypadku podmiotów przetwarzających można je wyprowadzić pośrednio z treści art. 28 ust. 1 i 4 RODO. Treść i wewnętrzną strukturę polityki administratorzy i podmioty przetwarzające mogą kształtować dowolnie, dostosowując je do potrzeb. Szczegóły zob. rozdział 2.

2. Dokumentacja serwisu internetowego. Szczególne wymagania dokumentacyjne odnoszą się do podmiotów świadczących usługi online. Chodzi zarówno o administratorów, jak i podmioty przetwarzające. Podstaw prawnych opracowania i wdrożenia dokumentacji w tym zakresie należy dopatrywać się nie tylko w RODO, lecz także w przepisach Prawa telekomunikacyjnego i u.ś.u.d.e. Obejmie ona w szczególności takie dokumenty jak polityka prywatności i polityka cookie, które z perspektywy RODO można potraktować jako specjalne rodzaje polityk ochrony danych osobowych, jednak nie ogranicza się do nich. Szczegóły zob. rozdział 3.

3. Dokumentacja w przypadku wykorzystywania sztucznej inteligencji. Inną szczególną dziedziną wymagającą opracowania odpowiednich dokumentów jest przetwarzanie danych osobowych z użyciem *artificial intelligence* (AI). To dziedzina, której obudowa prawna jest dopiero tworzona, niemniej już dzisiaj koniecznie należy zwrócić uwagę na wymagania i zalecenia dokumentacyjne, jakie w tym względzie zostały wypracowane lub są proponowane. Dotyczą one wszystkich podmiotów korzystających ze wskazanych systemów, a zatem zarówno administratorów, jak i podmiotów przetwarzających. Szczegóły zob. rozdział 4.

4. Dokumentacja oceny (szacowania) ryzyka. Procedura szacowania ryzyka nie musi przybrać postaci specjalnego dokumentu. Jednak taka ocena będzie musiała być przeprowadzona zarówno przez administratorów (art. 24 ust. 1 oraz art. 32 ust. 1 i 2 RODO), jak i przetwarzających (art. 28 ust. 3 lit. c oraz art. 32 ust. 1 i 2 RODO), a podmioty te muszą umieć wykazać, że zadanie to zrealizowały. Jakaś forma udokumentowania realizacji tego zadania jest więc konieczna. Szczegóły zob. rozdział 5.

5. Dokumentacja oceny skutków dla ochrony danych osobowych. Taka ocena będzie konieczna, gdy zostaną spełnione przesłanki zawarte w art. 35 RODO. Podmiotami

tego obowiązku są zasadniczo tylko administratorzy danych, jednak w szczególnych sytuacjach podmioty przetwarzające mogą być zobowiązane do współpracy w realizacji tego zadania (art. 28 ust. 3 lit. f RODO). Konieczność opracowania dokumentacji oceny skutków wynika z RODO wprost, gdyż art. 35 ust. 7 określa zawartość obowiązkowego raportu dokumentującego wyniki takiej oceny. Pozostałe elementy dokumentacji oceny skutków administratorzy mogą dostosować do specyfiki swojej organizacji i typów przetwarzania. Szczegóły zob. rozdział 6.

6. Rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania. Pierwszy ze wskazanych dokumentów będą zobowiązani przygotować administratorzy danych (art. 30 ust. 1 RODO), drugi zaś podmioty przetwarzające (art. 30 ust. 2 RODO). Nie licząc wyjątków wskazanych w art. 30 ust. 5 RODO, są to rejestry obowiązkowe. Ich treść obligatoryjna została określona we wspomnianych wyżej przepisach. Szczegóły zob. rozdział 7.

7. Dokumentacja współadministrowania danymi osobowymi. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, to w drodze wspólnych uzgodnień powinni oni określić odpowiednie zakresy swojej odpowiedzialności oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą (art. 26 ust. 1 i 2 RODO). Współadministratorzy mają swobodę w wyborze formy uzgodnień, niemniej takie porozumienie oczywiście wymaga udokumentowania. W praktyce najczęściej będą zawierali umowę. Szczegóły zob. rozdział 8.

8. Dokumentacja pracownicza. Liczni administratorzy oraz podmioty przetwarzające, przetwarzając dane osobowe, będą posługiwać się innymi osobami (podmiotami). Mogą być to albo osoby u nich zatrudnione, albo, jak już wiemy, podmioty zewnętrzne (które nazwaliśmy wcześniej przetwarzającymi). W pierwszym przypadku rodzi to konsekwencje w postaci obowiązku zapewnienia, że osoby działające z ich upoważnienia będą przetwarzać dane osobowe wyłącznie na ich polecenie, czyli zgodnie z ich instrukcjami (art. 29 i art. 32 ust. 4 RODO). W drugim przypadku należy zawrzeć umowy powierzenia danych osobowych lub posłużyć się innym dopuszczalnym przez prawo instrumentem powierzenia (art. 28 ust. 3 RODO). Jeśli to podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego (czyli powierza przetwarzanie takich danych osobowych, które jemu powierzył administrator), to mamy do czynienia z konstrukcją podpowierzenia (art. 28 ust. 4 RODO).

Ponadto, działając jako pracodawcy, administratorzy i przetwarzający będą mieli też inne prawa i obowiązki. Do tych drugich należy wymóg zrealizowania w stosunku do osób u nich zatrudnionych obowiązku informacyjnego (art. 13 RODO). Do praw należy natomiast możliwość wprowadzenia monitoringu wizyjnego na terenie zakładu pracy (art. 22^2 k.p.) oraz monitorowanie poczty elektronicznej pracownika (art. 22^3 k.p.). Prawo

wprowadzenia monitoringu jest skorelowane z odpowiednimi obowiązkami informacyjnymi (nieco innymi w przypadku monitoringu wizyjnego i monitoringu poczty).

Jak wynika z zasady rozliczalności, realizacja każdego ze wskazanych praw i obowiązków będzie musiała być jakoś udokumentowana. Wymagania oraz sugestie w tym względzie zawiera rozdział 9.

9. Dokumentacja naruszeń ochrony danych osobowych. Obowiązek dokumentowania naruszeń ochrony danych osobowych wynika wprost z RODO (art. 33 ust. 5). Jednocześnie rozporządzenie wskazuje elementy obligatoryjne zgłoszenia, przy pomocy którego należy powiadomić o naruszeniu organ nadzorczy (art. 33 ust. 3). Ten element dokumentacji należy więc uznać za obowiązkowy w przypadku administratorów, o ile tylko nastąpi jakieś naruszenie. W przypadku podmiotów przetwarzających istnieje jedynie obowiązek zgłoszenia naruszenia administratorowi. Szczegóły zob. rozdział 10.

10. Dokumentacja monitorowania zgodności z RODO. RODO nie nakłada ani na administratorów, ani na przetwarzających wprost obowiązku przeprowadzania audytów. Jednak zarówno pierwsi (art. 24 ust. 1 oraz art. 32 ust. 1), jak i drudzy (art. 28 ust. 1 i 4 oraz art. 32 ust. 1) są zobowiązani zapewnić, że przetwarzanie odbywa się zgodnie z RODO, a stopień bezpieczeństwa danych odpowiada ryzyku. Wykonanie wskazanego obowiązku trzeba umieć wykazać. Audyt należy zatem potraktować jako środek organizacyjny realizujący wskazane zadania, a dokumentację audytów jako metodę wykazania, że obowiązki te zostały spełnione. Szczegóły zob. rozdział 11.

11. Wzory zgód oraz klauzul informacyjnych. Liczni administratorzy przetwarzający dane osobowe będą działać na podstawie zgody podmiotów danych (art. 6 ust. 1 lit. a, art. 9 ust. 2 lit. a RODO). Zdecydowana większość administratorów ze względu na fakt pozyskiwania danych osobowych będzie musiała realizować obowiązki informacyjne (art. 13 i 14 RODO). Dla tych podmiotów będzie użyteczne opracowanie i włączenie do dokumentacji wzorów takich zgód i klauzul informacyjnych, dostosowanych do stosowanego przez nich zakresu i sposobów przetwarzania. Opracowanie wzorów nie jest obowiązkowe, ale umiejętność wykazania, że zgody zostały pozyskane, a obowiązek informacyjny zrealizowany, już tak. Trzeba więc spełnienie tych wymogów jakoś udokumentować. Wskazane w tym punkcie obowiązki zostały nałożone jedynie na administratorów i nie dotyczą podmiotów przetwarzających. Szczegóły zob. rozdział 12.

12. Transfer danych osobowych do państw trzecich. Jeśli administrator lub podmiot przetwarzający będzie przekazywać dane osobowe do tzw. państw trzecich, czyli poza Europejski Obszar Gospodarczy, to będzie musiał spełnić wymagania zawarte w art. 44–49 RODO. Wskazane wymagania są częstokroć dalece sformalizowane i wymagają przygotowania odpowiednich dokumentów. Treść tych dokumentów znajdzie

swoje oparcie albo bezpośrednio w RODO, albo w odpowiednich decyzjach organów (w praktyce: Komisji Europejskiej). Szczegóły zob. rozdział 13.

Literatura

Cwener M., *Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022

Grzelak A., *Główne cele ogólnego rozporządzenia o ochronie danych* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017

Jagielski M., *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010

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

Litwiński P., Barta P., Kawecki M., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych*, Warszawa 2018

Lubasz D., *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi*, Warszawa 2018

RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2017

RODO. Przewodnik ze wzorami, red. M. Gawroński, Warszawa 2018

UODO, *Dokumentacja przetwarzania danych osobowych zgodnie z RODO*, https://uodo.gov.pl/pl/138/273 (dostęp: 15.04.2022 r.)

UODO, *Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO*, https://www.uodo.gov.pl/data/filemanager_pl/708.pdf (dostęp: 15.04.2022 r.)

Paweł Tobiczyk

Rozdział 2

POLITYKA OCHRONY DANYCH OSOBOWYCH

2.1. Wprowadzenie

Regulacje obowiązujące przed wejściem w życie RODO – tj. w szczególności art. 36 ust. 2 u.o.d.o. z 1997 r. oraz przepisy rozporządzenia z 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych – w sposób jednoznaczny określały formę i zakres dokumentacji, do prowadzenia której zobligowany był administrator. Szczególne znaczenie w tym zakresie miał § 3 ust. 1 r.d.p.d.o., zgodnie z którym na dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych składały się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Minimalne wymagania w odniesieniu do treści tych dokumentów określone zostały w § 4 i 5 r.d.p.d.o. Zgodnie z tą regulacją polityka bezpieczeństwa miała zawierać w szczególności: 1) wykaz budynków; pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe; 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi; 4) sposób przepływu danych pomiędzy poszczególnymi systemami; 5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Z kolei instrukcja zarządzania systemem informatycznym miała obejmować w szczególności: 1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności; 2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem; 3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu; 4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania; 5) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych; 6) sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania,

którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego; 7) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. Opracowanie polityki i instrukcji obejmujących wyżej wymienione obszary pozwalały więc administratorowi spełnić wymogi formalne w zakresie prowadzonej dokumentacji.

Odmiennie sytuacja kształtuje się na gruncie RODO. Przepisy rozporządzenia nie zawierają wymogu opracowania i wdrożenia polityki ochrony danych osobowych[1]. Nie wskazują również, jaki zakres merytoryczny powinna taka dokumentacja zawierać, w przypadku gdy zostanie opracowana przez administratora. RODO pozostawia administratorowi w tym zakresie duży zakres swobody. Istotny wpływ na zakres informacji, jakie mogą być zawarte w polityce ochrony danych osobowych na gruncie RODO, ma jednak jego art. 24[2]. Przewiduje on, że administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby był w stanie to wykazać. Przepis ten wskazuje wyraźnie, że jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te mogą obejmować wdrożenie przez administratora odpowiednich polityk ochrony danych. Pomimo fakultatywnego charakteru prowadzonych polityk opracowanie odpowiedniej dokumentacji dostosowanej do specyfiki działalności jest zalecane jako środek minimalizujący ryzyko naruszenia przepisów RODO i pozwalający na zwiększenie ochrony prywatności osób fizycznych.

2.2. Struktura polityki

RODO nie przewiduje żadnych wymogów w zakresie struktury i formy polityki ochrony danych osobowych. Pojęcie „polityki ochrony danych", którym posłużono się w tekście rozporządzenia, również nie zostało zdefiniowane, co może prowadzić do różnych interpretacji w tym zakresie. Należy się zgodzić z wyrażanym w literaturze poglądem, zgodnie z którym „przez to pojęcie rozumieć można strategię ochrony danych, a więc przemyślany plan działań w dziedzinie ochrony danych, mający umożliwić osiągnięcie celu, jakim jest skuteczna ochrona danych"[3]. Zgodnie z tym założeniem możliwe są dwa podejścia przy planowaniu struktury polityki ochrony danych:

a) rozumienie polityki jako ogólnego dokumentu wskazującego podstawowe założenia i cele, natomiast nie jako aktu normującego szczegółowe zagadnienia związane z technicznymi i organizacyjnymi środkami zabezpieczenia danych[4];

[1] Zob. m.in. P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, komentarz do art. 24.

[2] W literaturze wyrażona została nawet wątpliwość, czy art. 24 ust. 2 RODO w zakresie, w jakim odnosi się do polityk ochrony danych, można uznać za swoisty odpowiednik art. 36 ust. 2 u.o.d.o. z 1997 r. (zob. P. Fajgielski, *Ogólne rozporządzenie...*, komentarz do art. 24).

[3] Zob. m.in. P. Fajgielski, *Ogólne rozporządzenie...*, komentarz do art. 24.

[4] Zob. m.in. P. Fajgielski, *Ogólne rozporządzenie...*, komentarz do art. 24.

b) szersze rozumienie polityki ochrony danych, tj. jako całokształtu procedur i reguł dotyczących ochrony danych osobowych w organizacji, składającego się z dwóch części:
   - części ogólnej polityki, określającej podstawowe zasady, cele i reguły przetwarzania i ochrony danych osobowych,
   - części szczegółowej polityki, obejmującej zbiór załączników, na które składają się wszystkie procedury, rejestry i narzędzia dotyczące określonych obszarów związanych z ochroną danych, w tym związane z technicznymi i organizacyjnymi środkami zabezpieczenia danych.

Niniejsze opracowanie bazuje na drugim z zaprezentowanych podejść, zgodnie z którym na politykę ochrony danych składa się zarówno dokument regulujący podstawowe cele i zasady ochrony danych, jak i zbiór szczegółowych procedur i narzędzi, które doprecyzowują i rozwijają te generalne cele i zasady. Dlatego też w dalszej części opracowania jako propozycję wzorcowej polityki ochrony danych przedstawiono zarówno ogólną część polityki (wzór 2.1), jak i przykładowe procedury dotyczące określonych wybranych zagadnień (wzory 2.2–2.5).

Możliwe jest również przyjęcie odmiennego podejścia i traktowanie polityki ochrony danych jako dokumentu odrębnego, niezwiązanego bezpośrednio ze szczegółowymi regulacjami dotyczącymi poszczególnych obszarów i środków ochrony danych wdrożonych w organizacji (w takim przypadku do stworzenia polityki także można wykorzystać wzór 2.1).

2.3. Zakres przedmiotowy polityki

RODO nie przesądza, jaki zakres merytoryczny powinien zostać objęty polityką ochrony danych, w przypadku gdy administrator podejmuje decyzję o jej opracowaniu i wdrożeniu. Zawarcie w polityce określonych regulacji powinno być więc uzależnione od oceny administratora co do użyteczności poszczególnych jej elementów z punktu widzenia realizacji nałożonych na niego obowiązków oraz proporcjonalne w stosunku do czynności przetwarzania[5]. Podejmując decyzję odnośnie do jej zakresu, administrator powinien uwzględnić w szczególności:

a) elementy wskazane w art. 24 ust. 1 RODO (a zatem charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych), a także stan techniki oraz koszty wdrożenia odpowiednich rozwiązań (zgodnie z art. 25 ust. 1 RODO)[6]. W praktyce wiąże się to z koniecznością dostosowania

[5] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018, komentarz do art. 24.

[6] E. Bielak-Jomaa [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, komentarz do art. 24.

wdrażanych zabezpieczeń m.in. do: rodzaju danych (czy są to dane „zwykłe", czy też szczególne kategorie danych); sposobu przetwarzania danych (czy dane są przetwarzane w wydzielonej sieci zamkniętej, czy przez ogólnodostępną sieć Internet) oraz ryzyka, jakie wiąże się z przetwarzaniem[7]. Ten ostatni wymóg związany jest z generalną zasadą przewidzianą w RODO, tj. tzw. podejściem opartym na ryzyku (ang. *risk based approach*). Zgodnie z podejściem prezentowanym przez organ nadzorczy zasada podejścia opartego na ryzyku oznacza, że podmiotom odpowiedzialnym za przetwarzanie danych nie wskazuje się ściśle określonych środków i procedur w zakresie bezpieczeństwa, np. kontroli dostępu, szyfrowania, rozliczalności czy sposobu monitorowania procesów przetwarzania. Zamiast tego zobowiązuje się je do samodzielnego przeprowadzania szczegółowej analizy prowadzonych procesów przetwarzania danych i dokonywania samodzielnej oceny ryzyka, na jakie przetwarzanie danych w konkretnym przypadku jest narażone[8]. Na tej podstawie należy podjąć decyzję o zakresie i charakterze organizacyjnych środków ochrony, w tym polityk i procedur, stosowanych w organizacji;

b) obowiązek realizacji zasady rozliczalności przewidzianej w art. 5 ust. 2 RODO. Grupa Robocza Art. 29 wskazała w swojej opinii, że w celu wykazania zgodności z przepisami administrator powinien przyjąć odpowiednie wewnętrzne procedury i mechanizmy[9]. Podobne stanowisko przedstawił PUODO: „Wymaganie zawarte art. 24 RODO stanowiące, że administrator powinien być w stanie wykazać przestrzegania przepisów RODO, oznacza w praktyce, że sposób przetwarzania danych, związane z nim procedury, jak i zastosowane zabezpieczenia techniczne i organizacyjne, również powinny zostać zawarte w przedmiotowej dokumentacji – jako spełnienie obowiązku wykazania, że przestrzegane są wymagania RODO"[10].

Należy także pamiętać, że w odniesieniu do niektórych obszarów RODO przewiduje pewne wymagania formalne dotyczące dokumentowania, m.in. w zakresie: prowadzenia rejestru czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO; zgłaszania naruszeń ochrony danych do organu nadzorczego, zgodnie z art. 33 ust. 3 RODO; prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO; raportowania dokumentującego wyniki przeprowadzonych ocen skutków dla ochrony danych, zgodnie z art. 35 ust. 7 RODO[11]. Również w tym zakresie RODO nie przesądza, jaki charakter powinna mieć i na ile szczegółowa powinna być dokumentacja dotycząca

[7] Zob. m.in. P. Fajgielski, *Ogólne rozporządzenie...*, komentarz do art. 24.

[8] GIODO, *Jak rozumieć podejście oparte na ryzyku?*, grudzień 2017, s. 4, https://giodo.gov.pl/pl/1520282/10294 (dostęp: 20.04.2022 r.).

[9] Tak m.in. Grupa Robocza Art. 29 w opinii 3/2010 w sprawie zasady rozliczalności z 13.07.2010 r., WP 173, https://archiwum.giodo.gov.pl/1520057 (dostęp: 20.04.2022 r.).

[10] Zob. wytyczne PUODO, *Dokumentacja przetwarzania danych osobowych zgodnie z RODO*, https://uodo.gov.pl/pl/138/273 (dostęp: 20.04.2022 r.).

[11] Zob. wytyczne PUODO, *Dokumentacja przetwarzania...*

wskazanych zagadnień (formalny wymóg dotyczy jedynie rejestru czynności przetwarzania oraz rejestru kategorii czynności przetwarzania). Prowadzona przez administratora polityka ochrony danych osobowych powinna jednak zasadniczo uwzględniać wymienione wyżej obszary.

Zgodnie z zaprezentowanym podejściem polityka ochrony danych może składać się dwóch zasadniczych elementów: części ogólnej i części szczegółowej. Podstawowe cele i zasady ochrony danych osobowych, które powinny zostać uwzględnione w ogólnej części polityki, mają w istotnym zakresie charakter uniwersalny (tj. znajdą zastosowanie do przetwarzania danych osobowych przez różnego typu administratorów), wynikają bowiem z konieczności przestrzegania wymogów przewidzianych w RODO. Należy do nich zaliczyć[12]:

a) stosowanie się do ogólnych zasad przetwarzania określonych w art. 5 RODO;
b) zapewnienie, aby dane przetwarzane były zgodnie z prawem (art. 6–11 RODO);
c) zapewnienie, aby przestrzegane były prawa osób, których dane są przetwarzane (art. 12–23 RODO);
d) zapewnienie wypełniania ogólnych obowiązków w zakresie przetwarzania danych ciążących na administratorze i podmiocie przetwarzającym (art. 24–31 RODO);
e) zapewnienie bezpieczeństwa przetwarzania danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania danych (art. 32–36 RODO);
f) zapewnienie kontroli nad przetwarzaniem danych w postaci monitorowania przestrzegania przepisów i przyjętych procedur przetwarzania przez inspektora ochrony danych lub podmioty certyfikujące czy monitorujące przestrzeganie przyjętych kodeksów postępowania (art. 27–43 RODO);
g) stosowanie się do wymagań w zakresie przekazywania danych do państw trzecich i instytucji międzynarodowych (art. 44–49 RODO).

W praktyce zagadnienia te mogą zatem zostać uwzględnione w ogólnej części polityki ochrony danych osobowych, której przykład stanowi wzór nr 2.1.

Konkretne rejestry, procedury i narzędzia, które w myśl prezentowanego w niniejszym opracowaniu podejścia stanowią szczegółową część polityki ochrony danych, powinny z kolei być dostosowane do konkretnej organizacji. Przy ocenie zasadności tworzenia określonych dokumentów i ustalaniu poziomu ich szczegółowości należy wziąć pod uwagę wiele czynników, takich jak m.in.: wielkość organizacji (w tym liczbę zatrudnionych osób oraz charakter zatrudnienia), strukturę organizacyjną (w tym występujące w organizacji powiązania kapitałowe oraz liczbę departamentów/działów funkcjonujących w organizacji), przedmiot działalności oraz liczbę i zakres procesów przetwarzania danych (w tym różnorodność świadczonych usług i rodzaj danych wykorzystywanych w procesach) itd.

[12] Zob. wytyczne PUODO, *Dokumentacja przetwarzania...*

Nie jest zatem możliwe stworzenie na gruncie RODO enumeratywnego katalogu procedur i narzędzi, które należy opracować i wdrożyć w organizacji. W każdym przypadku należy dokonać oceny, czy określona dokumentacja jest niezbędna lub przydatna do zapewnienia bezpieczeństwa danych i wykazania przed organem nadzorczym zgodności ich przetwarzania z wymogami prawa. Do stosowanych przez przedsiębiorców w praktyce dokumentów składających się na politykę ochrony danych na gruncie RODO można zaliczyć[13]:

a) **rejestr czynności przetwarzania danych osobowych** (w przypadku administratorów) oraz **rejestr kategorii czynności przetwarzania** (w przypadku procesorów). Prowadzenie rejestrów jest co do zasady obowiązkowe. Wymóg prowadzenia rejestru nie ma jednak zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO. Ze względu na wagę tego zagadnienia zostanie ono rozwinięte w rozdziale 5;
b) **procedurę oceny ryzyka i oceny skutków przetwarzania danych osobowych**. Procedura określa zasady realizacji obowiązków wynikających z RODO w zakresie oceny ryzyka naruszenia praw lub wolności podmiotów danych oraz sposób prowadzenia oceny skutków dla ochrony danych, o której mowa w art. 35 RODO. Zgodnie ze stanowiskiem PUODO dokumentacja powinna w szczególności uwzględniać raporty dokumentujące wyniki przeprowadzonych ocen skutków dla ochrony danych (art. 35 ust. 7 RODO)[14]. Ze względu na wagę wskazanych zagadnień zostaną ono rozwinięte w rozdziałach 3–4;
c) **procedurę oceny i notyfikacji naruszeń ochrony danych osobowych** wraz z **rejestrem naruszeń ochrony danych osobowych**. Procedura określa zasady identyfikacji i oceny naruszeń ochrony danych oraz sposób ich notyfikacji organowi nadzorczemu oraz podmiotom danych, w zakresie określonym w RODO. Określa ona również zasady prowadzenia rejestru naruszeń. Zgodnie ze stanowiskiem PUODO procedury dotyczące zgłaszania naruszeń ochrony danych do organu nadzorczego (art. 33 ust. 3 RODO) oraz procedury dotyczące prowadzenia wewnętrznego rejestru naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO, powinny zostać wdrożone w organizacji[15]. Ze względu na wagę tego zagadnienia zostanie ono rozwinięte w rozdziale 6;
d) **procedurę retencji danych osobowych**. Procedura stanowi sposób realizacji zasady ograniczenia przechowywania danych przewidzianej w art. 5 ust. 1 lit. e RODO, która wymusza przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż

[13] Pogląd ten jest oparty na doświadczeniach zawodowych autora.
[14] Zob. wytyczne PUODO, *Dokumentacja przetwarzania...*
[15] Zob. wytyczne PUODO, *Dokumentacja przetwarzania...*

jest to niezbędne do celów, w których dane te są przetwarzane. Procedura określa w szczególności zasady usuwania (anonimizowania) danych osobowych oraz okresy ich przetwarzania w zależności od celu przetwarzania. Zasady dotyczące retencji danych zostały omówione w pkt 2.6 poniżej, natomiast przykład procedury retencji danych osobowych stanowi wzór 2.2;

e) **procedurę obsługi żądań podmiotów danych** wraz z **rejestrem żądań podmiotów danych**. Procedura określa zasady obsługi (przyjmowania i rozpoznawania) żądań osób fizycznych dotyczących realizacji praw podmiotów danych, o których mowa w art. 12–23 RODO, w tym m.in. zasady przyjmowania żądań, terminy i sposoby ich realizacji oraz zasady identyfikowania wnioskodawców. Proces obsługi żądań został omówiony w pkt 2.6 poniżej. Przykład procedury obsługi żądań oraz rejestru żądań stanowi wzór 2.3;

f) **procedurę współpracy z organem nadzorczym**. Procedura określa zasady postępowania w zakresie wymagającym współpracy z organem nadzorczym, w tym w szczególności postępowania kontrolnego prowadzonego w oparciu o przepisy ustawy z 10.05.1997 r. o ochronie danych osobowych oraz postępowań administracyjnych i sądowoadministracyjnych. Przykład procedury współpracy z organem nadzorczym stanowi wzór 2.4;

g) **procedurę wyboru dostawcy przetwarzającego dane osobowe** wraz z **rejestrem podmiotów przetwarzających**. Procedura określa zasady weryfikacji dostawcy w zakresie gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych oraz ochrony praw osób, których dane dotyczą. Procedura i rejestr stanowią realizację obowiązku wynikającego z art. 28 RODO, zgodnie z którym administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków, by przetwarzanie spełniało wymogi RODO i chroniło prawa podmiotów danych. Procedura może w szczególności zawierać wykaz informacji i czynników, które powinny być brane pod uwagę przy weryfikacji podmiotów pośredniczących. Praktyczne wskazówki dotyczące procesu wyboru dostawcy znajdują się w pkt 2.6 poniżej, natomiast przykład procedury wyboru dostawcy stanowi wzór 2.5;

h) **plan utrzymania zgodności oraz prowadzenia audytów wewnętrznych**. Plan określa harmonogram oraz zakres zadań związanych z zapewnieniem przez administratora stałej zgodności z RODO i pozostałymi przepisami z zakresu danych osobowych. Obejmuje m.in. podział obowiązków poszczególnych osób odpowiedzialnych za realizację określonych zadań; zasady monitorowania i audytu polityk oraz procedur wewnętrznych oraz sposobu ich realizowania w organizacji; plan działań zwiększających świadomość personelu uczestniczącego w operacjach przetwarzania (szkolenia) itd. Ze względu na wagę tego zagadnienia zostanie ono rozwinięte w rozdziale 7.

2.4. Szczegółowa część polityki – uwagi praktyczne

Poszczególne procedury stanowiące szczegółową część polityki ochrony danych osobowych powinny odzwierciedlać rzeczywiste procesy operacyjne realizowane przez administratora. Przez procesy operacyjne należy rozumieć zbiór działań, które podejmowane są w celu bieżącego wykonywania poszczególnych obowiązków nałożonych na administratora przez RODO (np. obowiązku dokonywania oceny naruszeń ochrony danych osobowych, obowiązku obsługiwania żądań podmiotów danych czy obowiązku doboru zabezpieczeń odpowiednich do poziomu ryzyka związanego z przetwarzaniem danych osobowych). Sposób ukształtowania procesów operacyjnych w poszczególnych organizacjach może się jednak znacznie różnić. Różnice te mogą wynikać z wielu okoliczności, które należy uwzględnić, przygotowując procedury wewnętrzne.

Po pierwsze, w procesie opracowywania procedur należy uwzględnić strukturę organizacyjną administratora oraz liczebność i strukturę zespołu ochrony danych osobowych, o ile zespół taki istnieje (w wielu organizacjach za realizację zadań wynikających z RODO odpowiada jedna osoba, często świadcząca usługi na zasadzie outsourcingu, co też będzie miało wpływ na kształt procedur). Znaczenie w tym kontekście będzie miała w szczególności liczba merytorycznych jednostek organizacyjnych funkcjonujących w organizacji (np. dział zakupów, marketingu, sprzedaży, logistyki, HR itd.), usytuowanie w strukturze organizacyjnej takich jednostek, jak: dział prawny, dział *compliance*, dział bezpieczeństwa czy dział IT oraz relacje między zespołem ochrony danych (ewentualnie specjalistą ds. ochrony danych) a tymi działami. Okoliczności te będą bowiem w istotnym zakresie wpływały na decyzję administratora, czy poszczególne procesy operacyjne powinny być realizowane w modelu scentralizowanym czy zdecentralizowanym, co powinno znaleźć odzwierciedlenie w dokumentacji wewnętrznej:

a) model scentralizowany zakłada, że wszystkie działania podejmowane w ramach bieżącej realizacji procesu operacyjnego realizowane są przez zespół ochrony danych osobowych. Przykładowo wszystkie wnioski podmiotów danych wpływają na skrzynkę pocztową monitorowaną przez zespół ochrony danych i cały proces oceny wniosków oraz udzielenia odpowiedzi realizowany jest przez ten zespół (w określonych przypadkach zespół może być wspierany przez działy merytoryczne, ale wyłącznie na zasadach reaktywnych – inicjatorem wszelkich działań pozostaje jednak zespół ochrony danych). W bieżącą realizację procesu operacyjnego nie są zaangażowane żadne osoby spoza zespołu ds. ochrony danych, więc w procedurach nie trzeba uwzględniać roli takich osób;
b) w modelu zdecentralizowanym dochodzi natomiast do podziału konkretnych zadań pomiędzy zespół ochrony danych a inne osoby funkcjonujące w organizacji, np. przedstawicieli merytorycznych jednostek biznesowych, prawników lub pracowników działu IT wyznaczonych do konkretnych zadań w ramach procesów operacyjnych. W praktyce proces operacyjny obsługi wniosków podmiotów danych może w tym modelu zakładać, że weryfikacja i obsługa wniosku odby-

wa się na poziomie jednostki organizacyjnej, która odpowiada merytorycznie za obsługę podmiotu danych (np. dział sprzedaży czy dział HR), a zespół ochrony danych angażowany jest wyłącznie w pojedynczych przypadkach, wymagających zaawansowanej wiedzy eksperckiej. Model ten wymaga odpowiedniego przygotowania personelu – konieczne jest bowiem zapewnienie odpowiedniego poziomu wiedzy osobom zaangażowanym w realizację procesu, co wiąże się z koniecznością zaplanowania programu szkoleń, przygotowywania instrukcji i innych narzędzi wspomagających wykonywanie zadań oraz wdrożenie odpowiedniego modelu kontroli poprawności wykonywanych działań. Procedury powinny więc w sposób precyzyjny określać role poszczególnych zaangażowanych podmiotów, a administrator powinien podjąć dodatkowe działania, żeby zapewnić efektywność realizowanych zadań.

Po drugie, pod uwagę należy wziąć skalę występowania pojedynczych zdarzeń w ramach poszczególnych procesów operacyjnych (np. nowych projektów wymagających przeprowadzenia analizy ryzyka, nowych podmiotów przetwarzających wymagających zweryfikowania, naruszeń ochrony danych, które należy ocenić itd.). Inaczej bowiem trzeba zaplanować proces operacyjny w przypadku, gdy organizacja musi obsłużyć kilka skarg w skali roku, a inaczej gdy wniosków podmiotów danych pojawia się kilkadziesiąt czy kilkaset. Z jednej strony będzie to miało znaczenie przy wyborze modelu scentralizowanego lub zdecentralizowanego. W przypadku małej skali przypadków nakłady związane z przeszkoleniem personelu, żeby zapewnić odpowiedni poziom wiedzy umożliwiający podział obowiązków pomiędzy zespół ochrony danych a inne osoby w organizacji, będzie nieadekwatny do korzyści wynikających z przyjęcia modelu zdecentralizowanego. Nakład ten może być jednak uzasadniony w sytuacji, gdy skala przypadków jest bardzo duża. Z drugiej strony wolumen spraw może wpływać na merytoryczne aspekty poszczególnych procedur. Przy małej skali nie jest potrzebne optymalizowanie procesów operacyjnych. Przy dużej skali warto proces zautomatyzować, np. przygotowując odpowiednie wzorce odpowiedzi na typowe wnioski podmiotów danych czy przygotowując narzędzia audytowe służące do weryfikacji podmiotu przetwarzającego. Automatyzacja procesu wymaga wprawdzie większego nakładu pracy na etapie wdrożenia procedur, ale może przynieść wymierne korzyści zwiększając, efektywność obsługi procesu operacyjnego w bieżącej działalności.

Po trzecie, na treść procedur mogą wpływać dodatkowe wymogi niewynikające z przepisów RODO. Mogą to być wymogi branżowe (np. specyficzne wymogi dotyczące obsługi naruszeń w prawie telekomunikacyjnym) albo wymogi korporacyjne w przypadku administratorów działających w grupach przedsiębiorstw.

Przy opracowywaniu poszczególnych procedur warto także wziąć pod uwagę inne aspekty, właściwe dla poszczególnych procesów operacyjnych. Poniżej znajdują się bardziej szczegółowe uwagi dotyczące następujących procesów: zapewniania retencji

danych osobowych, obsługi żądań podmiotów danych oraz wyboru dostawcy przetwarzającego dane osobowe. Pozostałe procesy zostały szczegółowo omówione w dalszych rozdziałach niniejszego opracowania.

2.4.1. Procedura retencji danych osobowych

Konieczność wdrożenia procesu operacyjnego zapewniania retencji danych osobowych wynika z zasady ograniczenia przechowywania przewidzianej w art. 5 ust. 1 lit. e RODO. Zasada ta zakłada, że dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. W motywie 39 RODO prawodawca unijny wskazał także, że administrator powinien zapewnić ograniczenie okresu przechowywania danych „do ścisłego minimum". Proces operacyjny mający na celu bieżące zapewnienie ograniczenia przechowywania danych powinien więc zostać ukształtowany w taki sposób, żeby dane rzeczywiście były usuwane po upływie okresu retencji.

Wdrożenie procesu operacyjnego w zakresie retencji danych powinno więc uwzględniać kilka kroków:

1) zinwentaryzowanie istniejących procesów przetwarzania danych – proces usuwania danych po upływie okresu retencji powinien uwzględniać wszystkie czynności przetwarzania danych osobowych realizowane przez administratora; zarządzanie retencją danych wymaga więc prawidłowej identyfikacji czynności przetwarzania; identyfikacja taka może być realizowana poprzez prowadzenie rejestru czynności przetwarzania zgodnie z wymogami art. 30 RODO;
2) określenie okresów retencji dla poszczególnych celów przetwarzania w poszczególnych czynnościach – w przypadku prawidłowej identyfikacji czynności przetwarzania, do każdej czynności należy przypisać cele, w jakich dane są przetwarzane; okresy retencji powinny odnosić się do poszczególnych celów przetwarzania (inny będzie bowiem okres retencji dla danych osobowych gromadzonych w związku z realizacją umowy w celach obsługi posprzedażowej od okresu retencji obejmującego cele podatkowe);
3) przypisanie zasobów (nośników elektronicznych i fizycznych, na których znajdują się dane) w poszczególnych czynnościach – prawidłowa retencja danych zakłada, że po upływie okresu retencji zostaną one usunięte ze wszystkich nośników i lokalizacji w organizacji (a także nośników, za które odpowiadają podmioty przetwarzające); możliwość zarządzania retencją może więc wymagać inwentaryzacji wszystkich zasobów wykorzystywanych w ramach poszczególnych czynności do realizacji określonych celów (np. ustalenia, jakie formularze papierowe są wykorzystywane, z jakich systemów informatycznych korzysta się do realizacji procesu, na jakich nośnikach zewnętrznych pracownicy mogę przechowywać dane itd.);

4) przypisanie okresów retencji dla poszczególnych zasobów – w niektórych przypadkach może okazać się uzasadnione przypisywanie konkretnych okresów retencji do poszczególnych nośników danych; może się bowiem okazać, że część zasobów wykorzystywanych w procesie przetwarzania danych należy przechować dłużej niż pozostałe (np. tylko część dokumentacji zawierającej dane osobowe powinna być przechowywana w celach podatkowych, a reszta powinna być usunięta niezwłocznie po zakończeniu obowiązywania umowy);
5) przypisanie osób odpowiedzialnych za usuwanie danych w poszczególnych procesach lub zasobach – ze względu na strukturę organizacyjną i charakterystykę procesów przetwarzania danych osobowych w konkretnej organizacji może okazać się, że za faktyczne usuwanie danych osobowych powinni odpowiadać pracownicy działów merytorycznych mających bezpośredni dostęp do zasobów zawierających dane osobowe (np. pracownicy HR mogą odpowiadać za usuwanie danych z dokumentacji pracowniczej);
6) opracowanie instrukcji usuwania danych w zasobach i budowanie kompetencji personelu – w przypadku gdy za faktyczne usuwanie danych odpowiadają osoby odpowiedzialne wyznaczone w poszczególnych obszarach merytorycznych, konieczne może okazać się przygotowanie szczegółowych wytycznych (np. w formie instrukcji stanowiskowych) określających zasady postępowania z konkretnymi nośnikami zawierającymi dane osobowe; konieczne jest również budowanie kompetencji u osób, którym przydzielono zadania w ramach procesu operacyjnego;
7) nadzór nad prawidłowością realizowania procesu retencji – w przypadku delegowania zadań na pracowników z działów merytorycznych należy zapewnić odpowiednie instrumenty pozwalające zespołowi ochrony danych na kontrolę, czy proces operacyjny realizowany jest prawidłowo; instrumenty te mogą obejmować np. cykliczne audyty wewnętrzne.

W konsekwencji w procedurze retencji danych osobowych należy uwzględnić w szczególności:

a) precyzyjne okresy retencji dla poszczególnych celów przetwarzania danych osobowych (np. w formie tabeli stanowiącej załącznik do procedury albo poprzez odesłanie do rejestru czynności przetwarzania, w którym ustalone są poszczególne okresy retencji);
b) kryteria ustalania okresów retencji (w szczególności zdarzeń, od których należy liczyć terminy usunięcia danych w ramach poszczególnych celów – np. rozwiązanie umowy, wygaśnięcie stosunku pracy itd.);
c) dopuszczalne metody realizacji retencji – procedura może zakładać, że dane nie muszą być fizycznie usuwane, ale mogą być anonimizowane; procedura może określać konkretne zasady skutecznej anonimizacji danych;
d) role i zakresy odpowiedzialności – w przypadku decentralizacji procesu należy opisać role poszczególnych osób w realizacji procesu;

e) zasady weryfikacji przestrzegania procedury – należy uwzględnić metody kontroli nad prawidłowością realizacji procesu.

2.4.2. Procedura wyboru dostawcy przetwarzającego dane osobowe

Artykuł 28 ust. 1 RODO przewiduje, że w sytuacji, gdy przetwarzanie ma być dokonywane w imieniu administratora, jest on zobowiązany do korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Oznacza to, że to na administratorze ciąży obowiązek zbadania, czy podmiot przetwarzający, który na zlecenie administratora będzie realizował czynności wymagające przetwarzania danych osobowych, spełnia określone wymogi w tym zakresie. Wynika to z faktu, że administrator ponosi odpowiedzialność za zgodność przetwarzania danych osobowych z zasadami RODO. Odpowiedzialność ta rozciąga się nie tylko na sposób i środki przetwarzania stosowane przez niego samodzielnie, ale także na sposób i środki przetwarzania stosowane przez podmiot działający na jego zlecenie. Decydując się na usługi innego podmiotu, administrator odpowiada za bezpieczeństwo przetwarzania, które odbywa się poza jego organizacją. Administrator odpowiada również za nieprzeprowadzenie weryfikacji podmiotu, któremu planuje powierzyć przetwarzanie danych osobowych (dostawcy usług).

Co zatem należy zweryfikować i czym są właściwe gwarancje? Po pierwsze, weryfikacja powinna obejmować przestrzeganie przez podmiot przetwarzający wymogów prawnych obejmujących m.in. prawidłowy sposób prowadzenia rejestrów (w tym rejestru kategorii czynności przetwarzania), nadawanie upoważnień do przetwarzania dla wszystkich pracowników i współpracowników, stosowanie właściwych mechanizmów legalizujących transfer danych do państw trzecich (jeśli transfer ma miejsce), powołanie inspektora ochrony danych osobowych (o ile jest to konieczne) itd. Po drugie, weryfikacja może objąć poziom wiedzy po stronie pracowników podmiotu przetwarzającego, którzy będą zaangażowani w proces, m.in. poprzez zbadanie, czy istnieje dokumentacja ochrony danych osobowych, z którą pracownicy podmiotu przetwarzającego mogą się zapoznać, czy podmiot przetwarzający dba, aby budować świadomość pracowników w zakresie bezpieczeństwa danych (np. przez szkolenia onboardingowe i okresowe), czy kompetencje i kwalifikacje IOD (jeżeli istniał wymóg jego powołania) lub osoby odpowiadającej w organizacji za obszar ochrony danych osobowych są wystarczające itd. Po trzecie, sprawdzenie może dotyczyć wiarygodności podmiotu przetwarzającego, m.in. poprzez weryfikację, czy procesor posiada certyfikaty z zakresu bezpieczeństwa informacji, czy wdrożył prawidłowe mechanizmy identyfikacji naruszeń ochrony danych osobowych, czy były prowadzone wobec podmiotu przetwarzającego kontrole i postępowania przed

PUODO i jaki był ich wynik, czy były prowadzone kontrole lub audyty przez niezależne podmioty i jakie przyniosły rezultaty itd. Po czwarte, należy zweryfikować wdrożone środki techniczne i organizacyjne odpowiadające wymogom RODO, np. czy stosowany jest system kontroli dostępu do obszaru przetwarzania danych, czy zdefiniowano zasady nadawania uprawnień i dostępu do systemów informatycznych, czy istnieje polityka haseł (określono strukturę haseł, częstotliwość zmiany itp.), czy stosowane jest oprogramowanie antywirusowe, czy określono zasady dostępu do sprzętu mobilnego i zasady zabezpieczania tego sprzętu, czy określono zasady sporządzania i przechowywania kopii zapasowych, czy zapewniono zdolność szybkiego przywracania dostępu do danych w sytuacji incydentu fizycznego lub technicznego, jakie wdrożono inne środki gwarantujące poufność, integralność i dostępność danych osobowych.

Elementów wymagających weryfikacji jest wiele. Powstaje wiec pytanie, w jaki sposób należy ją realizować. Istnieją różne metody weryfikacji i to administrator powinien podjąć decyzję, która z nich będzie adekwatna. Powinien przy tym uwzględnić takie elementy jak kontekst i charakterystykę przetwarzania, które będą realizowane przez dostawcę, zakres otsourcowanych czynności itd. Weryfikacja może polegać więc m.in. na:

- weryfikacji podmiotu przetwarzającego na podstawie informacji publikowanych przez dostawcę na jego stronie internetowej lub odpowiedzi na pytania udzielone przez niego na etapie zapytań ofertowych;
- zebraniu opinii i rekomendacji dotyczących współpracy z podmiotem przetwarzającym dostępnych w Internecie i innych publicznych źródłach;
- uzyskaniu informacji od innych podmiotów, np. spółek z grupy kapitałowej administratora, na temat podmiotu przetwarzającego;
- uwzględnieniu własnych historycznych doświadczeń współpracy z konkretnym podmiotem;
- analizie przedłożonych przez podmiot przetwarzający oświadczeń dotyczących wdrożonego systemu zarządzania bezpieczeństwem informacji zgodnego z wymaganiami normy ISO/IEC 27001 lub innymi adekwatnymi normami;
- uzyskaniu oświadczeń podmiotu przetwarzającego;
- analizie udzielonych przez podmiot przetwarzających odpowiedzi na konkretne pytania administratora zawarte w ankietach audytowych;
- audycie przeprowadzonym w siedzibie dostawcy, w tym oględzinach miejsca i infrastruktury obszaru przetwarzania danych oraz analizie wdrożonej dokumentacji itd.

Procedura wyboru dostawcy (podmiotu przetwarzającego) powinna więc określać:

a) warunki i zasady dopuszczalności współpracy z podmiotem przetwarzającym;
b) sposoby weryfikacji podmiotu przetwarzającego – sposoby te mogą być uzależnione od typu procesu powierzanego do przetwarzania;
c) role w procesie weryfikacji podmiotu przetwarzającego – osoby odpowiedzialne za przeprowadzenie procesu, osoby oceniające i zatwierdzające dany podmiot;

d) sposoby dokumentowania przeprowadzonej weryfikacji – sposoby te powinny odzwierciedlać wymogi wynikające z zasady rozliczalności;
e) obowiązek okresowego monitorowania podmiotu przetwarzającego w celu oceny aktualnego poziomu istniejących wcześniej gwarancji.

2.4.3. Procedura obsługi żądań podmiotów danych

Przepisy RODO w art. 15–22 przyznają podmiotom danych wiele uprawnień, takich jak: prawo dostępu do treści danych, prawo uzyskania kopii danych, prawo żądania ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych oraz prawo wniesienia sprzeciwu względem przetwarzania danych. RODO wymaga, żeby administrator podejmował odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem prowadzić z podmiotami danych wszelką komunikację dotyczącą realizacji żądań wynikających z art. 15–22. Administrator powinien udzielać informacji na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Przepisy przewidują także, że administrator ma za zadanie ułatwiać podmiotom danych wykonywanie przysługujących im praw. Administrator może odmówić podjęcia działań na żądanie osoby, której dane dotyczą, tylko w wyjątkowym przypadkach, gdy wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.

Realizacja wniosków podmiotów danych powinna nastąpić bez zbędnej zwłoki, maksymalnie w terminie miesiąca od otrzymania żądania. W razie potrzeby termin ten można wprawdzie przedłużyć o kolejne dwa miesiące, ale musi to być uzasadnione skomplikowanym charakterem żądania lub liczbą żądań. W takim przypadku w terminie miesiąca od otrzymania żądania administrator musi jednak poinformować podmiot danych o przedłużeniu terminu, z podaniem przyczyn opóźnienia.

Administrator powinien udzielić podmiotowi danych informacji o działaniach podjętych w związku ze złożonym żądaniem. Jeżeli administrator nie podejmuje działań w związku z żądaniem podmiotu danych, to jest zobowiązany niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – poinformować podmiot danych o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Proces operacyjny obsługi żądań podmiotów danych oraz procedura wspierająca ten proces powinny więc uwzględniać następujące elementy:
a) zasady weryfikacji tożsamości wnioskodawcy przyjęte przez administratora – zasady te mogą się różnić w zależności do procesu i zakresu danych, które administrator posiada w odniesieniu do podmiotów danych;
b) role i odpowiedzialność poszczególnych osób zaangażowanych w proces obsługi żądań – w przypadku realizacji procesu w sposób zdecentralizowany przypisa-

nie odpowiedzialności powinno być szczegółowe ze względu na przewidziane w RODO terminy realizacji wniosków;
c) terminy realizacji poszczególnych zadań – obsługa żądań wymaga często podjęcia licznych czynności przez różne osoby w organizacji (działy merytoryczne, dział IT itd.); w niektórych przypadkach procedura może więc określać szczegółowe terminy na wykonywanie określonych czynności;
d) stosowanie wzorów odpowiedzi – przygotowanie szablonów odpowiedzi dotyczących typowych żądań podmiotów danych może mieć szczególne znaczenie w organizacjach, gdzie skala żądań jest bardzo duża; z jednej strony pozwoli to zoptymalizować proces obsługi, z drugiej zaś zapewni spójność rozstrzygnięć w podobnych przypadkach;
e) prowadzenie ewidencji wniosków – prawidłowe prowadzenie ewidencji wniosków jest bardzo istotne, ponieważ sposób realizacji wniosków jest badany podczas kontroli PUODO; administrator powinien być w stanie udokumentować cały przebieg obsługi żądania – od momentu wpływu wniosku do organizacji do momentu udzielenia odpowiedzi podmiotowi danych.

2.5. Możliwe rozszerzenie treści polityki

Elementem szeroko pojętej polityki ochrony danych osobowych mogą być również inne regulacje, wzory, narzędzia i mechanizmy stosowane przez administratora, wspierające go w realizowaniu wymogów nakładanych przez przepisy prawa.

Do instrumentów tych można zaliczyć:
a) opis środków bezpieczeństwa ochrony danych oraz zasady ich dokumentowania. Dokument ten powinien określać techniczne, fizyczne oraz organizacyjne środki bezpieczeństwa ochrony danych wdrożonych w organizacji. W tym zakresie można wykorzystać wykazy środków ochrony, które były elementem polityki bezpieczeństwa, prowadzonej na gruncie dotychczasowych przepisów;
b) regulacje, polityki i procedury dotyczące m.in.: zasad nadawania upoważnień, udzielania dostępu do systemów IT przetwarzających dane osobowe, zarządzania polityką haseł oraz incydentami, stosowania kryptografii i pseudonimizacji; zasad rozpoczęcia, zawieszenia i zakończenia pracy w systemach IT, stosowanych metod i środków uwierzytelnienia w systemach, wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych, tworzenia kopii zapasowych baz danych; wymogów w zakresie utrzymania ciągłości działania i zarządzania bezpieczeństwem sieci oraz systemami IT. Do opracowania tego rodzaju dokumentacji administrator wykorzystać może w szczególności rozwiązania przyjęte w instrukcji zarządzania systemem informacyjnym, która w przypadku gdy spełniała wymogi przewidziane w dotychczasowych przepisach, regulowała wiele ww. obszarów;

c) wzory stosowanych umów, m.in. umów powierzenia danych osobowych zgodnie z art. 28 RODO; umów transferowych: administrator – administrator i administrator – podmiot przetwarzający, bazujących na klauzulach modelowych stanowiących załącznik do decyzji Komisji nr 2004/915/WE, umów intragrupowych, w przypadku podmiotów działających w ramach grup kapitałowych; porozumień o udostępnianiu danych oraz o współadministrowaniu danymi itd.;
d) dokumentację pracowniczą (np. polityki korzystania ze sprzętu służbowego, polityki korzystania z własnego sprzętu na potrzeby realizowania zadań służbowych – BYOD);
e) wzory klauzul informacyjnych realizujące wymogi z art. 13 i 14 RODO, polityki prywatności stosowane przez administratora, np. w związku ze świadczeniem usług drogą elektroniczną itd.

2.6. Polityka w świetle dotychczasowej dokumentacji

Jak zostało już wskazane, przepis art. 36 ust. 2 u.o.d.o. z 1997 r. nakładał na administratora obowiązek prowadzenia dokumentacji przetwarzania i ochrony danych, na którą zgodnie z przepisami rozporządzenia z 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych składała się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych.

Po wejściu w życie RODO wdrożenie ww. dokumentów w organizacji nie jest już obligatoryjne. Nie oznacza to jednak, że w praktyce konieczne jest zrezygnowanie z ich prowadzenia, co zostało już wskazane powyżej. Rezygnacja oznaczałaby bowiem często konieczność konstruowania zasad i procedur ochrony danych osobowych od początku, co nie jest uzasadnione z praktycznych względów, a także nie jest spójne z założeniami reformy, które miały na celu kontynuację i doskonalenie dotychczasowych rozwiązań[16]. Kierunek ten potwierdza stanowisko PUODO, zdaniem którego obecnie prowadzona dokumentacja z powodzeniem może być wykorzystana w celu stworzenia dokumentacji, której celem będzie wykazanie zgodności realizowanych procesów przetwarzania z wymaganiami RODO[17].

Dokumenty funkcjonujące w organizacji na gruncie starych przepisów powinny być jednak dostosowane do nowych wymogów przewidzianych w RODO[18]. Dostosowanie może w szczególności polegać na:

[16] Zob. m.in. P. Fajgielski, *Ogólne rozporządzenie...*, komentarz do art. 24.

[17] Zob. wytyczne PUODO, *Dokumentacja przetwarzania...*

[18] Zob. m.in. P. Fajgielski, *Ogólne rozporządzenie...*, komentarz do art. 24. Na konieczność odpowiedniego dostosowania dotychczasowej dokumentacji w zakresie wynikającym z oceny ryzyka oraz charak-

a) modyfikacji polityki bezpieczeństwa poprzez uczynienie z niej dokumentu ogólnego, wskazującego założenia i cele ochrony danych[19]. W tym celu można wykorzystać w szczególności wzór 2.1;
b) uzupełnieniu (o ile wymagają tego przepisy RODO) dotychczas stosowanej dokumentacji o nowe elementy, takie jak: rejestr czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO; procedury dotyczące zgłaszania naruszeń ochrony danych do organu nadzorczego (art. 33 ust. 3 RODO); procedury dotyczące prowadzenia wewnętrznego rejestru naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO; raporty dokumentujące wyniki przeprowadzonych ocen skutków dla ochrony danych (art. 35 ust. 7 RODO)[20];
c) uzupełnieniu dotychczas stosowanej dokumentacji o inne procedury, rejestry i narzędzia pozwalające na realizację przez administratora podejścia opartego na ryzyku i zapewnienie rozliczalności, takie jak np.: procedura retencji danych osobowych, procedura obsługi żądań podmiotów danych, rejestr żądań dotyczących praw podmiotów danych, procedura współpracy z organem nadzorczym, procedura wyboru dostawcy przetwarzającego dane osobowe, plan utrzymania zgodności oraz prowadzenia audytów wewnętrznych itd.;
d) weryfikacji, czy wszystkie elementy dotychczas stosowanej dokumentacji znajdują uzasadnienie w świetle wymogów RODO. Przykładowo przewidziany w § 4 pkt 2 i 3 r.d.p.d.o. wymóg zamieszczenia w polityce bezpieczeństwa wykazu zbiorów danych osobowych oraz opisu ich struktury wskazującego zawartość poszczególnych pól informacyjnych i powiązania między nimi poddawany był na gruncie poprzednio obowiązujących przepisów krytyce jako z jednej strony niemający istotnego znaczenia dla ochrony danych, a z drugiej nakładający na administratorów uciążliwe obowiązki, których spełnienie w praktyce było bardzo pracochłonne, a niekiedy nawet trudne do wykonania[21]. Wydaje się więc, że zamieszczanie tego elementu w nowej dokumentacji nie będzie celowe. Z kolei takie elementy, jak przewidziane w § 4 pkt 1, 4 i 5 r.d.p.d.o.: wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; opis przepływu danych między systemami oraz specyfikacje środków organizacyjnych i technicznych zastosowanych do ochrony przetwarzanych danych, będą mogły często zostać przeniesione do nowej dokumentacji jako informacje pozwalające na wykazanie, że administrator prawidłowo przeprowadził

teru, zakresu, kontekstu i celów przetwarzania zwraca również uwagę E. Bielak-Jomaa, *RODO. Ogólne...*, komentarz do art. 24, oraz K. Wygoda [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, komentarz do art. 24. Pogląd taki wyraził również PUODO, zob. wytyczne PUODO, *Dokumentacja przetwarzania...*

[19] Zob. m.in. P. Fajgielski, *Ogólne rozporządzenie...*, komentarz do art. 24.

[20] Zob. wytyczne PUODO, *Dokumentacja przetwarzania...*

[21] Zob. P. Fajgielski, *Obowiązki związane z zabezpieczeniem danych osobowych* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, red. P. Fajgielski, Lublin 2008, s. 141 i n.

ocenę adekwatności środków ochrony na gruncie RODO[22]. Podobnie instrukcja zarządzania systemem informatycznym, opracowana zgodnie z § 5 r.d.p.d.o., może być przez administratora wykorzystana, po uprzedniej weryfikacji jej aktualności i adekwatności, do oceny zidentyfikowanego ryzyka w odniesieniu do przetwarzania danych osobowych.

2.7. Wzory

Wzór 2.1. Polityka ochrony danych osobowych

1. Definicje

1.1. Administrator – …….

1.2. Dane osobowe – informacje o osobie fizycznej zidentyfikowanej lub możliwej do zidentyfikowania poprzez jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość, w tym wizerunek, nagranie głosu, dane kontaktowe, dane o lokalizacji, informacje zawarte w korespondencji, informacje gromadzone za pośrednictwem sprzętu rejestrującego lub innej podobnej technologii.

1.3. Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez Administratora, nadzorująca przestrzeganie przepisów o ochronie Danych osobowych w organizacji Administratora, wykonująca zadania określone w art. 39 RODO.
albo
Koordynator Ochrony Danych Osobowych (KODO) – osoba wyznaczona przez Administratora, realizująca w organizacji Administratora zadania związane z zapewnieniem zgodności przetwarzania Danych osobowych z obowiązującym prawem.

1.4. Organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych lub ewentualnie właściwy organ nadzorczy w zakresie Danych osobowych wyznaczony przez inne państwo członkowskie Unii Europejskiej.

1.5. Podmiot danych – osoba fizyczna, której dotyczą Dane osobowe przetwarzane przez Administratora.

1.6. Polityka – niniejsza Polityka ochrony Danych osobowych.

1.7. Pracownik – osoba fizyczna zatrudniona przez Administratora na podstawie umowy o pracę.

1.8. 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.

[22] Zob. wytyczne PUODO, *Dokumentacja przetwarzania...*

1.9. Współpracownik – osoba fizyczna świadcząca na rzecz Administratora usługi na podstawie umowy cywilnoprawnej (np. umowa zlecenia, umowa o dzieło).

2. Zasady ogólne

2.1. Niniejsza Polityka stanowi podstawowy dokument regulujący zasady przetwarzania Danych osobowych przez Administratora.

2.2. Wdrożenie Polityki ma na celu zapewnienie zgodności z RODO procesów przetwarzania Danych osobowych przez Administratora, bez względu na formę (elektroniczną bądź papierową), w jakiej to przetwarzanie następuje.

2.3. W związku z prowadzoną działalnością Administrator zbiera i przetwarza Dane osobowe zgodnie z właściwymi przepisami prawa, w tym w szczególności RODO, i przewidzianymi w nich zasadami przetwarzania, tj.:

2.3.1. Administrator zapewnia, że przetwarzanie przez niego Danych osobowych jest zgodne z prawem i odbywa się w oparciu o jedną z podstaw przetwarzania określonych w RODO, tj. w art. 6 ust. 1, art. 9 ust. 2 albo art. 10 (zasada zgodności z prawem);

2.3.2. Administrator zapewnia rzetelność i przejrzystość przetwarzania Danych osobowych, w szczególności zawsze informuje o przetwarzaniu Danych osobowych w momencie ich zbierania, w tym o celu i podstawie prawnej przetwarzania (zasada rzetelności i przejrzystości);

2.3.3. Administrator zapewnia, że Dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie są przetwarzane dalej w sposób niezgodny z tymi celami (zasada ograniczenia celu);

2.3.4. Administrator zapewnia, że przetwarza dane wyłącznie w zakresie niezbędnym do realizacji celu, dla którego Dane osobowe zostały zebrane (zasada minimalizacji);

2.3.5. Administrator zapewnia, że przetwarzane przez niego Dane osobowe są prawidłowe i w razie potrzeby uaktualniane oraz że podejmuje on wszelkie rozsądne działania, aby Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (zasada prawidłowości);

2.3.6. Administrator zapewnia, że Dane osobowe są przetwarzane tylko przez okres, w jakim jest to niezbędne dla zrealizowania celów przetwarzania (zasada ograniczenia czasowego);

2.3.7. Administrator zapewnia bezpieczeństwo Danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez wdrożenie odpowiednich środków technicznych lub organizacyjnych (zasada integralności i poufności).

2.4. Administrator poprzez odpowiednie środki techniczne i organizacyjne zapewnia możliwość wykazania zgodności przetwarzania Danych osobowych

z RODO oraz pozostałymi przepisami dotyczącymi Danych osobowych (rozliczalność).

2.5. Administrator zapewnia przestrzeganie Polityki przez wszystkich Pracowników oraz Współpracowników Administratora.

3. Organizacja systemu ochrony Danych osobowych

3.1. Przed udzieleniem dostępu do przetwarzania Danych osobowych Administrator zapoznaje każdego Pracownika, Współpracownika lub inne osoby przetwarzające Dane osobowe z jego upoważnienia z Polityką, w tym procedurami i zasadami dotyczącymi ochrony Danych osobowych obowiązującymi w organizacji Administratora.

3.2. Przetwarzanie Danych osobowych przez Pracowników i Współpracowników może odbywać się wyłącznie na podstawie udokumentowanego upoważnienia Administratora. Ponadto Administrator zobowiązuje osoby upoważnione do zachowania poufności Danych osobowych oraz informacji dotyczących zabezpieczeń Danych osobowych, a także do przestrzegania Polityki, w tym procedur i zasad dotyczących ochrony Danych osobowych obowiązujących w organizacji Administratora.

3.3. Administrator wyznacza osobę odpowiedzialną za obszar ochrony Danych osobowych, powierzając jej funkcję IOD/KODO, i zapewnia adekwatne środki oraz zasoby niezbędne do wykonywania powierzonych jej zadań.

3.4. Do zadań IOD/KODO należy w szczególności:

3.4.1. informowanie Administratora oraz Pracowników i Współpracowników, którzy przetwarzają Dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i innych przepisów unijnych lub krajowych o ochronie Danych osobowych oraz doradzanie im w tym zakresie;

3.4.2. monitorowanie przestrzegania przez osoby upoważnione przepisów RODO oraz innych przepisów unijnych i krajowych z zakresu ochrony Danych osobowych, jak również wewnętrznych polityk i procedur wdrożonych u Administratora w tym zakresie;

3.4.3. podejmowanie działań zwiększających świadomość w zakresie ochrony Danych osobowych, w tym szkoleń personelu uczestniczącego w operacjach przetwarzania, oraz prowadzenie powiązanych z tym audytów;

3.4.4. udzielanie, na żądanie, zaleceń co do oceny skutków dla ochrony Danych osobowych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

3.4.5. współpraca z Organem nadzorczym;

3.4.6. pełnienie funkcji punktu kontaktowego dla Organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

3.4.7. ……

3.5. IOD/KODO wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

3.6. Pracownicy i Współpracownicy przetwarzający Dane osobowe są zobowiązani w szczególności do:

3.6.1. przetwarzania Danych osobowych zgodnie z posiadanym upoważnieniem oraz z należytą starannością;

3.6.2. w przypadku zaobserwowania zdarzenia mogącego stanowić naruszenie ochrony Danych osobowych niezwłocznego informowania o nim bezpośredniego przełożonego oraz IOD/KODO na zasadach opisanych w odrębnej procedurze;

3.6.3. uczestnictwa w organizowanych szkoleniach z zakresu ochrony Danych osobowych;

3.6.4. zachowania poufności Danych osobowych oraz informacji na temat sposobu ich zabezpieczenia, zgodnie z podpisaną klauzulą poufności;

3.6.5. ……

4. Bezpieczeństwo Danych osobowych

4.1. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Administrator uwzględnia przy tym stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania.

4.2. Przy ocenie, czy stopień bezpieczeństwa jest odpowiedni, Administrator uwzględnia 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.

4.3. W celu zapewnienia integralności i poufności Danych osobowych Administrator zapewnia dostęp do Danych osobowych jedynie osobom upoważnionym i wyłącznie w zakresie, w jakim jest to niezbędne ze względu na wykonywane przez nie zadania. Administrator stosuje rozwiązania organizacyjne i techniczne w celu zapewnienia, że wszystkie operacje na Danych osobowych są rejestrowane i realizowane tylko przez osoby uprawnione.

4.4. Administrator prowadzi na bieżąco analizę ryzyka związanego z przetwarzaniem Danych osobowych i monitoruje adekwatność stosowanych zabezpieczeń Danych osobowych do identyfikowanych zagrożeń. W razie konieczności Administrator wdraża dodatkowe środki służące zwiększeniu bezpieczeństwa Danych osobowych.

4.5. W przypadku gdy rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym