Uniwersytet Wrocławski

Maciej Błażewski
Jolanta Behr

Środki prawne ochrony danych osobowych

Wrocław 2018

Środki prawne ochrony danych osobowych

Prace Naukowe
Wydziału Prawa, Administracji i Ekonomii
Uniwersytetu Wrocławskiego

Seria: **e-Monografie** Nr 124

Dostęp online: http://www.bibliotekacyfrowa.pl/publication/100544
DOI: 10.23734/23.18.032

Środki prawne ochrony danych osobowych

Maciej Błażewski
dr nauk prawnych
Uniwersytet Wrocławski

Jolanta Behr
dr nauk prawnych
Uniwersytet Wrocławski

Wrocław 2018

Recenzent: *dr hab. Tadeusz Kocowski, prof. UWr*

Zadanie publiczne pod nazwą „Środki prawne ochrony
danych osobowych w prawie polskim" – publikacja.

Projekt współfinansowany z budżetu Województwa Dolnośląskiego.

Korekta: *Dorota Sideropulu*
Projekt i wykonanie okładki: *Karolina Drozd*
Skład i opracowanie techniczne: *Bartłomiej Siedlarz, eBooki.com.pl*

Druk: *Drukarnia Beta-druk, www.betadruk.pl*

Wydawca
E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa.
Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

ISBN 978-83-66066-24-3 (druk)
ISBN 978-83-66066-25-0 (online)

Spis treści

Rozdział V

Rozdział VI

Wykaz ważniejszych skrótów

Źródła prawa

dyrektywa 95/46/WE	dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281 z 23.11.1995 r., Nr 31 ze zm.).
k.c.	ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2018 r. poz. 1025 ze zm.).
Konstytucja RP	Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.).
k.p.	ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2018 r. poz. 917 ze zm.).
k.p.a.	ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2017 r., poz. 1257 ze zm.).
k.p.c.	ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2018 r. poz. 1360 ze zm.).
KPD	Konwencja o prawach dziecka (przyjęta przez Zgromadzenie Ogólne ONZ w dniu 20 listopada 1989 r. (Dz. U. z 1991 r. Nr 120, poz. 526 ze zm.).
KPP	Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 303 z 12.12.2007 r., s. 1 ze zm.).
MPPOiP	Międzynarodowy Pakt Praw Obywatelskich i Politycznych (przyjęty przez Zgromadzenie Ogólne ONZ w dniu 16 grudnia 1966 r. Dz. U. z 1977 r. Nr 38, poz. 167).
PDPCz	Powszechna Deklaracja Praw Człowieka (uchwalona przez Zgromadzenie Ogólne ONZ w dniu 10 grudnia 1948 r. rezolucją 217/III A).
p.p.s.a.	ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2018 r. poz. 1302).
rozporządzenie 2016/679 lub RODO	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016 r. poz. 1).
TFUE	Traktat o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 202 z 07.06.2016 r., s. 47 i n.).
TUE	Traktat o Unii Europejskiej (Dz. Urz. UE C 202 z 7.06.2016 r., s. 13 i n.).
u.o.d.o.	ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 ze zm.).
u.o.d.o.97.	ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133 poz. 883).
u.s.o.z.	ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2017 r. poz. 1398 ze zm.).

Organy administracji publicznej i organy orzekające

KRIO	Kolegium Regionalnej Izby Kontroli
NSA	Naczelny Sąd Administracyjny
Prezes UODO lub Prezes Urzędu	Prezes Urzędu Ochrony Danych Osobowych
SA	Sąd Apelacyjny
SN	Sąd Najwyższy
TK	Trybunał Konstytucyjny
TS	Trybunał Sprawiedliwości
WSA	Wojewódzki Sąd Administracyjny

Publikatory

Dz. U.	Dziennik Ustaw
Dz. Urz. UE C	Dziennik Urzędowy Unii Europejskiej seria C
Dz. Urz. UE L	Dziennik Urzędowy Unii Europejskiej seria L
M. P.	Monitor Polski

Inne skróty

art.	artykuł
BIP	Biuletyn Informacji Publicznej
ePUAP	elektroniczna platforma usług administracji publicznej
lit.	litera
nt.	na temat
pkt	punkt
poz.	pozycja
red. nacz.	redaktor naczelny
red. nauk.	redaktor naukowy
red.	redaktor
s.	strona
sygn.	sygnatura
t.j.	tekst jednolity
ust.	ustęp
ze zm.	ze zmianami
zob.	zobacz

Wstęp

Zapewnienie ochrony danych osobowych jest jedną z bardziej istotnych gwarancji prawnych dla osób fizycznych. Służy ono zachowaniu osobie fizycznej określonej przez nią granicy pomiędzy jej sferą prywatną a sferą publiczną. Ma znaczenie zarówno dla relacji interpersonalnych tej osoby, jak również dla jej relacji zawodowych i gospodarczych[1].

Problematyka ochrony danych osobowych jest szeroko analizowana w nauce prawa, szczególnie aktualnie, w pierwszym okresie obowiązywania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych[2] oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[3], jak również w okresie poprzedzającym, gdy podstawowymi aktami normatywnymi regulującymi tę problematykę były: dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[4] oraz ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[5].

---

[1] Naruszenie danych osobowych może mieć wpływ np. na określenie zdolności kredytowej osoby fizycznej. Zob. M. T. Kłoda, *Naruszenie dóbr osobistych kredytobiorcy jako skutek uchybienia przez bank zasadom przetwarzania danych osobowych*, „Bezpieczny Bank" 2016, Nr 2, s. 162–163.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L z dnia 4 maja 2016 r., Nr 119 poz. 1.

[3] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 ze zm.).

[4] Dz. Urz. UE L z dnia 23 listopada 1995 r. Nr 281, Nr 31 ze zm.

[5] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883).

Monografia zawiera sześć rozdziałów. Pierwsze cztery dotyczą podstawowych zagadnień ochrony danych osobowych: pojęć wprowadzających, źródeł prawa, zasad prawa oraz podmiotów. Dwa kolejne obejmują wyniki analizy przepisów prawa, które dotyczą bezpośrednich i pośrednich środków ochrony danych.

Pierwszy rozdział dotyczy pojęć wprowadzających problematykę ochrony danych osobowych, w tym wyjaśnienia uwarunkowań społeczno-gospodarczych, wpływających na treść i zakres tej ochrony.

Badania środków prawnych ochrony danych osobowych objęły także źródła prawa. Problematyka ta została przedstawiona w rozdziale drugim. Jest ona szczególnie istotna także z powodu ostatnich zmian prawa. Podstawowe źródła prawa powszechnie obowiązującego obejmują akty prawa Unii Europejskiej oraz akty prawa polskiego (krajowego).

Prawo Unii Europejskiej wyraża gwarancję dla ochrony danych osobowych uregulowaną w podstawowych aktach prawnych, takich jak Traktat o funkcjonowaniu Unii Europejskiej gwarantujący ochronę danych osobowych w związku z ich przetwarzaniem i przepływem[6] oraz w Karcie praw podstawowych Unii Europejskiej, która wyraża prawo do życia prywatnego i bardziej szczegółowe prawo do ochrony danych osobowych[7]. Rozwinięte regulacje dotyczące ochrony danych osobowych zawiera natomiast rozporządzenie 2016/679.

Prawo polskie także zapewnia ochronę danych osobowych, zarówno normami Konstytucji RP, gwarantującymi autonomię informacyjną oraz prawo do prywatności[8], jak i normami ustawowymi, do któ-

[6] Artykuł 16 ust. 1–2 wersji skonsolidowanej Traktatu o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 202 z 7.06.2016 r., s. 47 i n.). Zob. E. Czarny-Drożdżejko, *Ochrona danych osobowych w Internecie w świetle orzecznictwa Trybunału Sprawiedliwości*, „Przegląd Sądowy" 2015, Nr 11–12, s. 81.

[7] Artykuł 7–8 Karty praw podstawowych Unii Europejskiej (Dz. Urz. UE C z 12.12.2007 r., Nr 303, s. 1 ze zm.). Zob. E. Czarny-Drożdżejko, *op. cit.*, s. 81.

[8] W świetle art. 51 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.) każdy ma zapewnioną autonomię informacyjną, a zgodnie z art. 47 Konstytucji RP, każdy ma prawo do ochrony prawnej życia prywatnego. Zob. M. T. Kłoda, *op. cit.*,

rych należy zaliczyć m.in. ustawę o ochronie danych osobowych czy Kodeks cywilny[9].

Trzeci rozdział dotyczy zasad ochrony danych osobowych. Służą one prawidłowemu stanowieniu i stosowaniu prawa w tym zakresie. Mają one zatem znaczenie dla interpretacji przepisów dotyczących środków ochrony danych osobowych. Zasady te mają dyrektywalny charakter. Zostały one bezpośrednio wyrażone w rozporządzeniu 2016/679, dzięki czemu łatwiejsze jest wyrażenie ich związku z przepisami prawa.

Czwarty rozdział odnosi się do podmiotów procesu przetwarzania danych osobowych. Są to osoby, których te dane dotyczą, administrator, podmiot przetwarzający, inspektor ochrony danych, Prezes Urzędu Ochrony Danych Osobowych, jako organ nadzorczy oraz podmiot certyfikujący. Badania, których wyniki zostaną przedstawione w tym rozdziale, obejmują status tych podmiotów w procesie przetwarzania oraz ich wzajemne relacje. Prowadzenie badań nad tymi podmiotami jest nieodzowne dla analizy środków ochrony danych, ponieważ podejmują one te środki.

Piąty rozdział obejmuje analizę środków pośrednich ochrony danych osobowych, podejmowanych przez podmioty procesu przetwarzania działające w interesie administratora lub w interesie publicznym. Są to środki techniczne i organizacyjne, środki informacyjne, ocena skutków przetwarzania danych osobowych wraz z konsultacjami z Prezesem

s. 162; B. Czerwińska, *Ochrona danych osobowych a prawo dostępu do dziennika elektronicznego – aspekt formalnoprawny*, „Ogrody Nauk i Sztuk" 2017, Nr 7, s. 103, 104; Ł. Wojciechowski, *Bezpieczeństwo informacji i ochrona danych osobowych jako polityka publiczna – analiza wprowadzenia mechanizmów i uregulowań prawnych*, „Polityka i Społeczeństwo" 2016, Nr 4, s. 87–88; P. Sobczyk, *Ochrona danych osobowych jako element prawa do prywatności*, „Zeszyty Prawnicze" 2009, Nr 9/1, s. 302–312.

[9] Prawo do prywatności nie zostało określone wprost w katalogu dóbr osobistych, wyrażonym w art. 23 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2018 r., poz. 1025 ze zm.), lecz katalog ten ma otwarty charakter, a prawo do prywatności zostało wskazane w innych przepisach szczególnych. Zob. B. Czerwińska, *op. cit*., s. 103. Problematykę ochrony danych osobowych jako dobra osobistego porusza także P. Sobczyk, *op. cit*., s. 300.

Urzędu, rejestrowanie czynności przetwarzania, certyfikat oraz wiążące reguły korporacyjne.

Monografia przedstawia także wyniki badań nad ochroną danych osobowych z perspektywy osoby, której te dane dotyczą, oraz jej bezpośredniej relacji z innymi podmiotami procesu przetwarzania. W szóstym rozdziale została zatem przedstawiona problematyka zgody na przetwarzanie oraz praw osoby, której dane dotyczą, w tym prawa do sprostowania, usunięcia, ograniczenia oraz przenoszenia danych, a także prawa do sprzeciwu wobec przetwarzania danych osobowych, wniesienia skargi do organu nadzorczego oraz ochrony prawnej przed sądem.

Wstępnym założeniem badawczym jest podział środków ochrony danych na pośrednie oraz bezpośrednie. Może on zostać przeprowadzony z uwzględnieniem kryterium podmiotowego. Środki bezpośrednie są podejmowane z inicjatywy osoby, której dane dotyczą, w celu ochrony jej interesu. Środki pośrednie podejmują natomiast inne podmioty procesu przetwarzania, działające w interesie publicznym lub w interesie administratora, lecz obowiązane do podejmowania działań z mocy samego prawa. Należy podkreślić, że każdy z tych środków powinien służyć interesowi osoby, której dane dotyczą.

Monografia ma także wykazać, że celem środków ochrony danych osobowych jest wyważenie interesów występujących w procesie przetwarzania: interesu publicznego, interesu osoby, której dane dotyczą, oraz interesu administratora. Analizie tego wyważenia służy podział na środki bezpośrednie i pośrednie ochrony danych. Wyważenie w przypadku środków bezpośrednich, przysługujących osobie, której dane dotyczą, obejmuje jej interesy oraz interesy administratora. Wyważenie to odrębnie przebiega w przypadku środków pośrednich, które dotyczą interesów publicznego i administratora. Podział tych interesów nie jest całkowicie rozłączny. Jeżeli administratorem jest podmiot publiczny, jego interes może realizować interes publiczny. Wyważenie interesów wpływa na zakres, sposób oraz skutki realizacji środków ochrony danych osobowych.

W pracy zastosowano metodę analityczno-dogmatyczną. Przedmiotem pracy była analiza aktualnie obowiązujących przepisów prawa, w szczególności zawartych w rozporządzeniu 2016/679 oraz w ustawie o ochronie danych osobowych. Interpretację przepisów prawa wzbogacono przedstawieniem dominujących poglądów przedstawicieli nauki prawa oraz orzecznictwem sądów krajowych i europejskich.

Praca uwzględnia stan prawny na dzień 15 sierpnia 2018 r.

Rozdział I

Wprowadzenie do prawa ochrony danych osobowych

1. Dane osobowe w społeczeństwie informacyjnym

(Jolanta Behr)

Od lat 70. XX wieku obserwuje się intensywny rozwój nowych technologii oraz narzędzi informacyjnych i komunikacyjnych[10]. Ze względu na dynamiczne zmiany w tym obszarze twierdzi się, że żyjemy obecnie w dobie „rewolucji elektronicznej", „transformacji digitalnej" i „rozwoju usług teleinformacyjnych"[11]. Zwiększa się dostępność nowych technologii, a korzystanie z nich zyskuje na znaczeniu w przestrzeni publicznej i prywatnej. Dzięki nim bez wychodzenia z domu możemy wykonywać obowiązki służbowe, załatwiać sprawy urzędowe, nabywać towary i usługi oraz komunikować się w czasie rzeczywistym, przesyłając obraz i dźwięk.

Zmiany te wywarły wpływ na funkcjonowanie ludzi w społecznościach. Kontakt w „świecie realnym" zastępuje stopniowo „kontakt wirtualny", sprowadzający się niejednokrotnie do prostego przekazu informacji ujętych w niewielkiej liczbie znaków. Wpływa to na osłabianie więzi społecznych[12].

---

[10] M. Castells, *Społeczeństwo sieci*, Wydawnictwo Naukowe PWN, Warszawa 2008, s. 78.

[11] T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999, s. 31–36.

[12] M. Golka, *Czym jest społeczeństwo informacyjne*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2005, z. 4, s. 253–254 i 258–259.

Twierdzi się, że przemiany te spowodowały powstanie nowego typu społeczeństwa – tzw. społeczeństwa informacyjnego[13] (*jahoka shakai*)[14]. Istotną rolę odgrywa w nim wiedza i informacje. Wiedza jest wykorzystywana dla rozwoju innowacyjności różnych dziedzin. Informacje są natomiast traktowane jak produkt – towar na sprzedaż – będący główną siłą napędową cywilizacji. Zwiększyła się szybkość ich obiegu i liczba ich źródeł. Są one tworzone, gromadzone i przekazywane na niespotykaną dotąd skalę. Coraz większe znaczenie ma umiejętność dokonywania ich selekcji i oceny ich prawidłowości[15]. Odbierane przez ludzi informacje wpływają bowiem na postrzeganie otaczającego ich świata. Niejednokrotnie większe znaczenie od faktów ma wykreowany wizerunek. Coraz większą popularność zyskują więc portale społecznościowe, ułatwiające szybkie przekazywanie starannie wyselekcjonowanych informacji na nasz temat[16]. W społeczeństwie informacyjnym rzeczywistość jest bowiem kreowana przez informacje, które wykorzystuje się również jako „narzędzie" walki społecznej i politycznej.

Informacje nie tworzą jednolitej kategorii, podlegając licznym podziałom. Biorąc pod uwagę ich przedmiot, można wyróżnić m.in. informacje odnoszące się do osób, rzeczy, zjawisk i procesów. Jeśli dotyczą one zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych, są one określane jako „dane osobowe"[17]. Już od pierwszych dni życia człowieka gromadzi się dotyczące go dane. W niektórych przypad-

[13] Zob. szerzej na ten temat: Y. Masuda, *The Information Society as Post-Industrial Society*, World Future Society, Washington D. C. 1980; F. Webster, *Theories of the Information Society*, Routledge Taylor & Francis Group, London – New York 2006, wyd. 3.

[14] Pojęciem tym posłużył się jako pierwszy japoński badacz Tadao Umesao. Spopularyzował je natomiast Kenichi Koyama.

[15] M. Golka, *op. cit*., s. 258-259.

[16] Liczbę ludności świata szacuje się na ok. 7,4 miliarda, a liczbę – aktywnych co najmniej raz w miesiącu – użytkowników jednego z najpopularniejszych portali społecznościowych na 2,3 miliarda, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [dostęp 04.10.2018].

[17] Zob. art. 6 ust. 1 u.o.d.o.97. i art. 4 pkt 1 zd. 1 RODO.

kach jesteśmy nawet prawnie zobowiązani do ich przekazania właściwym organom władzy publicznej[18].

Informacje te przetwarzają[19] podmioty publiczne i niepubliczne. Następuje to na ogromną skalę. Rozpowszechniło się korzystanie z tzw. Big Data, czyli ogromnych ilości różnorodnych i zmiennych danych przetwarzanych błyskawicznie dzięki zastosowaniu nowych technologii[20]. Umożliwia to szybkie wyciąganie wniosków, służących m.in. wprowadzaniu ulepszeń technologicznych i tworzeniu profili osobowych. Sposób i zakres przetwarzania danych i brak kontroli nad podmiotami przetwarzającymi sprawia jednak, że przetwarzanie to jest również źródłem zagrożeń, w szczególności, gdy jest ono dokonywane w niewłaściwym celu, zakresie lub przez nieuprawnione podmioty.

2. Przyczyny ochrony danych osobowych

(Jolanta Behr)

Coraz większe znaczenie zyskuje zatem zapewnienie właściwej ochrony przetwarzanych danych, w szczególności danych osobowych. Ich przetwarzanie może bowiem powodować negatywne konsekwencje dla społeczeństwa (zbiorowości) i dla jego poszczególnych członków.

[18] Zob. np. zakres i tryb gromadzenia informacji w rejestrze PESEL i rejestrze mieszkańców (ustawa z dnia 24 września 2010 r. o ewidencji ludności, t.j. Dz. U. z 2018 r., poz. 1382 ze zm.) oraz obowiązek zgłoszenia urodzenia, małżeństwa i zgonu (ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego, t.j. Dz. U. z 2016 r., poz. 2064 ze zm.).

[19] Przetwarzaniem jest operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, jak np. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (art. 4 pkt 2 RODO).

[20] M. Tabakow, J. Korczak, B. Franczyk, *Big Data – definicje, wyzwania i technologie informatyczne*, „Informatyka Ekonomiczna" 2014, Nr 1(31), s. 141.

Ataki cybernetyczne skutkujące wyciekiem danych do sieci, rozwój przestępczości cybernetycznej, wykradanie tożsamości, nielegalna sprzedaż danych do celów marketingowych oraz niekontrolowane i niezgodne z prawem przetwarzanie tych danych, to tylko niektóre ze zjawisk szkodliwych społecznie, których eliminowanie jest w interesie publicznym. Realizacja zadań z tego obszaru mieści się w zakresie funkcji policyjnej administracji, której celem jest zapewnienie porządku i bezpieczeństwa publicznego[21].

Zapewnienie ochrony danych osobowych ma również istotne znaczenie dla osób fizycznych. Wpływa ono bowiem na skuteczność realizacji prawa do prywatności. Prawo to obejmuje „zasady i reguły odnoszące się do różnych sfer życia jednostki, a ich wspólnym mianownikiem jest przyznanie jednostce prawa «do życia własnym życiem układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej» […]. Tak rozumiana prywatność odnosi się przede wszystkim do życia osobistego, rodzinnego, towarzyskiego i czasem jest określana jako «prawo do pozostawienia w spokoju»"[22].

Artykuł 51 Konstytucji RP stwarza podstawę wyróżnienia trzech głównych wymiarów prawa prywatności: 1) prawa do decydowania o swojej cielesności, 2) prawa do prywatności (autonomii) informacyjnej, 3) prawa do prywatności lokalnej (autonomicznego określania relacji i zachowań w rodzinie, domu i społeczności, do której należymy)[23]. Dla ochrony danych osobowych szczególne znaczenie ma autonomia informacyjna. Jest ona prawem do samodzielnego decydowania przez człowieka o udostępnianiu innym osobom informacji na jego temat i prawem umożliwiającym sprawowanie kontroli nad tymi informacjami, gdy znajdują się one w posiadaniu innych podmiotów. Autonomia ta obejmuje dane o charak-

[21] Zob. szerzej: W. Kawka, *Policja w ujęciu historycznym i współczesnym*, Zakład Administracji i Prawa Administracyjnego U.S.B., Wilno 1939.

[22] Orzeczenie TK z dnia 24 czerwca 1997 r., sygn. K 21/96, LEX nr 29146.

[23] A. Młynarska-Sobaczewska, *Trzy wymiary prywatności. Sfera prywatna i publiczna we współczesnym prawie i teorii społecznej*, „Przegląd Prawa Konstytucyjnego" 2013, nr 1(13), s. 35.

terze personalnym (osobowym) oraz dane dotyczące majątku i sfery ekonomicznej jednostki. Autonomia nie ma jednak charakteru absolutnego. Doznaje ograniczeń w szczególności w relacji „władza publiczna – obywatel". Organy tej władzy mogą pozyskiwać, gromadzić i udostępniać informacje o obywatelach w sposób inny niż w drodze zgłoszenia przez nich tych danych. Może to jednak nastąpić wyłącznie w przypadkach określonych w ustawie, a tak określony zakres gromadzonych danych nie może być kształtowany dowolnie. Podlega on ograniczeniu ze względu na niezbędność informacji w demokratycznym państwie prawnym[24].

Ochrona danych osobowych leży w interesie publicznym i w interesie prywatnym. Zmierza bowiem do zapewnienia realizacji praw osób, których dane dotyczą, oraz do wyeliminowania występowania zjawisk szkodliwych społecznie[25]. Ochronę danych osobowych uznaje się za prawo autonomiczne lub za element (wymiar) prawa do prywatności[26].

3. Wyodrębnianie się prawa ochrony danych osobowych

(Jolanta Behr)

Ochrona danych osobowych jest zagwarantowana przepisami wielu aktów prawnych prawa krajowego i międzynarodowego. Regulacje prawne dotyczące tej materii nie mają długiej historii[27]. Mimo to zakres i sposo-

[24] Wyrok TK z dnia 17 czerwca 2008 r., sygn. K 8/04, LEX nr 387751; wyrok TK z dnia 20 listopada 2002 r., sygn. 41/02, LEX nr 57092.

[25] I. Lipowicz, *Konstytucyjne podstawy ochrony danych osobowych*, [w:] P. Fajgielski (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Wydawnictwo KUL, Lublin 2008, s. 49.

[26] P. Sobczyk, *op. cit*., s. 299–317.

[27] Od uchwalenia pierwszych europejskich regulacji prawnych dotyczących ochrony danych osobowych minęło niespełna pięćdziesiąt lat. Mowa przede wszystkim o: ustawie parlamentu Hesji z 1970 r.; ustawie szwedzkiej z 1973 r.; ustawie federalnej RFN z 1977 r.; francuskiej ustawie o informatyce, kartotekach i wolnościach obywatelskich z 1978 r.; duńskich ustawach z dotyczących rejestrów publicznych i prywatnych rejestrów danych z 1978 r.; austriackiej usta-

by ochrony uległy istotnej zmianie, a liczba aktów prawnych poświęconych tej kwestii stale wzrasta.

Kwalifikacja prawa ochrony danych osobowych w ramach gałęzi prawa jest sporna. Przedstawiciele doktryny uznają je najczęściej za część prawa administracyjnego[28], prawa dóbr materialnych lub prawa nowych technologii. W ocenie I. Lipowicz jest to „najbardziej zaawansowana w rozwoju" część prawa informacyjnego, posiadająca wykształconą część konstrukcyjną prawnokarną i prawa pracy. Wymaga ono jednak uzupełnienia, w szczególności w zakresie teoretycznym. Niektóre pojęcia – powszechnie znane i stosowane w doktrynie zachodniej – jak np. „informacyjne prawo administracyjne" i „publiczny porządek informacyjny" nie zostały jeszcze rozpowszechnione w polskiej nauce prawa[29].

W debacie dotyczącej kwalifikacji prawa ochrony danych osobowych wyrażane są również poglądy odnośnie do usamodzielnienia się tej dziedziny prawa. Argumentuje się to m.in. możliwym do wyodrębnienia przedmiotem ochrony danych osobowych[30], stosowaniem właściwej temu prawu terminologii, wprowadzeniem przedmiotów o tej nazwie do oferty ośrodków akademickich i powstawaniem podręczników poświęconych wyłącznie

wie o ochronie danych osobowych z 1978 r. i luksemburskiej ustawie o wykorzystaniu danych w systemach informatycznych z 1979 r. (wyliczenie za: E. Bielak-Jomaa, *Źródła prawa ochrony danych osobowych*, [w:] T.A.J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *Prawo ochrony danych osobowych*, Difin, Warszawa 2016, s. 35).

[28] Zob. np.: M. Miemiec, *Wstęp*, [w:] M. Miemiec (red. nauk.), *Materialne prawo administracyjne*, Wolters Kluwer Polska, Warszawa 2013, s. 21; H. Maurer, *Allgemeines Verwaltungsrecht*, Verlag C.H. Beck, München 2006, s. 473 i n.; D. Ehlers, M. Fehling, H. Pünder (red.), *Besonderes Verwaltungsrecht*, C.F. Müller, Heidelberg München Landsberg 2013, wyd. 3, t. 3, s. 48 i n.; E. Riedel, U. Derpa, *Kompetenzen des Bundes und der Länder im Gesundheitswesen – dargestellt anhand ausgewählter Regelungen im Sozialgesetzbuch*, Springer-Verlag, Berlin Heidelberg 2002, cz. 5, s. 56 i n.

[29] I. Lipowicz, *Prawne formy działania administracji publicznej – między stabilizacją a potrzebą przełomu*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2016, z. 4, s. 51.

[30] Jest nim ochrona „informacji, która z uwagi na jej treść daje co najmniej możliwość identyfikacji osoby fizycznej" (M. Kawecki, *Prawo ochrony danych osobowych jako nowa dziedzina prawa*, „Europejski Przegląd Sądowy" 2017, Nr 5, s. 8).

tej problematyce[31]. Postulaty wyodrębnienia prawa ochrony danych osobowych mogą budzić kontrowersje. Argument odwołujący się do oferty ośrodków akademickich i podręczników z tego zakresu może budzić wątpliwości. Jego przyjęcie prowadziłoby bowiem do konieczności rozważenia wyodrębnienia wielu innych dziedzin prawa[32]. Usamodzielnienie może być również kwestionowane z powodu braku swoistej dla tego prawa metody regulacji. Należy jednak zauważyć, że jej istnienie nie jest warunkiem *sine qua non* wyodrębnienia. Potwierdzeniem jest prawo pracy, w którym – podobnie jak w prawie ochrony danych osobowych – jest stosowana metoda administracyjnoprawna i cywilnoprawna, co określa się jako tzw. kompleksową metodę regulacji[33]. I chociaż można polemizować ze stanowiskiem dotyczącym usamodzielnienia się prawa ochrony danych osobowych twierdząc, że uznanie to jest jeszcze przedwczesne[34], to nie sposób kwestionować odrębności przedmiotowych tego prawa.

Niezależnie od sporów dotyczących kwalifikacji, należy zgodzić się z T. A. J. Banyś i przyjąć, że prawo ochrony danych osobowych realizuje pięć funkcji: ochronną, kontrolną, regulacyjną, edukacyjną i prewencyjną. Pierwsza polega na ochronie słusznych interesów osób fizycznych w związku z przetwarzaniem danych osobowych ich dotyczących, a więc przede wszystkim na ochronie prawa do prywatności tych osób. Druga polega na kontrolowaniu przez właściwe organy administracji publicznej procesu przetwarzania danych osobowych. Kontrola ta ma na celu porównanie stanu faktycznego (m.in. sposobu, zakresu i podmiotów przetwarzających dane osobowe) ze stanem postulowanym (m.in. sposobem,

[31] *Ibidem*, s. 4–10.

[32] Mowa np. o prawie farmaceutycznym i prawie ochrony dziedzictwa kultury.

[33] T. Zieliński, *Stosunek prawa pracy do prawa administracyjnego*, Państwowe Wydawnictwo Naukowe, Warszawa 1977, s. 19–22.

[34] Zob. analizę czynników i cech prawa administracyjnego: Z. Duniewska, *Zakres, przedmiot, rola, cele, funkcje, czynniki wyznaczające i cechy prawa administracyjnego*, [w:] R. Hauser, Z. Niewiadomski, A. Wróbel (red. nacz.), *System prawa administracyjnego. Instytucje prawa administracyjnego*, C.H. Beck, Instytut Nauk Prawnych PAN, Warszawa 2010, t. 1, s. 106–115.

zakresem i podmiotami upoważnionymi przepisami prawa do przetwarzania danych osobowych), ustalenie istnienia i zakresu nieprawidłowości ujawnionych w wyniku kontroli oraz wyciągnięcie wniosków umożliwiających ich wyeliminowanie. Trzecia polega na objęciu regulacją prawną stosunków społecznych dotyczących przetwarzania danych osobowych w sposób wyznaczający minimalne standardy przetwarzania tych danych i zapewniający im odpowiednią ochronę. Czwarta natomiast polega na popularyzacji idei ochrony danych osobowych oraz zwiększaniu świadomości społecznej z tym związanej, a piąta na zapobieganiu niezgodnemu z prawem przetwarzaniu danych osobowych[35].

Nawiązując do wyróżnionych funkcji prawa ochrony danych osobowych warto odnieść się do funkcji ochronnej i rozważyć, czy w jej zakresie powinna mieścić się również „ochrona przed nami samymi". Chodzi o to, czy jest dopuszczalne wprowadzenie przepisami prawa zakazu tzw. ekshibicjonizmu informacyjnego, a więc ujawniania informacji, które mogą powodować szkodę względem osób je ujawniających. Jeśli tak, to czy jest dopuszczalne aprioryczne ustalenie katalogu danych osobowych niepodlegających ujawnieniu nawet w przypadku uzyskania zgody osoby, której dane dotyczą.

Przyjęcie tego poglądu prowadziłoby do wniosku, że prawo może wyznaczać zakres danych osobowych niepodlegających udostępnieniu w żadnym przypadku[36], podobnie jak prawo może chronić osobę wbrew jej woli, gdy podejmuje ona działania ze szkodą dla niej samej (np. przymusowe

[35] T.A.J. Banyś, *Funkcje prawa ochrony danych osobowych*, [w:] T.A.J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *op. cit*., s. 21–22.

[36] Zob. np. art. 19 ust. 1 ustawy o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów, który obejmuje tajemnicą dane potencjalnych dawców i biorców. J. Haberko zauważa jednak, że „założenie ochrony danych osobowych jest rozwiązaniem, jak się wydaje, czysto technicznym i nie powinno być sprowadzone do rozważań natury administracyjnoprawnej w kontekście" u.o.d.o. (J. Haberko, *Komentarz do art. 19*, [w:] Haberko J., Uhrynowska-Tyszkiewicz I., *Ustawa o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów. Komentarz*, wersja el., https://sip.lex.pl/#/commentary/587370341/167781 [dostęp 30.07.2018].

skierowanie na leczenie[37]). Organy administracji publicznej byłyby wówczas uprawnione do ingerowania w życie prywatne osób fizycznych. Uzasadnienie ingerencji mogłoby być skonstruowane na dwa sposoby. Cechowałaby je precyzja – co skutkowałoby znaczną kazuistyką przepisów – lub zawierałoby ono pojęcia niedookreślone. Swoboda organu administracji publicznej w dokonywaniu ich interpretacji powodowałaby jednak ryzyko naruszeń praw i wolności człowieka. Trudności wiązałyby się ponadto z ustaleniem konkretnych danych osobowych objętych ochroną.

Przyjęcie analizowanego rozwiązania jest niedopuszczalne również z powodu istnienia sfery wolnej od ingerencji władz publicznych, kojarzonej intuicyjnie z ludzką wolnością. W jej ramach człowiek może działać zgodnie z własną wolą i jest pozostawiony samemu sobie. Ingerencja w tę sferę jest warunkowana zrealizowaniem kilku przesłanek. Po pierwsze, ustaleniem, że podejmowane działanie powoduje szkodę względem innych osób. Po drugie, rozważeniem, czy istnieją interesy publiczne uzasadniające ograniczenie tej wolności. Po trzecie, ustaleniem, czy tym interesom publicznym przysługuje prymat nad interesem indywidualnym, a więc nad wykonywaniem prawa do bycia pozostawionym samemu sobie[38]. Rozważając ingerencję należy również uwzględnić postanowienia przepisu art. 31 ust. 3 Konstytucji RP, określającego zasadę proporcjonalności ingerencji w konstytucyjne prawa i wolności[39]. Wymaga ona, aby ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw nie naruszały istoty tych wolności i praw oraz aby ich wprowadzenie było konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Konstytucja ogranicza więc przypadki, w których jest dopuszczalna ingerencja.

[37] Zob. art. 32 ustawy z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (t.j. Dz. U. z 2016 r., poz. 487 ze zm.) i art. 30 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. Dz. U. z 2018 r., poz. 1030).

[38] J. Braxton Craven Jr., *Personhood: the right to be let alone*, „Duke Law Journal" 1976, s. 699 i 711.

[39] B. Banaszak, *Prawo konstytucyjne*, C.H. Beck, Warszawa 2008, wyd. 4 zm., s. 233.

4. Podstawowe pojęcia dotyczące prawa ochrony danych osobowych

(Maciej Błażewski)

4.1. Dane osobowe

Pojęcie danych osobowych jest określane z uwzględnieniem dwóch elementów: informacji oraz podmiotu, który jest opisywany przez te informacje. Przepisy prawa określają wymogi względem elementów tej definicji. Informacja powinna umożliwiać identyfikację podmiotu, którego dotyczy, a podmiotem tym może być wyłącznie osoba fizyczna. Jedynie spełnienie tych dwóch elementów pozwala określić, że dane mają osobowy charakter. Na takie ujęcie wskazuje definicja legalna danych osobowych, która została wyrażona w rozporządzeniu 2016/679, w którego świetle są nimi informacje o osobie fizycznej, które można przyporządkować tej osobie. Informacje te mogą dotyczyć zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której dane dotyczą. Osoba jest możliwa do identyfikacji np. na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[40]. Jak słusznie wskazuje A. Krasuski, przytoczona definicja legalna danych osobowych jest ściśle związana z procesem identyfikacyjnym. Skutkiem tego procesu jest możliwość określenia tożsamości osoby fizycznej[41]. Autor, podkreślając znaczenie dla pojęcia danych osobowych, wymogu możliwości identyfikacji osoby fizycznej, wskazuje, że tymi danymi nie są informacje anonimowe[42]. Ochrona da-

[40] Artykuł 4 pkt 1 RODO.

[41] A. Krasuski, *Ochrona danych osobowych na podstawie RODO*, Wolters Kluwer Polska, Warszawa 2018, s. 76–77.

[42] *Ibidem*, s. 79.

nych nie obejmuje zatem informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną ani z danymi osobowymi zanonimizowanymi w taki sposób, że osób, których dane dotyczą, w ogóle lub już nie można zidentyfikować[43]. Zdaniem K. Kaźmierczaka oraz P. Litwińskiego forma informacji jest natomiast relatywna względem określenia informacji jako danych osobowych[44].

4.2. Przetwarzanie danych osobowych

Pojęcie danych osobowych należy uzupełnić definicją przetwarzania danych osobowych, również wprost wyrażaną w rozporządzeniu 2016/679. W. Chomiczewski słusznie podkreśla, że definicja legalna zawarta w tym akcie prawnym składa się z dwóch elementów: ogólnego określania przetwarzania oraz przykładowego katalogu czynności przetwarzania. Autor wskazuje także, że nie ma znaczenia, że pojęcie przetwarzania w tej definicji nie zostało uzupełnione o wyraźne wskazanie, że dotyczy ono danych osobowych. Wykładnia dalszej części tej definicji oraz jej umieszczenie w rozporządzeniu 2016/679 pozwala założyć, że dotyczy ona przetwarzania danych osobowych[45]. Zgodnie z pierwszą częścią tej definicji, obejmującej ogólne określenie, przetwarzanie jest pojedynczą operacją lub zestawem operacji podejmowanych z zastosowaniem danych osobowych. Może mieć formę automatyczną prowadzoną z użyciem systemu informatycznego lub formę niezautomatyzowaną[46]. Ten podział na dwa sposoby prze-

[43] Motyw 26 zd. 5 RODO.

[44] K. Kaźmierczak, P. Litwiński, *Zagadnienia wstępne z zakresu ochrony danych osobowych pracowników*, [w:] D. Dorre-Kolasa (red.), *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, C.H. Beck, Warszawa 2017, s. 4–5. Zdaniem autorów w celu określenia informacji jako danych osobowych nie ma znaczenia sposób ich wyrażenia, zapisania oraz prezentacji.

[45] W. Chomiczewski, *Komentarz do art. 4*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Wolters Kluwer Polska, Warszawa 2018, s. 186–187.

[46] Artykuł 4 pkt 2 RODO.

twarzania jest związany z rozwojem technologii teleinformatycznych, lecz nie skutkuje różnicą stopnia ochrony danych w każdym z nich[47].

Przepisy rozporządzenia 2016/679 wprowadzają szeroki, a jednocześnie otwarty katalog czynności stanowiących przykład przetwarzania danych osobowych. Przetwarzanie obejmuje takie czynności, jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie[48]. Włączenie do definicji legalnej katalogu czynności przetwarzania danych osobowych znacząco ogranicza niepewność co do kwalifikacji prawnej konkretnych czynności[49]. Należy podkreślić, że czynności te nie będą stanowiły przetwarzania danych osobowych, jeżeli nie spełnią wymagań wyrażonych w pierwszej, ogólnej części definicji przetwarzania danych osobowych[50].

5. Pojęcie środka prawnego

(Maciej Błażewski)

Prowadzone badania, których wyniki zostały zaprezentowane w monografii, koncentrowały się nad środkami prawnymi ochrony danych osobowych, czyli uwarunkowanymi prawnie środkami służącymi w sposób bezpośredni lub pośredni zapewnieniu ochrony danych osobowych.

Pojęcie środków prawnych nie zostało jednolicie zdefiniowane w nauce prawa. Problematyka pojęcia środków prawnych nie stanowiła przed-

[47] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4*, [w:] P. Litewski (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 197.

[48] Artykuł 4 pkt 2 RODO.

[49] A. Krasuski, *Ochrona danych osobowych…*, s. 76–77.

[50] W. Chomiczewski, *Komentarz do art. 4.…*, s. 187.

miotu wnikliwych, wieloaspektowych badań, lecz była analizowana jedynie przez pryzmat innych zagadnień. Można jednak wyróżnić dwie grupy poglądów dotyczących tej problematyki.

Część przedstawicieli nauki prawa utożsamia środki prawne z czynnościami jednostki skierowanymi wobec administracji publicznej. W. Taras odnosi to pojęcie do czynności bądź działań podejmowanych przez jednostkę wobec organu administracji publicznej[51]. Podobnie uważa M. Guziński, którego zdaniem środki prawne to „opisane i dopuszczone przez prawo sposoby oddziaływania na podmioty publiczne"[52]. Na takie ujęcie środków prawnych wskazuje także E. Pierzchała, która podkreśla, że za te środki powszechnie są uważane instytucje procesowe umożliwiające weryfikację rozstrzygnięć organów administracji publicznej[53]. Analogicznie uważa J.G. Firlus, który wskazuje, że przykładem środka prawnego jest wniosek o ponowne rozpatrzenie sprawy[54].

Inna grupa przedstawicieli nauki prawa wskazuje, że środki prawne oznaczają działania podmiotów publicznych względem podmiotów zewnętrznych wobec administracji publicznej. Przykładowo K. Strzyczkowski wręcz zrównuje środki prawne do narzędzi, przysługujących podmiotom publicznym, umożliwiających ingerencję w sfery zewnętrzne

[51] Zdaniem W. Tarasa środek prawny jest instytucją procesową (czynnością procesową), której celem jest ponowne rozpatrzenie sprawy przez oznaczony ustawą podmiot. W. Taras, *Środki prawne – pojęcia i podziały*, [w:] K. Chorąży, W. Taras, A. Wróbel (red.), *Postępowanie administracyjne, egzekucyjne i sądowoadministracyjne*, Wolters Kluwer business, Warszawa 2009, s. 99.

[52] M. Guziński, *Środki prawne w ustawie – Prawo zamówień publicznych (wybrane zagadnienia)*, [w:] L. Kieres (red.), *Środki prawne publicznego prawa gospodarczego*, Kolonia Limited, Wrocław 2007, s. 22. Autor analizuje problematykę środków prawnych podejmowanych względem podmiotu publicznego zarządzającego mieniem publicznym.

[53] E. Pierzchała, *Standardy funkcjonowania administracyjnych środków prawnych w postępowaniu przed organami pomocy społecznej*, [w:] J. Blicharz, L. Klat-Wertelecka, E. Rutkowska-Tomaszewska (red.), *Ubóstwo w Polsce*, E-Wydawnictwo, Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2017, s. 123.

[54] J.G. Firlus, *Fakultatywny charakter wniosku o ponowne rozpatrzenie sprawy w świetle zmodyfikowanego kształtu zasady dwuinstancyjności postępowania administracyjnego,* Zeszyty Naukowe Towarzystwa Doktorantów UJ Nauki Społeczne 2017, Nr 17, s. 38.

wobec administracji[55]. Natomiast S. Pieprzny utożsamia środki prawne z prawnymi formami działania organów administracji publicznej[56]. Podobnie uważa K. Horubski, utożsamiając środki prawne z rozstrzygnięciami administracyjnymi[57].

Pojęcie środków prawnych nie zostało także zdefiniowane w samym rozporządzeniu 2016/679. Prawodawca, w polskiej wersji językowej, użył w tytule Rozdziału VIII sformułowania „środki ochrony prawnej", które dla porównania w angielskiej wersji językowej jest określone jako *remedies.* Tytuł angielskojęzyczny odnosi się zatem bezpośrednio do ochrony prawnej przed innym podmiotem wobec nieprawidłowego działania jednego podmiotu. Rozporządzenie 2016/679 stosuje sformułowania „środki" w innych kontekstach, wśród których należy wyróżnić środki przetwarzania danych osobowych[58]; środki zapewniające zgodność z prawem[59]; środki chroniące prawa podstawowe i dane osobowe osób fizycznych[60]; środki techniczne i organizacyjne[61] oraz środki mające chronić prawa i wolności osoby[62]. Każdy z tych środków jest uwarunkowany prawnie.

Ze względu na niejednolite ujęcie problematyki środków prawnych w nauce prawa oraz w rozporządzeniu 2016/679 na potrzeby badań naukowych, których wyniki zostały zaprezentowane w tej monografii, przyjęto, że środki prawne służą zarówno podmiotom zewnętrznym wobec

[55] Według K. Strzyczkowskiego środkiem prawnym jest narzędzie, za pomocą którego państwo (podmioty publiczne) osiąga określone cele poprzez integrację w sferę gospodarki. K. Strzyczkowski, *Prawo gospodarcze publiczne*, Warszawa 2005, s. 205.

[56] S. Pieprzny, *Policja. Organizacja i funkcjonowanie*, Wolters Kluwer business, Warszawa 2011, s. 80

[57] K. Horubski, *Charakter prawny zezwolenia na prowadzenie działalności gospodarczej na terenie specjalnej strefy ekonomicznej uprawniającego do korzystania z pomocy publicznej*, [w:] L. Kieres (red.), *Środki prawne publicznego prawa gospodarczego*, Kolonia Limited, Wrocław 2007, s. 35. Autor wskazuje, że zezwolenie jest środkiem prawnym reglamentacji.

[58] Motyw 18 RODO.

[59] Motyw 45 RODO.

[60] Motyw 53 RODO.

[61] Motyw 29, motyw 71 RODO.

[62] Motyw 162 RODO.

administracji względem podmiotów publicznych oraz innych podmiotów związanych z ochroną danych, jak i samym podmiotom publicznym względem podmiotów zewnętrznych wobec administracji. Jedynie takie szerokie ujęcie środków prawnych pozwala na pełne opisanie działań nakierowanych na ochronę danych osobowych, które to działania są uwarunkowane prawnie. Na potrzeby tej monografii środkami prawnymi ochrony danych osobowych będą zatem prawnie uwarunkowane działania skierowane na zapewnienie przestrzegania przepisów prawa w toku procesu przetwarzania danych osobowych. Tak szerokie ujęcie podmiotowe oznacza akceptację każdego z wyżej wymienionych poglądów przedstawicieli nauk prawa, odnoszących się z jednej strony do działań jednostki, a z drugiej do działań podmiotów publicznych. Przedstawione w monografii naukowej ujęcie środków prawnych ochrony danych osobowych pozwala przyjąć ogół działań uwarunkowanych prawnie, a związanych z przetwarzaniem danych osobowych, co oznacza objęcie zakresem tego pojęcia innych środków wskazanych w rozporządzeniu 2016/679.

W celu przedstawienia pełniejszego obrazu tej problematyki można wyróżnić podział środków prawnych, wyrażonych w rozporządzeniu 2016/679, na środki prawne *sensu stricto* oraz środki prawne *sensu largo*. Środkami prawnymi *sensu stricto* są środki obejmujące działania zmierzające do ochrony prywatności konkretnej osoby oraz indywidualnie określonych danych, które jej dotyczą. Środkami prawnymi *sensu largo* obejmującymi wyżej opisane środki ochrony konkretnej osoby i jej indywidualnych danych oraz środki nakierowane na działania zmierzające do ochrony tej osoby, lecz jedynie pośrednio. Przedmiotem tych środków może być także ochrona danych osobowych określonych w sposób generalny i abstrakcyjny. Jedynie zastosowanie obu rodzajów tych środków umożliwia optymalną ochronę danych osobowych. Ze względu na szerokie ujęcie problematyki środków prawnych na potrzeby prowadzonego badania w tej monografii przyjęto w szczególności ujęcie środków prawnych *sensu largo*.

W ramach tego ujęcia można wyróżnić drugi podział środków prawnych o charakterze pośrednim i bezpośrednim. Podział ten uwzględnia kryterium podmiotowe. Środki pośrednie są podejmowane przez podmioty procesu przetwarzania, inne niż osoba, której dane dotyczą. Środki bezpośrednie podejmowane są jedynie przez tę osobę.

Proponowany w pracy podział na bezpośrednie i pośrednie środki ochrony danych osobowych ma wyłącznie porządkujący charakter, umożliwiający wnikliwe przeprowadzenie badań nad procesem przetwarzania danych osobowych. Wszystkie omawiane prawa należy bowiem pojmować jako złożoną całość związaną z procesem przetwarzania danych osobowych. Podział ten jest korzystny dla analizy problematyki środków prawnych ochrony danych. Pozwala na jednoczesne uwzględnienie opisanego wyżej podziału środków prawnych na *sensu largo* i *sensu stricto.* Środki prawne *sensu largo* obejmują jednocześnie środki bezpośrednie i pośrednie. Natomiast środki prawne *sensu stricto* odpowiadają jedynie środkom bezpośrednim. Podział pracy na środki bezpośrednie i pośrednie pozwala zatem jednocześnie przeprowadzić całościową analizę problematyki środków prawnych ochrony danych osobowych, a wyróżnienie w tym podziale środków bezpośrednich umożliwia wyodrębnienie środków *sensu stricto.*

Jednocześnie podział ten pozwala uwzględnić dwie grupy celów przepisów dotyczących ochrony danych osobowych. Pierwsza obejmuje zapewnienie jak najszerszego zakresu ochrony osobom, których dane dotyczą, przed nielegalną ingerencją i naruszaniem ich praw związanych z przetwarzaniem danych osobowych. Tym celom służą w szczególności środki prawne o pośrednim charakterze. Druga obejmuje ochronę tych osób w przypadku wystąpienia naruszenia i zagwarantowanie im odpowiedniej procedury umożliwiającej skuteczne dochodzenie praw przed właściwym sądem lub organem, uzyskanie przez nie rekompensaty za poniesione szkody i ukaranie podmiotów odpowiedzialnych za niezgod-

ne z prawem przetwarzanie. Te cele mogą być osiągnięte poprzez zastosowanie środków prawnych o bezpośrednim charakterze.

5.1. Pojęcie pośrednich środków prawnych ochrony danych osobowych

Środki prawne ochrony danych osobowych *sensu largo* o charakterze pośrednim są podejmowane przez administratora lub podmiot przetwarzający bez potrzeby konkretyzacji ich w żądaniu osoby, których dane dotyczą, lub Prezesa UODO, jako organu nadzorczego. Pośrednimi środkami prawnymi są środki techniczne i organizacyjne, środki informacyjne, ocena skutków przetwarzania danych osobowych wraz z konsultacjami z Prezesem UODO, rejestry dotyczące czynności przetwarzania, certyfikat, wiążące reguły korporacyjne oraz kodeks postępowania opracowany przez zrzeszenie lub podmiot reprezentujący administratorów lub podmioty przetwarzające.

Przepisy dotyczące części pośrednich środków prawnych są kontynuacją regulacji wyrażonych w dyrektywie 95/46/WE, w świetle której do tych środków można było zaliczyć środki informacyjne względem osoby, której dane dotyczą, oraz organu nadzorczego, jak również kodeks postępowania[63]. Rozporządzenie 2016/679 wprowadza częściowo odmienny sposób określenia środków technicznych i organizacyjnych, w porównaniu z tymi, które były wymagane na podstawie poprzednich regulacji wyrażonych w dyrektywie 95/46/WE. Jednocześnie rozporządzenie 2016/679 konkretyzuje na poziomie Unii Europejskiej takie środki[64]. Zmiana dotyczy także sposobu prowadzenia prewencyjnej kontroli operacji przetwarzania[65], którą zastąpiła ocena skutków przetwarzania danych osobowych. Zmiany regulacji dotyczą także wprowadzenia no-

[63] Artykuły 10, 11, 18, 27 dyrektywy 95/46/WE.

[64] Poprzednie regulacje, wyrażone w art. 17 dyrektywy 95/46/WE, pozostawiały określenie środków technicznych i organizacyjnych państwom członkowskim.

[65] Artykuł 20 dyrektywy 95/46/WE.

wych środków pośrednich, takich jak certyfikaty, wiążące reguły korporacyjne oraz rejestrowanie czynności przetwarzania przez administratora lub podmiot przetwarzający[66].

Przepisy prawa nadały administratorowi częściową swobodę stosowania tych środków. Można wyróżnić sfery tej swobody ich stosowania, do których należy zaliczyć: sferę całkowitej swobody, sferę ograniczonej swobody oraz sferę wyłączonej swobody.

Sfera całkowitej swobody obejmuje środki pośrednie, których stosowanie jest zależne w całości od woli administratora lub podmiotu przetwarzającego. Administrator stosuje je wyłącznie w celu wykazania, że przestrzega przepisów o ochronie danych osobowych. Środkami tymi są uzyskanie certyfikatu, wiążących reguł korporacyjnych oraz stosowanie Kodeksy postępowania. Stosowanie tych środków służy wypełnieniu założeń zasady rzetelności, a jednocześnie umożliwia administratorowi podejmowanie czynności przetwarzania w szerszym zakresie.

Sfera ograniczonej swobody odnosi się do środków pośrednich, które powinny być stosowane, lecz administrator lub podmiot przetwarzający samodzielnie określają sposób i zakres ich wdrożenia. Samodzielność tego wyboru także ma ograniczony charakter, jest ona bowiem determinowana ryzykiem naruszenia ochrony danych osobowych. Przykładem tych środków pośrednich są środki techniczne i organizacyjne. Administrator samodzielnie wybiera środek, który będzie odpowiedni wobec konkretnego ryzyka naruszenia prywatności. W świetle zasady rzetelności ponosi on jednak odpowiedzialność za ten wybór.

Sfera wyłączonej swobody odnosi się do środków pośrednich, których obowiązek stosowania wprost wynika z przepisów prawa. Regulacje te określają także, w jaki sposób środki te powinny być wdrożone. Sfera wyłączonej swobody odnosi się do działań prewencyjnych oraz następczych.

[66] W świetle art. 21 ust. 2 w zw. z art. 18 dyrektywy 95/46/WE organ nadzorczy w państwie członkowskim prowadził rejestr operacji przetwarzania, które zostały mu wcześniej zgłoszone przez administratora.

Środkiem o charakterze prewencyjnym jest ocena skutków przetwarzania danych osobowych oraz konsultacje z Prezesem UODO, jako organem nadzorczym. Środki następcze są związane z informowaniem o przetwarzaniu danych osobowych lub o naruszeniach ochrony tych danych. Środek informacyjny związany z przetwarzaniem odnosi się do przekazania informacji osobie, której dane dotyczą, o przetwarzaniu jej danych. Środkami informacyjnymi o naruszeniach są: zgłoszenie naruszenia ochrony danych oraz zawiadomienie osoby, której dane dotyczą, o naruszeniu tej ochrony.

Środki pośrednie są znacząco zróżnicowane, lecz wzajemnie się uzupełniają, zapewniając ochronę danych osobowych. Ich bezpośrednie cele mogą być inne. Ułatwiają one ochronę danych administratorowi, podmiotowi przetwarzającemu oraz Prezesowi UODO, jako organowi nadzorczemu. Ułatwieniem tym jest przyjęcie domniemania ochrony, którego podstawą jest np. certyfikat lub wiążące reguły korporacyjne. Ułatwieniu takiemu służy także określenie jasnych reguł komunikacji pomiędzy podmiotami procesu przetwarzania. Przepisy prawa wyraźnie określają procedurę oraz treść komunikacji pomiędzy administratorem lub podmiotem przetwarzającym a Prezesem UODO. Komunikacja ta odbywa się m.in. za pomocą środków pośrednich, jakimi są: konsultacje po przeprowadzonej ocenie skutków przetwarzania danych oraz zgłoszenie naruszenia ochrony danych. Środki pośrednie mają także na celu zwiększenie efektywności ochrony danych poprzez nałożenie obowiązku na administratora oceny skutków, obejmującej analizę ryzyka, oraz nałożenie na niego odpowiedzialności za wybór odpowiednich środków technicznych i organizacyjnych. Tym samym Prezes UODO, jako organ nadzorczy, może podejmować czynności nadzorcze w sytuacjach, gdy jego ingerencja jest rzeczywiście potrzebna[67].

[67] Środki pośrednie odnoszące się do komunikacji administratora oraz podmiotu przetwarzającego z Prezesem Urzędu, jako organem nadzorczym, są bardziej efektywne, w porównaniu ze środkami, do których stosowania obligowała dyrektywa 95/46/WE. W świetle motywu 89 zd. 1–2 RODO ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych stanowił znaczące obciążenie administracyjne i finansowe, a jednocześnie nie zawsze przyczyniał się do poprawy ochrony danych osobowych.

5.2. Pojęcie bezpośrednich środków prawnych ochrony danych osobowych

Bezpośrednie środki ochrony danych osobowych są podejmowane przez osobę, której dane dotyczą. Środkami tymi są: wyrażenie zgody na przetwarzanie danych osobowych i jej cofnięcie, żądanie dostępu do danych, sprostowania danych, usunięcia lub ograniczenia ich przetwarzania, przeniesienia danych i wyrażenie sprzeciwu wobec ich przetwarzania, a także skarga do organu nadzorczego. Bezpośrednie środki są również związane z ochroną prawną osoby, której dane dotyczą, podejmowaną przed sądem przeciwko organowi nadzorczemu lub przeciwko administratorowi i podmiotowi przetwarzającemu, z czym związane jest także prawo do odszkodowania.

Przepisy rozporządzenia 2016/679 oraz ustawy o ochronie danych osobowych nadały osobie, której dane dotyczą, swobodę stosowania bezpośrednich środków prawnych ochrony danych. Od jej inicjatywy zależy podjęcie tych środków. Korzystanie z nich jest warunkowane działaniem (aktywną postawą) osób, których dane dotyczą.

Odniesienie tych celów do rozważań prowadzonych w tym rozdziale umożliwia wyróżnienie dwóch grup bezpośrednich środków ochrony danych osobowych. Pierwsza mieści w sobie działania podejmowane względem administratora przez osobę, której dane dotyczą. Są nimi: wyrażenie zgody na przetwarzanie danych osobowych i jej cofnięcie, żądanie dostępu do danych, sprostowania danych, usunięcia lub ograniczenia ich przetwarzania, przeniesienia danych i wyrażenie sprzeciwu wobec ich przetwarzania.

Druga obejmuje działania osoby uprawnionej podejmowane przed właściwym sądem lub organem nadzorczym w przypadku, gdy osoba ta jest przekonana, że naruszono jej – przyznane przepisami rozporządzenia 2016/679 – prawa. Żąda ona wówczas zobowiązania podmiotu naruszającego do podjęcia określonego prawem działania (np. usunięcia da-

nych osobowych, rozpatrzenia wniesionej skargi, zapłaty odszkodowania za poniesioną szkodę). Działania te, mimo że są podejmowane w relacji „osoba dochodząca realizacji swoich praw – sąd lub organ nadzorczy", wywołują skutki względem podmiotu naruszającego prawa[68].

[68] Przykład: administrator przetwarza dane osobowe, mimo że wniesiono skutecznie sprzeciw wobec przetwarzania. Osoba, której dane dotyczą, wnosi więc skargę do właściwego organu nadzorczego, żądając zobowiązania administratora do zaprzestania przetwarzania. Wnosi ona również pozew do sądu, wykazując, że niezgodne z prawem przetwarzanie wyrządziło jej szkodę. Organ nadzorczy może zobowiązać administratora do zaprzestania przetwarzania objętych sprzeciwem danych i nałożyć na niego administracyjną karę pieniężną, a sąd może zobowiązać administratora do zapłaty odszkodowania tej osobie.

Rozdział II

Źródła prawa ochrony danych osobowych

(Jolanta Behr)

1. Źródła prawa – uwagi ogólne

Pojęcie „źródła prawa" jest wieloznaczne[69] i sporne[70]. W szczegółowych analizach odnosi się je najczęściej do źródeł poznania prawa (*fontes iuris cognoscendi*) i źródeł powstawania prawa (*fontes iuris oriundi*). Pierwsze to czynniki dostarczające informacji o prawie[71]. Drugie są rozumiane niejednolicie i są najczęściej uznawane za czynniki wpływające na ukształ-

[69] M. Haczkowska, *Komentarz do art. 87*, [w:] M. Haczkowska (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Wolters Kluwer, Warszawa 2014, wyd. 1, s. 218; B. Banaszak, *Prawo konstytucyjne*..., s. 38.

[70] Postulowano nawet rezygnację z jego stosowania (zob. J.S. Langrod, *Instytucje prawa administracyjnego. Zarys części ogólnej*, Kantor Wydawniczy Zakamycze, Zakamycze 2003, reprint, s. 282; M. Pichlak, *Zamknięty system źródeł prawa. Studium instytucjonalizacji dyskursu prawniczego*, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2013, s. 18–19 i powołana tam literatura). Jego ugruntowanie w dogmatyce prawa i przydatność do systematyzacji wywodów uzasadnia jednak posługiwanie się nim jako pojęciem-narzędziem.

[71] Są nimi m.in. dzienniki urzędowe takie jak: Dziennik Ustaw Rzeczypospolitej Polskiej, Dziennik Urzędowy Rzeczypospolitej Polskiej „Monitor Polski", dzienniki urzędowe ministrów kierujących działami administracji rządowej, dzienniki urzędowe urzędów centralnych oraz wojewódzkie dzienniki urzędowe (art. 8 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych, t.j. Dz. U. z 2017 r., poz. 1523).

towanie się określonej treści przepisów prawa (źródła prawa w znaczeniu materialnym) lub za działania organów prawotwórczych albo efekty tej działalności (źródła prawa w znaczeniu formalnym)[72].

Zdaniem M. Haczkowskiej w świetle przepisów Konstytucji RP źródłami prawa są „akty prawotwórcze (normatywne) zawierające przynajmniej jedną normę generalną i abstrakcyjną, które mogą stać się podstawą aktu indywidualnego i konkretnego"[73]. Są to zatem akty stanowienia prawa będące formalnymi źródłami prawa. Przyjęcie tego stanowiska uzasadnia ograniczenie rozważań dotyczących źródeł prawa ochrony danych osobowych wyłącznie do przepisów aktów normatywnych.

Celem niniejszej pracy nie jest kompleksowa i wszechstronna analiza wszystkich aktów prawnych będących źródłami prawa ochrony danych osobowych. Jest nim natomiast dokonanie przeglądu najważniejszych z nich, w sposób umożliwiający uchwycenie istoty prawa ochrony danych osobowych w polskim porządku prawnym oraz jego głównych założeń.

2. Akty normatywne będące podstawą prawną ochrony danych osobowych

Przepisy dotyczące ochrony danych osobowych są zawarte w wielu aktach normatywnych prawa krajowego i międzynarodowego. Zależnie od przyjętego kryterium można wprowadzić ich liczne podziały. Wyliczenie wszystkich przekraczałoby znacznie ramy niniejszego opracowania i byłoby zbędne do osiągnięcia celów pracy. Mając to na uwadze, zostaną przedstawione tylko niektóre z nich[74].

[72] J. Nowacki, Z. Tobor, *Wstęp do prawoznawstwa*, Wolters Kluwer Polska, Warszawa 2007, wyd. 3, s. 113–114.

[73] M. Haczkowska, *op. cit*., s. 218–219.

[74] Szczegółowe wyliczenie źródeł zob.: G. Szpor, *Strategia ochrony danych osobowych w polityce społecznej*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2012, Nr 87, s. 137–138; A. Drozd, *Komentarz do art. 4*, [w:] A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy,* LexisNexis, Warszawa 2007, wyd. 3, s. 32–35.

Uwzględnienie kryterium zakresu obowiązywania źródła prawa umożliwia wyróżnienie aktów prawa powszechnie obowiązującego[75] (obowiązujących wszystkich na określonym terytorium) i wewnętrznie obowiązującego[76] (obowiązujących jednostki podległe organizacyjnie organowi wydającemu te akty[77]).

Akty prawa powszechnie obowiązującego tworzą zamknięty system źródeł prawa[78]. Zgodnie z art. 87 Konstytucji RP tworzą go: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia. Na obszarze działania organów, które je ustanowiły, są nimi również akty prawa miejscowego. Kolejność wymienienia aktów nie jest przypadkowa. Uwzględnia ona zasadę hierarchicznej struktury systemu źródeł prawa. Przejawia się ona przede wszystkim w „zakazie tworzenia aktów sprzecznych co do treści i trybu ich stanowienia z aktami organów wyższego szczebla oraz […] w obowiązku organów niższych szczebli do stanowienia aktów prawnych mających służyć realizacji norm aktów wyższego stopnia”[79].

Zawarte w przepisie art. 87 Konstytucji RP wyliczenie aktów normatywnych prawa powszechnie obowiązującego nie jest enumeratywne. Zauważa się, że inne przepisy tego aktu stanowią podstawę do przyjęcia, że do omawianych źródeł należy również zaliczyć inne akty prawne, tj.: rozporządzenia z mocą ustawy (art. 234 ust. 1), umowy międzynarodowe (art. 9 w zw. z art. 91 ust. 1 i 2), akty prawa wtórnego Unii Europejskiej

[75] Jest nim np. ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

[76] Jest nim np. zarządzenie nr 563 Wojewody Dolnośląskiego z dnia 30 września 2015 r. w sprawie: wprowadzenia Polityki Bezpieczeństwa Ochrony Danych Osobowych i Instrukcji zarządzania systemem informatycznym w Dolnośląskim Urzędzie Wojewódzkim we Wrocławiu.

[77] K. Działocha, *Komentarz do art. 93*, [w:] L. Garlicki (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* Wydawnictwo Sejmowe, Warszawa 2001, t. 2, wyd. 1, s. 15.

[78] „Zamknięcie” ma charakter podmiotowy i przedmiotowy. Oznacza to, że akty prawa powszechnie obowiązującego mogą być tworzone wyłącznie w formach określonych w Konstytucji RP i przez organy, którym akt ten przyznaje kompetencję do stanowienia tego typu aktów (L. Garlicki, *Konstytucyjne źródła prawa administracyjnego*, [w:] R. Hauser, Z. Niewiadomski, A. Wróbel (red.), *System prawa administracyjnego. Konstytucyjne podstawy funkcjonowania administracji publicznej*, C.H. Beck, Instytut Nauk Prawnych PAN, Warszawa 2012, t. 2, s. 55-56).

[79] B. Banaszak, *Prawo konstytucyjne*…, s. 46.

(art. 91 ust. 3), układy zbiorowe pracy i inne porozumienia (art. 59 ust. 2) oraz Regulamin Sejmu w części dotyczącej sposobu wykonywania obowiązków organów państwowych względem Sejmu[80]. Nie wszystkie te akty regulują jednak kwestie związane z ochroną danych osobowych.

Aktem prawa krajowego o najwyższej mocy prawnej jest Konstytucja RP. Wszystkie inne akty prawne obowiązujące w Rzeczypospolitej Polskiej muszą być z nią zgodne. Przepisy Konstytucji RP są co do zasady stosowane bezpośrednio (art. 8 ust. 2). Gwarantują one m.in. ochronę danych osobowych, uznając ją za element prawa do prywatności (art. 47) oraz za prawo autonomiczne (art. 51). Określają także warunki wprowadzania ograniczeń konstytucyjnych wolności i praw (art. 31).

Ochrona danych osobowych jest również regulowana w prawie międzynarodowym. Obowiązek przestrzegania tego prawa wynika z przepisu art. 9 Konstytucji RP[81]. Prawo międzynarodowe jest specyficznym porządkiem prawnym, którego podstawą obowiązywania jest wola państw. Źródłami tego prawa są: umowy międzynarodowe, zwyczaj międzynarodowy, zasady ogólne prawa uznane przez narody cywilizowane[82], akty jednostronne państw oraz wiążące i prawotwórcze uchwały organów organizacji międzynarodowych[83]. Źródłami pomocniczymi są judykatura i doktryna[84]. Nie wszystkie z wymienionych źródeł prawa międzynaro-

[80] M. Haczkowska, *op. cit.*, s. 220.

[81] Stanowi on, że Rzeczpospolita Polska przestrzega wiążącego ją prawa międzynarodowego.

[82] Zgodnie z art. 38 Statutu Międzynarodowego Trybunału Sprawiedliwości umowy międzynarodowe, zwyczaj międzynarodowy, zasady ogólne prawa uznane przez narody cywilizowane, judykatura i doktryna są wyłącznie podstawami wyrokowania Trybunału. W szczegółowych analizach są one traktowane jako podstawa konstruowania katalogu źródeł prawa międzynarodowego.

[83] Mimo że nie zostały one wymienione w art. 38 Statutu Międzynarodowego Trybunału Sprawiedliwości, są one uznawane za źródło prawa międzynarodowego (T. Srogosz, *Źródła prawa międzynarodowego*, [w:] J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, C.H. Beck, Warszawa 2017, s. 112–113).

[84] Zob.: A. Kozłowski, *Istota zasad ogólnych prawa i orzeczeń sądów międzynarodowych jako źródło prawa międzynarodowego*, [w:] J. Kolasa (red.), *Istota źródła w porządku prawa międzynarodowego*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2016, s. 179–247;

dowego są aktami normatywnymi. Z uwagi na przyjęte w pracy znaczenie pojęcia „źródła prawa", przedmiotem rozważań tej części pracy będą więc wyłącznie akty normatywne.

Kwestia obowiązywania przepisów prawa międzynarodowego i ich pozycja w krajowym porządku prawnym jest wciąż przedmiotem ożywionych dyskusji przedstawicieli nauki prawa. Źródła tego prawa tworzą bowiem obszerną i niejednolitą grupę, której zakres obowiązywania i moc prawna nie są jednakowe[85].

Za źródło prawa powszechnie obowiązującego w Rzeczypospolitej Polskiej Konstytucja RP uznaje wyłącznie ratyfikowane umowy międzynarodowe (art. 87 ust. 1). Postanowienia Konstytucji RP umożliwiają wyróżnienie dwóch grup ratyfikowanych umów międzynarodowych. Pierwsza to ratyfikowane umowy międzynarodowe, których ratyfikacja wymaga uprzedniej zgody wyrażonej w ustawie lub referendum. Dotyczą one spraw wymienionych wyczerpująco w art. 89 ust. 1 Konstytucji RP. Umowy te mają pierwszeństwo przed ustawami, jeżeli ustaw nie da się pogodzić z umowami (art. 91 ust. 2 Konstytucji RP). Druga to ratyfikowane umowy międzynarodowe, dla których ratyfikacji nie jest wymagana zgoda wyrażona w ustawie lub referendum. Umowy te nie mają pierwszeństwa przed ustawami w przypadku sprzeczności ich postanowień. Ratyfikowane umowy międzynarodowe, po ich ogłoszeniu w Dzienniku Ustaw Rzeczypospolitej Polskiej, są częścią krajowego porządku prawnego i są bezpośrednio stosowane, chyba że ich stosowanie uzależnia się od wydania ustaw (art. 91 ust. 1 Konstytucji RP)[86].

Odrębnego omówienia wymaga prawo Unii Europejskiej. Poglądy doktryny na temat uznania tego prawa za prawo międzynarodowe są po-

S. Kennedy, *The Sources of International Law*, "American University International Law Review" 1987, Vol. 2, Nr 1, s. 1–96.

[85] B. Banaszak, *Prawo konstytucyjne*…, s. 146.

[86] *Ibidem*, s. 149–151.

dzielone[87]. Nie wdając się w polemikę, warto zwrócić uwagę na źródła tego prawa. Są one zróżnicowane i podlegają licznym podziałom. Jednym z nich jest podział na prawo pierwotne i prawo wtórne[88]. Prawem pierwotnym są traktaty założycielskie i akcesyjne z późniejszymi zmianami[89], akty Rady lub Rady Europejskiej o charakterze konstytucyjnym i ogólne zasady prawa. Akty prawa pierwotnego regulują kwestie dotyczące ochrony danych osobowych. Istotną rolę w tym obszarze odgrywają również przepisy Karty praw podstawowych Unii Europejskiej.

Prawo wtórne jest tworzone na podstawie prawa pierwotnego. Aktami prawa wtórnego są: rozporządzenia, dyrektywy, decyzje, zalecenia i opinie (art. 288 TFUE). Rozporządzenia są wiążącymi aktami o ogólnym zasięgu. Wiążą one w całości i są bezpośrednio stosowane we wszystkich państwach członkowskich Unii Europejskiej[90]. „Bezpośrednie stosowanie rozporządzenia oznacza, że jego wejście w życie oraz stosowanie na korzyść lub przeciwko tym podmiotom jest niezależne od przyjęcia jakiegokolwiek środka recypującego jego treść do prawa krajowego. Przepis prawa krajowego, który powtarza treść bezpośrednio stosowalnego przepisu prawa wspólnotowego, nie ma żadnego wpływu na

[87] Można wyróżnić trzy dominujące. Pierwsze przyjmuje, że jest „ono odrębnym porządkiem prawnym, niezależnym od porządku międzynarodowego, rządzącym się innymi regułami, […] charakteryzującym się wewnętrznym systemem wartości" (A. Wentkowska, *Prawo UE wobec prawa międzynarodowego i prawa krajowego*, [w:] J. Barcik, A. Wentkowska, *Prawo Unii Europejskiej*, C.H. Beck, Warszawa 2014, s. 334). Drugie przyjmuje, że „prawo pierwotne (traktatowe) posiada cechy międzynarodowego systemu prawnego, niemniej jednak nie jest klasycznym prawem międzynarodowym" (A. Trubalski, *Prawne aspekty implementacji prawa UE do systemu prawnego RP*, C.H. Beck, Warszawa 2016, s. 1). Trzecie uznaje je za „szczególny system ponadnarodowego prawa międzynarodowego" (J. Gołaczyński, *Umowy elektroniczne w prawie prywatnym międzynarodowym*, Wolters Kluwer Polska, Warszawa 2007, s. 29).

[88] Wyliczenie i omówienie za: Z. Duniewska, *Pojęcie prawa, określenie i charakterystyka systemu*, [w:] M. Stahl (red. nauk.), *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie*, Warszawa 2016, s. 210–211.

[89] Przede wszystkim TUE i TFUE.

[90] Artykuł 288 TFUE.

bezpośrednie stosowanie tego przepisu lub na wynikającą z Traktatu jurysdykcję Trybunału”[91].

Dyrektywy wiążą każde państwo członkowskie Unii Europejskiej, do którego są kierowane w odniesieniu do rezultatu, jaki ma być osiągnięty. Pozostawiają one organom krajowym swobodę wyboru formy i środków ich realizacji[92]. Dzięki temu w procesie implementacji (wdrożenia) przepisów dyrektywy do prawa krajowego jest możliwe uwzględnienie specyficznych uwarunkowań krajowych. Dyrektywy mają na celu zbliżenie ustawodawstw państw członkowskich i ich harmonizację.

Decyzje są aktami wiążącymi w całości. Gdy wskazują one adresatów, wiążą tylko tych adresatów[93]. Decyzje organów Unii Europejskiej regulują co do zasady kwestie indywidualne i konkretne. Ich adresatami mogą być państwa członkowskie oraz inne podmioty prawne[94].

Zalecenia i opinie są aktami, które nie mają mocy wiążącej. Nie jest więc dopuszczalne nakładanie przez nie obowiązków na osoby trzecie. Celem ich wydania jest skłonienie ich adresatów do podjęcia określonego działania, bez zastosowania przymusu[95].

Prawo międzynarodowe i prawo Unii Europejskiej jest istotnym źródłem prawa ochrony danych osobowych w Rzeczypospolitej Polskiej. Określa ono m.in.: prawo do ochrony danych osobowych; przyznaje osobom, których dane dotyczą, konkretne prawa związane z jego realizacją; nakłada na podmioty przetwarzające określone obowiązki związane z procesem przetwarzania danych; określa zasady ochrony danych osobowych oraz definiuje podstawowe pojęcia związane z ochroną danych osobowych.

[91] Wyrok TSUE z dnia 10 października 1973 r. w sprawie C 34/73 *Fratelli Variona S.p.A.* przeciwko *Amministrazione italiana delle Finanze* (http://eulaw.pl/data/documents/Fratelli-Variola.docx, dostęp: 07.07.2018).

[92] Artykuł 288 TFUE.

[93] *Ibidem*.

[94] A. Wróbel (red.), *Stosowanie prawa Unii Europejskiej przez sądy*, Wolters Kluwer Polska, Warszawa 2010, wyd. 2, t. I, s. 72–73.

[95] *Ibidem*, s. 74.

Źródłami prawa ochrony danych osobowych są również ustawy. Są one aktami samoistnymi, a zatem do ich wydania nie jest wymagane istnienie odrębnego, konstytucyjnego upoważnienia. Uchwala je Sejm w procedurze określonej w Konstytucji RP (art. 118–123). Z ustawami łączą się dwie zasady. Pierwsza to zasada wyłączności ustaw. Wymaga ona, aby wszelkie kwestie istotne dla funkcjonowania państwa i organów władzy publicznej oraz dla obywateli były regulowane w formie ustawy. Druga to zasada nadrzędności ustaw w systemie źródeł prawa. W jej myśl akty podustawowe powinny być zgodne z ustawami w płaszczyźnie formalnej i materialnej[96]. Ustawom przyznano wyłączność regulacyjną. Przejawia się ona dopuszczalnym, nieograniczonym zakresem przedmiotowym ustawy – pod warunkiem, że zachowuje się ogólny charakter jej przepisów – oraz dopuszczalnością regulowania niektórych kwestii wyłącznie w drodze ustawy[97] (np. ograniczenia korzystania z konstytucyjnych wolności i praw, w tym prawa do prywatności i prawa do ochrony danych osobowych oraz zobowiązania określonych osób do ujawniania informacji ich dotyczących).

Ustawami odgrywającymi istotną rolę w ochronie danych osobowych są ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Regulują one podstawowe kwestie dotyczące ochrony danych osobowych, a przepisy wielu aktów normatywnych nawiązują wprost do ich treści. Ustawy te definiują pojęcia kluczowe z tego obszaru oraz ustalają m.in. zasady przetwarzania danych osobowych i konsekwencje ich naruszenia. Określają również organy ochrony danych osobowych i ich kompetencje oraz przyznają osobom, których dane dotyczą, konkretne prawa w zakresie ochrony danych osobowych. Wprowadzają ponadto warunki przekazywania danych osobowych do państw trzecich.

[96] E. Ochendowski, *Prawo administracyjne. Część ogólna*, Wydawnictwo „Dom Organizatora", Toruń 2004, s. 86.

[97] L. Garlicki, *op. cit.*, s. 59.

Rozporządzenia z mocą ustawy są aktami, które mogą zostać wydane wyłącznie w czasie stanu wojennego, gdy Sejm nie może zebrać się na posiedzenie. Kompetencję do ich wydania posiada Prezydent RP, działający na wniosek Rady Ministrów. Akty te są wydawane w zakresie i granicach określonych w Konstytucji RP. Ich przedmiotem może być m.in. ograniczenie wolności i praw człowieka i obywatela w czasie stanu wojennego, a więc także ograniczenie prawa do prywatności i prawa ochrony danych osobowych. Rozporządzenia z mocą ustawy podlegają zatwierdzeniu przez Sejm na najbliższym posiedzeniu, inaczej tracą moc obowiązującą (art. 234 ust. 1 w zw. z art. 228 ust. 3–5 Konstytucji RP). Nie zostały one dotychczas wydane.

Źródłami prawa powszechnie obowiązującego Rzeczypospolitej Polskiej są również rozporządzenia. Wydają je organy wymienione w Konstytucji RP. Rozporządzenia są aktami niesamoistnymi, do których wydania jest wymagane szczegółowe upoważnienie ustawowe określające: organ właściwy do wydania rozporządzenia[98], przedmiot rozporządzenia oraz wytyczne dotyczące treści. Konsekwencją niesamoistnego charakteru rozporządzeń jest również to, że rozporządzenie „dzieli los ustawy". Oznacza to, że utrata mocy obowiązującej ustawy wiąże się co do zasady z utratą mocy obowiązującej rozporządzeń wydanych na ich podstawie. Rozporządzenia nie zastępują ustaw. Ich rolą jest odciążenie od szczegółów technicznych i specjalistycznej terminologii oraz uregulowań zmiennych w czasie[99]. W rozporządzeniach dotyczących ochrony danych osobowych reguluje się m.in.: warunki, sposób i tryb ochrony danych osobowych w związku z realizowaniem określonych zadań publicznych, tryb i zakres przekazywania danych osobowych między organami admi-

[98] Organy upoważnione do wydawania rozporządzeń określa w sposób abstrakcyjny Konstytucja RP. Są nimi: Prezydent RP, Prezes Rady Ministrów, Rada Ministrów, minister kierujący działem administracji rządowej (tzw. minister „z teką"), Krajowa Rada Radiofonii i Telewizji oraz przewodniczący określonych w ustawach komitetów. Ustawy przyznają natomiast konkretnym organom kompetencje do wydania określonych rozporządzeń.

[99] E. Ochendowski, *op. cit.*, s. 92–101.

nistracji publicznej, sposób prowadzenia określonych rejestrów i ewidencji, w których gromadzi się dane osobowe, oraz wzory niektórych dokumentów związanych z przetwarzaniem danych osobowych.

Źródłami prawa powszechnie obowiązującego Rzeczypospolitej Polskiej są również akty prawa miejscowego. Obowiązują one na obszarze działania organów, które je ustanowiły. Są one aktami podustawowymi o charakterze niesamoistnym. Wydają je organy jednostek samorządu terytorialnego i terenowe organy administracji rządowej na podstawie i w granicach upoważnień ustawowych (generalnych lub szczegółowych). Akty te tworzą niejednolitą kategorię. Dzielą się na: statutowe, wykonawcze i porządkowe. Pierwsze dotyczą ustroju określonych jednostek. Przedmiotem drugich są kwestie przekazane do uregulowania przepisami ustaw w zakresie w nich wskazanym, umożliwiającym ich realizację. Trzecie są wydawane w zakresie nieuregulowanym w ustawach lub innych przepisach powszechnie obowiązujących, gdy jest to niezbędne dla ochrony wartości lub stanów określonych w upoważnieniu do ich wydania, w tym ochrony życia, zdrowia lub mienia. Mogą one zawierać nakazy i zakazy określonego zachowania i przewidywać sankcję za ich naruszenie (karę grzywny)[100]. Ze względu na ograniczony terytorialnie zakres obowiązywania, tworząc akty prawa miejscowego, uwzględnia się możliwości i potrzeby społeczności lokalnej. W praktyce powoduje to zróżnicowanie pozycji faktycznej i prawnej członków różnych jednostek samorządu terytorialnego. Z uwagi na to oraz na charakter prawa ochrony danych osobowych ustawodawca nie przekazuje do uregulowania kwestii z nim związanych w formie aktów prawa miejscowego.

Ostatnimi aktami prawnymi dotyczącymi ochrony danych osobowych są akty prawa wewnętrznie obowiązującego. Tworzą one otwarty katalog źródeł prawa. Oznacza to, że określone w przepisie art. 93 Kon-

[100] *Ibide*m, s. 118–128; D. Dąbek, *Prawo miejscowe*, Wolters Kluwer SA, Warszawa 2015, wyd. 2, s. 66; art. 94 Konstytucji RP.

stytucji RP wyliczenie organów uprawnionych do ich stanowienia – obejmujące Radę Ministrów, Prezesa Rady Ministrów i ministrów – jest przykładowe. Taki sam charakter mają wymienione tam nazwy aktów, tj. uchwały i zarządzenia. Aktom prawa wewnętrznie obowiązującego można nadać dowolną nazwę, z wyjątkiem niektórych nazw zastrzeżonych dla aktów prawa powszechnie obowiązującego. W praktyce określa się je najczęściej jako: uchwały, zarządzenia, statuty, regulaminy, instrukcje, wytyczne i okólniki. Ich cechą charakterystyczną jest ograniczony zakres obowiązywania. Obowiązują one „tylko jednostki organizacyjnie podległe organowi wydającemu te akty". To konstytucyjne sformułowanie jest pewnym uproszczeniem. Adresatami tych aktów są bowiem nie tylko podmioty podporządkowane organizacyjnie lub służbowo organowi wydającemu te akty. Są nimi również osoby ubiegające się o uzyskanie statusu użytkownika zakładu administracyjnego (w zakresie wymogów i procedur regulujących przyjęcie w poczet użytkowników tego zakładu) oraz osoby przebywające na terenie zakładu administracyjnego (w zakresie przepisów porządkowych). Dostrzega się ponadto oddziaływanie tych aktów na osoby znajdujące się poza strukturą zakładu. Mimo że prawo wewnętrzne nie może być podstawą podejmowania decyzji względem podmiotów spoza struktury (mogą być nią tylko przepisy prawa powszechnie obowiązującego), to dostrzega się jego pośrednie oddziaływanie. Określony w nich sposób postępowania wiąże bowiem osoby obowiązane do ich stosowania, a więc może mieć m.in. wpływ na sposób załatwiania spraw w urzędzie[101].

Przedmiotem aktów prawa wewnętrznie obowiązującego są również kwestie dotyczące ochrony danych osobowych. Akty te określają najczęściej politykę bezpieczeństwa danych osobowych w danej jednostce, a więc sposoby zabezpieczania danych osobowych i uzyskiwania dostępu do tych danych, wydawanie upoważnień do ich przetwarzania,

[101] E. Ochendowski, *op. cit.*, s. 133–135.

zadania określonych osób w związku z przetwarzaniem danych osobowych i zapewnieniem ich bezpieczeństwa, szczegółowe wymogi dotyczące bezpieczeństwa oraz sposób postępowania w przypadku wystąpienia incydentów bezpieczeństwa. Prawo wewnętrzne umożliwia dostosowanie sposobu ochrony danych osobowych w danej jednostce do sposobu i zakresu realizowanych przez nią zadań. Musi być ono zgodne z prawem powszechnie obowiązującym.

3. Przegląd wybranych aktów prawnych dotyczących ochrony danych osobowych

Oprócz omówionego podziału aktów prawnych, uwzględniającego akty powszechnie i wewnętrznie obowiązujące, istnieje jeszcze wiele innych podziałów. Biorąc pod uwagę stopień szczegółowości aktu i to w jakim zakresie jego przepisy dotyczą ochrony danych osobowych, można wyróżnić akty prawne o charakterze ogólnym (tylko niektóre ich przepisy dotyczą prawa do prywatności lub prawa ochrony danych osobowych[102]) i akty prawne o charakterze szczegółowym (zawierają głównie lub wyłącznie przepisy dotyczące ochrony danych osobowych[103]).

W celu uporządkowania wywodów podział ten będzie podstawą rozważań w tej części pracy. Ze względu na ich ograniczony zakres zostaną one dokonane w sposób syntetyczny, z uwzględnieniem wybranych aktów prawa krajowego i międzynarodowego należących do różnych systemów ochrony praw człowieka.

[102] Jest nim np. Konstytucja RP.
[103] Jest nim np. RODO.

3.1. Akty prawne o charakterze ogólnym

3.1.1. Akty prawne Organizacji Narodów Zjednoczonych

Powszechna Deklaracja Praw Człowieka i Konwencja o prawach dziecka

W tym roku mija siedemdziesiąt lat od uchwalenia Powszechnej Deklaracji Praw Człowieka[104]. Jest ona uznawana za podstawowy akt międzynarodowego prawa praw człowieka w wymiarze uniwersalnym, a wymienione w niej prawa nie tracą na aktualności. Chociaż status PDPCz jest przedmiotem sporu – jest ona uznawana za prawo zwyczajowe, a nie traktatowe – to nie ulega wątpliwości, że odgrywa ona istotną rolę w uniwersalnym systemie ochrony praw człowieka[105].

Artykuł 12 PDPCz reguluje prawo do prywatności. Zabrania on samowolnej ingerencji w czyjekolwiek życie prywatne, rodzinne, domowe i korespondencję. Za niedopuszczalne uznaje uwłaczanie honorowi lub dobremu imieniu i przyznaje każdemu człowiekowi prawo do ochrony prawnej przed takimi działaniami. Przepis ten jest również podstawą ochrony danych osobowych, w szczególności w zakresie wymiany informacji dotyczących prywatnych stosunków i ochrony danych przekazywanych w korespondencji, w tym drogą elektroniczną[106].

Prawo do prywatności jest uregulowane również w przepisie art. 16 Konwencji o prawach dziecka[107]. Akt ten formułuje je podobnie jak Powszechna Deklaracja Praw Człowieka. Adresatami prawa są jednak wy-

[104] Uchwalona przez ZO ONZ dnia 10 grudnia 1948 r. rezolucją 217/III A.

[105] M. Piechowiak, *Filozofia praw człowieka. Prawa człowieka w świetle ich międzynarodowej ochrony*, Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego, Lublin 1999, s. 25–26.

[106] L.A. Rehof, *Article 12*, [w:] G. Alfreddson, A. Eide (red.), *The Universal Declaration of Human Rights. A Common Standard of Achievement*, Martinus Nijhoff Publishers, Hague, Boston, London 1999, s. 263–264.

[107] Przyjęta przez ZO ONZ dnia 20 listopada 1989 r. (Dz. U. z 1991 r. Nr 120, poz. 526 ze zm.).

łącznie dzieci. Zapewnia on im ochronę przed arbitralną i bezprawną ingerencją podmiotów publicznych i prywatnych[108].

Międzynarodowy Pakt Praw Obywatelskich i Politycznych

Międzynarodowy Pakt Praw Obywatelskich i Politycznych[109] – w odróżnieniu od Powszechnej Deklaracji Praw Człowieka – jest wiążącą strony umową międzynarodową. Jej stronami są prawie wszystkie państwa świata[110]. Zobowiązały się one do popierania powszechnego poszanowania i przestrzegania praw i wolności człowieka, w szczególności określonych w Pakcie. Jednym z nich jest prawo do prywatności[111]. Sposób sformułowania tego prawa jest analogiczny do przyjętego w Powszechnej Deklaracji Praw Człowieka.

Kodeks Postępowania Funkcjonariuszy Porządku Prawnego

Kodeks Postępowania Funkcjonariuszy Porządku Prawnego jest aneksem do rezolucji 34/169 Zgromadzenia Ogólnego ONZ z 1979 r.[112] Określa on sposób postępowania funkcjonariuszy porządku prawnego w związku z pełnioną przez nich funkcją. Nakazuje, aby będące w ich posiadaniu poufne informacje – poza wyjątkami określonymi w rezolucji – były przechowywane w sposób zapewniający ich szczególną ochronę[113]. Dotyczy to przede wszystkim informacji z życia prywatnego osób i informacji mogących powodować szkodę ich interesom oraz ich reputacji. Informacje te

[108] S. Detrick, *A Commentary on the United Nations Convention on the Rights of the Child*, Martinus Nijhoff Publishers, Hague, Boston, London 1999, s. 269–271.

[109] Otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167).

[110] Zob. interaktywną mapę państw stron i sygnatariuszy, http://indicators.ohchr.org/ [dostęp 31.07.2018].

[111] Artykuł 17 Paktu.

[112] http://www.un.org/documents/ga/res/34/a34res169.pdf [dostęp 30.07.2018].

[113] Artykuł 4 rezolucji.

powinny być wykorzystywane wyłącznie do celów określonych w akcie, mieszczących się w zakresie realizacji zadań publicznych[114].

3.1.2. Akty prawne Rady Europy

Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności

Prawo do poszanowania życia prywatnego gwarantuje przepis art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[115]. W odróżnieniu od PDPCz dopuszcza on wprost ograniczenie prawa w drodze ustawy przez państwa członkowskie. Może to nastąpić wyłącznie w przypadkach koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe lub publiczne, dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.

Określone w Konwencji prawa przysługują osobom będącym pod jurysdykcją Państw-Stron Konwencji, a więc państw członkowskich Rady Europy[116]. Ich przestrzeganie gwarantuje Europejski Trybunał Praw Człowieka w Strasburgu. Osoba, która uważa, że jej prawo zostało naruszone, może – po wyczerpaniu wszystkich środków odwoławczych przysługujących jej na mocy prawa wewnętrznego – wnieść skargę do Trybunału[117].

[114] Wykładnia autentyczna rezolucji: http://www.un.org/documents/ga/res/34/a34res169.pdf [dostęp 30.07.2018].

[115] Sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284).

[116] Stronami Konwencji jest 47 państw. Dostęp: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=XzqJo591 [dostęp 31.07.2018 r.].

[117] Rozdział II Konwencji.

3.1.3. Akty prawne Unii Europejskiej

Traktat o Unii Europejskiej i Traktat o funkcjonowaniu Unii Europejskiej

Traktat o Unii Europejskiej[118] ustanowił Unię Europejską. Jest ona organizacją ponadnarodową[119] opartą na wspólnych wartościach, do których należą m.in. poszanowanie godności osoby ludzkiej i poszanowanie praw człowieka[120]. Jednym z praw uznawanych przez Unię jest prawo do ochrony danych osobowych. Zostało ono potwierdzone w głównych aktach prawa pierwotnego, którymi są Traktat o Unii Europejskiej, Traktat o funkcjonowaniu Unii Europejskiej[121] i Karta praw podstawowych Unii Europejskiej[122]. Wiążą one wszystkie państwa członkowskie Unii Europejskiej.

Przepis art. 16 TFUE wprowadza powszechne prawo do ochrony danych osobowych. Jest on wyraźną i wyczerpującą podstawą podejmowania środków mających na celu ochronę tych danych[123]. Przepisy TUE i TFUE upoważniają również – w ograniczonym zakresie – Radę i Parlament do określenia zasad ochrony osób fizycznych w związku z przetwarzaniem ich danych i określenia zasad przepływu tych danych. Kontrolę przestrzegania zasad sprawują niezależne organy[124].

---

[118] Zob. art. 1 i preambuła Traktatu o Unii Europejskiej podpisanego dnia 7 lutego 1992 r. w Maastricht (Dz. U. z 2004 r. Nr 90, poz. 864/30 ze zm.).

[119] Posiada ona „struktury (instytucje) utworzone przez państwa członkowskie, na które delegowano uprawnienia narodowe. […] Zarządzają one otrzymanymi uprawieniami i dzięki temu wytwarzają autonomiczny porządek prawny, a nawet mają nadzór nad elementami składowymi systemu, w którym działają" (J. Ruszkowski, *Ponadnarodowość w systemie politycznym Unii Europejskiej*, Wolter Kluwer Polska, Warszawa 2010, s. 109).

[120] Artykuł 2 TUE.

[121] Dz. U. z 2004 r. Nr 90, poz. 864/2 ze zm.

[122] Dz. Urz. UE C 303 z 14.12.2007 r., s. 1 ze zm.

[123] F. Pizzetti, *Article 39 TEU*, [w:] H.J. Blake, S. Mangiameli (red.), *The Treaty on European Union (TEU). A commentar*, Springer, Heidelberg-New York-Dordrecht-London 2013, s. 1160.

[124] Artykuł 39 TUE i art. 16 TFUE.

Karta praw podstawowych Unii Europejskiej

Powszechne prawo do ochrony danych osobowych jest również uregulowane w przepisie art. 8 KPP. Określa on wprost zasady przetwarzania danych osobowych przyjmując, że powinno ono być rzetelne i celowe, a jego legalność wymaga uzyskania zgody osoby zainteresowanej lub wykazania istnienia innej podstawy prawnej uzasadniającej przetwarzanie. Na mocy tego przepisu osoby, których dane dotyczą, mają prawo dostępu do danych ich dotyczących i do dokonania ich sprostowania.

Prawa określone w KPP – w tym prawo do ochrony danych osobowych – nie są wyłącznie kontynuacją dotychczasowego dorobku Wspólnot Europejskich, lecz wykraczają poza ten zakres. Czerpią w znacznym stopniu ze standardów uniwersalnego systemu ochrony praw człowieka i systemu ochrony praw człowieka Rady Europy[125]. Określone w KPP prawo nie powiela zatem wyłącznie treści przepisów innych aktów prawnych, lecz rozwija je i doprecyzowuje.

3.1.4. Akty prawne prawa krajowego

Konstytucja Rzeczypospolitej Polskiej

Konstytucja Rzeczypospolitej Polskiej jest aktem prawa powszechnie obowiązującego w Rzeczypospolitej Polskiej mającym najwyższą moc prawną[126]. Zawiera ona przepisy o wysokim stopniu ogólności, uszczegóławiane w aktach normatywnych niższego rzędu.

Przepis art. 47 Konstytucji RP określa prawo do prywatności, obejmujące swym zakresem autonomię informacyjną[127]. Przepis ten jest uznawany za *lex generalis* względem pozostałych norm konstytucyjnych do-

[125] J. Sobczak, *Komentarz do art. 8*, [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, C.H. Beck, Warszawa 2013, s. 263–264.

[126] Artykuł 87 Konstytucji RP.

[127] Zob. M. Safjan, *Ochrona danych osobowych – granice autonomii informacyjnej. Paradoks towarzyszący rozwojowi współczesnych technik informatycznych*, [w:] M. Wyrzykowski, *Ochrona danych osobowych*, Instytut Spraw Publicznych. Centrum Konstytucjonalizmu i Kultury Prawnej, Warszawa 1999, s. 9–33.

tyczących prywatności, w tym prawa do ochrony danych osobowych, z którym jest ściśle związany[128].

W świetle orzecznictwa Trybunału Konstytucyjnego prawo do prywatności służy ochronie tych samych wartości, które są chronione w ramach prawa do ochrony danych osobowych. W ocenie I. Lipowicz przyjęcie tego twierdzenia jest jednak ryzykowne. Prowadzi bowiem do błędu w rozumowaniu powodującego istotne skutki praktyczne. Skoro prawa te przysługują tylko „osobom", a osoby zmarłe nie są już „osobami", to nie możemy rozważać prawa ochrony danych osobowych w kontekście osób zmarłych. Interpretacja ta jest niespójna z innymi regulacjami prawnymi nakazującymi m.in. poszanowanie szczątków osób zmarłych, wykonanie ich ostatniej woli oraz ochronę ich twórczości[129]. Wynika to z błędnego wywodzenia prawa do ochrony danych osobowych z prawa do prywatności. Wobec tego postuluje się, aby wyprowadzać je również z przepisów dotyczących ochrony godności człowieka, która jest fundamentem i podstawą wszelkich praw[130].

Szczegółowe przepisy Konstytucji RP dotyczące ochrony danych osobowych stanowią, że każdej osobie przysługuje prawo dostępu do danych jej dotyczących, w tym zawartych w dokumentach urzędowych, oraz prawo żądania sprostowania danych i żądania usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Zakazują one zobowiązania osób do ujawniania informacji ich dotyczących na innej podstawie niż ustawa (art. 51 Konstytucji RP).

Obywatelom polskim przyznają ponadto dodatkowy zakres ochrony. Konstytucja zakazuje bowiem pozyskiwania, gromadzenia i udostęp-

[128] B. Banaszak, *Komentarz do art. 47*, [w:] B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, C.H. Beck, Warszawa 2012, s. 294; D. Ossowska, *Wolności i prawa osobiste*, [w:] M. Chmaj (red.) *Wolności i prawa człowieka w Konstytucji Rzeczypospolitej Polskiej*, Wolters Kluwer Polska, Warszawa 2008, wyd. 2, s. 107–108.

[129] Zob. szerzej nt. praw zmarłych: J. Mazurkiewicz, *Non omnis moriar. Ochrona dóbr osobistych zmarłego w prawie polskim*, Prawnicza i Ekonomiczna Biblioteka Cyfrowa, Wrocław 2010.

[130] I. Lipowicz, *Konstytucyjne podstawy ochrony…*, s. 47–48.

niania innych informacji ich dotyczących niż te, które są niezbędne w demokratycznym państwie prawnym.

Uzasadnienie gromadzenia informacji ze względu na niezbędność w demokratycznym państwie prawnym może budzić wątpliwości. „Niezbędność" jest bowiem pojęciem nieostrym, które może być interpretowane w różny sposób[131]. Trudno ustalić jednoznacznie i bezspornie, że dana informacja jest np. niezbędna dla realizacji zadania publicznego. Nawet gdy udzielimy odpowiedzi twierdzącej, to nie jesteśmy w stanie zapobiec trudnym do przewidzenia skutkom gromadzenia, przetwarzania i udostępniania tych informacji. Mogą one bowiem powodować negatywne skutki nie tylko względem osób, których dane dotyczą, lecz także względem innych osób.

Przykładowo, twierdzi się, że ujawnianie danych osobowych osób skazanych prawomocnym wyrokiem za popełnienie przestępstw na tle seksualnym w publicznym rejestrze sprawców tych przestępstw służy zapewnieniu porządku i bezpieczeństwa publicznego. W takim ujęciu ujawnianie ich danych osobowych jest niezbędne dla realizacji zadania publicznego, mieszczącego się w zakresie funkcji policyjnej administracji. Podanie do publicznej wiadomości tych danych skutkuje jednak kierowaniem gróźb karalnych pod adresem osób, których dane ujawniono w rejestrze. Skutkuje również dokonywaniem na nich samosądów. Rzecznik Praw Obywatelskich zauważa ponadto pośredni skutek udostępniania tych danych. Jest nim negatywny stosunek osób z otoczenia do członków rodzin sprawców przestępstw, którzy są niejednokrotnie osobami przez nich pokrzywdzonymi. Ujawnienie informacji prowadzi więc do ich stygmatyzacji, przyczyniając do spotęgowania negatywnych doznań, a w długofalowej perspektywie także do ich wykluczenia społecznego[132].

[131] Przykładowo, zdaniem niektórych gromadzenie informacji dotyczących osób będących w związkach jednopłciowych, domagających się dokonania transkrypcji zagranicznego aktu małżeństwa, jest niezbędne dla realizacji zadań demokratycznego państwa prawnego. Zdaniem innych jest ono niedopuszczalne.

[132] RPO do Ministra Sprawiedliwości: *„rejestr pedofilów" uderza w niewinnych członków rodzin sprawców. Są już pierwsze takie przypadki*, wersja el., https://www.rpo.gov.pl/pl/content/Bodnar-do-Ziobry-rejestr-pedofilow-uderza-w-niewinnych [dostęp 30.07.2018].

3.1.5. Inne akty prawne o charakterze ogólnym dotyczące ochrony danych osobowych

Przepisy dotyczące ochrony i sposobu przetwarzania danych osobowych są zawarte w wielu aktach normatywnych. Wykazują one znaczne zróżnicowanie. Są to przede wszystkim akty regulujące pozycję prawną określonych osób[133] lub służb[134] albo akty regulujące sposób lub tryb podejmowania określonych działań[135], w tym świadczenia usług[136]. Niekiedy wyznaczają one precyzyjnie cel i zakres przetwarzania danych osobowych[137], innym razem odnoszą się do niego w sposób ogólny, odsyłając w nieuregulowanym zakresie do stosowania przepisów dotyczących ochrony danych osobowych zawartych w innych aktach normatywnych[138]. W niektórych przypadkach ograniczają one zastosowanie przepisów ogólnych, w tym RODO[139].

[133] Zob. np. art. 22^1-22^3 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2018 r., poz. 917 ze zm.), dalej k.p.

[134] Zob. np. art. 29 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (t.j. Dz. U. z 2018 r., poz. 430 ze zm.); art. 56–61 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r., poz. 138 ze zm.), art. 20 ustawy z dnia 6 kwietnia 1990 r. o Policji (t j. Dz. U. z 2017 r., poz. 2067 ze zm.).

[135] Zob. np. art. 16–18 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań z zakresu informatyzacji działalności organów Krajowej Administracji Skarbowej (t.j. Dz. U. z 2017 r., poz. 2192); rozdział 6 ustawy z dnia 24 września 2010 r. o ewidencji ludności (t.j. Dz. U. z 2018 r., poz. 1382); art. 19–19a ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (t.j. Dz. U. z 2017 r., poz. 1000); art. 39–42 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (t.j. Dz. U. z 2018 r., poz. 999 ze zm.).

[136] Zob. np. rozdział 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2017 r., poz. 1219 ze zm.) i art. 8 i 22a ustawy z dnia 6 lipca 2001 r. o usługach detektywistycznych (t.j. Dz. U. z 2017 r., poz. 556 ze zm.).

[137] Zob. np. dział VII ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2017 r., poz. 1907 ze zm.) i rozdział 4a ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (t.j. Dz. U. z 2018 r., poz. 997 ze zm.).

[138] Zob. np. art. 9 ustawy z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych (t.j. Dz. U. z 2018 r., poz. 410 ze zm.).

[139] Zob. np. art. 121 ustawy z dnia 15 czerwca 2018 r. o zbiorowym zarządzaniu prawami autorskimi i prawami pokrewnymi (Dz. U. poz. 1293).

3.2. Akty prawne o charakterze szczegółowym

3.2.1. Akty prawne Organizacji Narodów Zjednoczonych

Rezolucja 45/95 Zgromadzenia Ogólnego ONZ

Rezolucja 45/95 Zgromadzenia Ogólnego ONZ[140] zawiera niewiążące wytyczne w sprawie uregulowania kartotek skomputeryzowanych plików danych osobowych. Składa się ona z dwóch części. Pierwsza określa zasady, które powinny być zapewnione w prawie krajowym w celu zagwarantowania minimalnej ochrony danych osobowych. Są nimi:

- zasada zgodnego z prawem i sprawiedliwego przetwarzania danych;
- zasada dokładności/precyzyjności gromadzenia danych (wymaga m.in. bieżących aktualizacji danych i dbałości o ich kompletność);
- zasada celowości przetwarzania (cel powinien być jasno określony i prawnie uzasadniony, a gromadzone dane powinny być z nim zgodne. Okres przetwarzania danych powinien pozostawać w ścisłej relacji do celu przetwarzania);
- zasada dostępu osoby zainteresowanej do danych jej dotyczących (możliwa do zidentyfikowania osoba, której dane dotyczą, ma prawo uzyskać informację na temat tego, czy są przetwarzane jej dane. Ma ona również prawo do ich sprostowania i wykreślenia, gdy są zbędne dla przetwarzania lub nieprawidłowe);
- zasada niedyskryminacji (dotyczy gromadzenia danych wrażliwych, które mogłyby być powodem dyskryminowania. Są to np. dane dotyczące pochodzenia rasowego lub etnicznego, rasy, orientacji seksualnej i wyznawanej religii);

[140] Przyjęta przez ZO ONZ w dniu 14 grudnia 1990 r.

– zasada bezpieczeństwa (wymaga stosowania odpowiednich środków ochrony danych przed zagrożeniami naturalnymi i niezgodnym z prawem dostępem do danych)[141].

Zgodnie z rezolucją prawo krajowe powinno urzeczywistniać te zasady i przewidywać kary za ich naruszenie[142]. Właściwe przestrzeganie zasad powinien zagwarantować niezależny krajowy organ nadzorczy. Z zastrzeżeniem wyjątków określonych w rezolucji zasady te stosuje się również do przechowywania danych przez rządowe organizacje międzynarodowe (cześć druga rezolucji).

3.2.2. Akty prawne Rady Europy

Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych wraz z protokołem dodatkowym

Dane osobowe mogą być przetwarzane ręcznie lub w sposób zautomatyzowany, polegający na gromadzeniu danych, stosowaniu do nich operacji logicznych i/lub arytmetycznych, ich modyfikowaniu, usuwaniu, wybieraniu lub rozpowszechnianiu w całości lub części za pomocą procedur zautomatyzowanych. Niezależnie od sposobu przetwarzania dane osobowe powinny być chronione w jak największym zakresie[143].

Ochronę danych osobowych w związku z automatycznym przetwarzaniem danych (w tym międzynarodowym) w sektorze publicznym i prywatnym regulują przepisy Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych oraz

[141] *Principle of lawfulness and fairness; principle of accuracy; principle of the purpose-specification; principle of interested-person access; principle of non-discrimination; principle of security.*

[142] W określonym zakresie może przewidywać odstępstwa ich stosowania (pkt 6 rezolucji).

[143] Artykuł 2 lit. c Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych sporządzonej w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25 ze zm.).

przepisy protokołu dodatkowego do tej Konwencji[144]. Ich celem jest zapewnienie wszystkim osobom fizycznym znajdującym się na terytorium Państw-Stron Konwencji poszanowania praw i podstawowych wolności. Jednym z nich jest prawo do prywatności, z którego Konwencja wywodzi prawo ochrony danych osobowych.

Konwencja określa zasady przetwarzania danych, w tym: rzetelność, legalność, celowość, ograniczony zakres przetwarzania, dokładność i aktualność oraz ograniczony czas przechowywania. Wymaga ona podejmowania odpowiednich środków bezpieczeństwa względem przetwarzanych danych, zakazując równocześnie przetwarzania niektórych kategorii danych w sposób automatyczny. Konwencja określa ponadto prawa[145] osób, których dane dotyczą, w związku z przetwarzaniem ich danych[146]. W celu zabezpieczenia realizacji tych praw Państwa-Strony zobowiązały się do utworzenia niezależnych organów nadzorczych i przyznania im niezbędnych kompetencji w tym zakresie[147].

3.2.3. Akty prawne Unii Europejskiej

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 – RODO

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie w sprawie ochrony danych) jest potocznie określane rozporządzeniem

[144] Protokół dodatkowy do Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych.

[145] Są nimi: prawo uzyskania informacji dotyczących przetwarzania jej danych, prawo dostępu do danych, prawo sprostowania i usunięcia danych oraz prawo złożenia skargi w przypadku naruszenia określonych praw.

[146] Artykuły 5–8 Konwencji.

[147] Artykuł 1 protokołu dodatkowego.

o ochronie danych osobowych (RODO). Akt ten nawiązuje w wielu kwestiach do nieobowiązującej już dyrektywy 95/46/WE. Jest on jej rozwinięciem i doprecyzowaniem, uwzględniającym problemy praktyczne występujące dotychczas pod rządami dyrektywy. Uregulowanie kwestii związanych z ochroną danych osobowych osób fizycznych w rozporządzeniu powinno przyczynić się do zagwarantowania bardziej efektywnej ochrony tych osób, jednakowej w każdym państwie członkowskim[148]. Przetwarzanie danych z uwzględnieniem przepisów RODO powinno sprzyjać swobodnemu przepływowi danych osobowych wewnątrz Unii[149].

Celem RODO jest zwiększenie kontroli osób fizycznych nad ich danymi osobowymi[150]. RODO poszerza zakres niektórych praw uregulowanych dotychczas w dyrektywie 95/46/WE i przyznaje osobom, których dane dotyczą, nowe prawa[151].

RODO określa zasady przetwarzania danych osobowych. Nakłada nowe obowiązki na administratorów danych i podmioty przetwarzające, zwiększając ich odpowiedzialność za przetwarzanie. Jeśli naruszą oni prawa osób, których dane dotyczą, może im zostać wymierzona administracyjna kary pieniężna w wysokości określonej przepisami w RODO[152].

Osoby, których prawa zostały naruszone w związku z przetwarzaniem, mogą skutecznie dochodzić realizacji tych praw w postępowaniu administracyjnym i sądowym oraz uzyskać odszkodowanie za poniesione szkody.

Przepisy RODO znajdują zastosowanie do ręcznego przetwarzania danych oraz do przetwarzania całkowicie lub częściowo zautomatyzowanego. Wyznaczają standardy ochrony danych osobowych w przypadku przekazywania ich z Unii administratorom, podmiotom przetwarza-

[148] Zob. terytorialny zakres stosowania, określony w art. 3 RODO.
[149] Motyw 10 i 13 preambuły RODO.
[150] Motyw 7 preambuły RODO.
[151] Zob. art. 14–22 i art. 77–82 RODO.
[152] Zob. art. 83 RODO.

jącym lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym[153].

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 – tzw. dyrektywa policyjna

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 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 uchylająca decyzję ramową Rady 2008/977/WSiSW[154] jest potocznie zwana dyrektywą policyjną.

Określa ona zasady przetwarzania danych, zobowiązując państwa członkowskie do ustalenia terminów usuwania danych lub dokonywania ich okresowego przeglądu. Dyrektywa wyróżnia kilka kategorii osób, których dane dotyczą, z uwzględnieniem ich statusu w ramach określonego postępowania. Określa ponadto różne kategorie danych osobowych.

Osobom, których dane dotyczą, przyznaje określone prawa związane z przetwarzaniem ich danych osobowych. W przypadku ich naruszenia mogą one dochodzić ich realizacji w postępowaniu administracyjnym i sądowym, a podmiotowi dokonującemu naruszeń może zostać wymierzona kara[155].

Dyrektywa nie została dotychczas implementowana do polskiego porządku prawnego. Aktualnie trwają prace nad projektem ustawy wdrażającej – ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[156]. W ocenie Rzecznika Praw Obywatelskich niektóre przepisy projektu ustawy budzą wątpliwości,

[153] Motyw 101 RODO.

[154] Dz. Urz. UE L 119 z 4.05.2016 r., s. 89 ze zm.

[155] Artykuł 4–10, 12–16, 52–57 dyrektywy.

[156] Zob. projekt ustawy: https://bip.kprm.gov.pl/kpr/form/r8706884065,Projekt-ustawy-o-ochronie-danych-osobowych-przetwarzanych-w-zwiazku-z-zapobiegan.html [dostęp 28.07.2018].

w szczególności w zakresie wyłączenia z zakresu jej stosowania danych osobowych przetwarzanych przez niektóre służby specjalne, sprawowania kontroli nad przestrzeganiem przepisów dyrektywy oraz ograniczaniem praw osób, których dane dotyczą[157].

3.2.4. Akty prawne prawa krajowego

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych w zakresie obowiązującym przed ostatnimi nowelizacjami – związanymi z polską i europejską reformą ochrony danych osobowych[158] – miała na celu dokonanie implementacji dyrektywy 95/46/WE. W nauce prawa wyrażano jednak wątpliwości dotyczące jej prawidłowości i zupełności[159].

W związku ze zmianami wprowadzonymi przez RODO została ona w znacznym stopniu znowelizowana. Stosuje się ją obecnie do przetwarzania danych przez organy państwowe, organy samorządu terytorialnego oraz państwowe i komunalne jednostki organizacyjne. Dotyczy ona przetwarzania w sposób ręczny i zautomatyzowany[160].

Przepisy ustawy określają powszechne prawo do ochrony danych osobowych. Definiują istotne pojęcia dotyczące danych osobowych, a w szczególności: dane osobowe, zgodę na przetwarzanie danych[161],

[157] Zob. szerzej: *Pismo Rzecznika Praw Obywatelskich z dnia 26 kwietnia 2018 r. do Ministra Spraw Wewnętrznych i Administracji, sygn. VII.501.315.2014.AG*, wersja el., https://www.rpo.gov.pl/sites/default/files/Stanowisko RPO w sprawie projektu ustawy wdrażającej dyrektywę policyjną .pdf [dostęp 30.07.2018].

[158] Zob. szerzej: E. Bielak-Jomaa, D. Lubasz (red. nauk.), *Polska i europejska reforma ochrony danych osobowych*, Wolters Kluwer, Warszawa 2016.

[159] J. Barta, R. Markiewicz, *Prawo polskie a prawo wspólnotowe (zgodność polskiego ustawodawstwa z dyrektywą w sprawie ochrony danych osobowych)*, [w:] J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Zakamycze, Kraków 2001, s. 102–124.

[160] Artykuł 2 i 3 ustawy.

[161] Szerzej nt. zgody: P. Fajgielski, *Zgoda na przetwarzanie danych osobowych*, [w:] G. Sibiga, X. Konarski (red.), *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Wolters Kluwer Polska, Warszawa 2007, s. 41–60.

zbiór danych, system teleinformatyczny, zabezpieczenie danych osobowych w systemie teleinformatycznym i usunięcie danych. Ustawa określa również kompetencje organu centralnego właściwego w zakresie ochrony danych osobowych[162]. Ustala także sposób prowadzenia kontroli procesu przetwarzania danych i sposób postępowania w przypadku naruszenia przepisów prawa dotyczących ochrony danych osobowych. Ustawa określa ponadto zasady przetwarzania i prawa osób, których dane dotyczą. Wyznacza także warunki dopuszczalności przekazywania danych do państwa trzeciego[163].

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych dostosowuje częściowo polskie ustawodawstwo do zmian wprowadzonych europejską reformą prawa danych osobowych[164]. Nadal konieczne jest jednak przyjęcie dodatkowych przepisów dotyczących przetwarzania danych osobowych w różnych sektorach. Obecnie przygotowywany jest projekt ustawy, którego przyjęcie zaplanowano na czwarty kwartał 2018 r.[165]

Przepisy ustawy o ochronie danych osobowych uzupełniają przepisy RODO, w szczególności w zakresie dotyczącym przeprowadzania kontroli przestrzegania przepisów o ochronie danych osobowych, prowadzenia postępowań w sprawie naruszenia tych przepisów i ustalenia procedur stosowanych w przypadku realizacji praw określonych w RODO. Wynika to z zasady autonomii proceduralnej państw członkowskich, zgodnie

[162] W tym zakresie posługuje się już nieaktualną nomenklaturą, nawiązuje bowiem do Generalnego Inspektora Ochrony Danych Osobowych (art. 14), który został już zastąpiony Prezesem Urzędu Ochrony Danych Osobowych.

[163] Artykuły 1, 6, 15–19b, 23–35 i 47–48 ustawy.

[164] Zob. rozdział 12 ustawy.

[165] Zob. projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/prace-legislacyjne-rm-i/prace-legislacyjne-rady/wykaz-prac-legislacyjny/r7079293730832,Projekt-ustawy-Przepisy-wprowadzajace-ustawe-o-ochronie-danych-osobowych.html [dostęp 30.07.2018].

z którą właściwe procedury – w tym służące realizacji praw osób, których dane dotyczą – określają samodzielnie państwa członkowskie. Przepisy te zostaną szczegółowo omówione w rozdziale poświęconym analizie bezpośrednich środków ochrony danych osobowych.

Ustawa o ochronie danych osobowych zawiera ponadto przepisy dotyczące sposobu nakładania administracyjnych kar pieniężnych i terminu ich uiszczenia. Przewiduje również kary za nielegalne przetwarzanie danych osobowych i udaremnienie lub utrudnienie prowadzenia kontroli. Reguluje ponadto szczegóły związane z wyznaczaniem inspektorów ochrony danych, udzielaniem akredytacji podmiotom certyfikującym, certyfikacją oraz kodeksami postępowania.

Ustawa wyznacza pozycję prawną krajowego organu właściwego w sprawach ochrony danych osobowych – Prezesa Urzędu Ochrony Danych Osobowych. Ustala tryb jego powołania i przyznaje kompetencje niezbędne do realizacji zadań. Organ ten zastąpił istniejącego dotychczas Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera

Ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera[166] jest aktem prawa krajowego regulującym kwestie związane z przetwarzaniem danych osobowych dotyczących przelotu pasażerów korzystających z usług przewoźników lotniczych w celu zapobiegania, wykrywania i zwalczania przestępstw o charakterze terrorystycznym i innych przestępstw (w tym skarbowych) oraz ścigania ich sprawców[167].

Określa ona szczegółowo cele przetwarzania danych przez przewoźników lotniczych, kategorie danych, zasady ich przetwarzania i procedurę ich przekazywania odpowiednim organom. Ustala sposoby przetwarzania danych zapewniające ich bezpieczeństwo, w tym określa procedurę deperso-

[166] Dz. U. poz. 894.

[167] Artykuł 1 ust. 1 ustawy.

nalizacji danych, polegającą na „uczynieniu niewidocznymi" niektórych danych dla osób je przetwarzających. Przewiduje ponadto wyznaczenie osoby pełniącej funkcję inspektora do spraw ochrony danych o pasażerach.

Ustawa reguluje kwestie dotyczące współpracy międzynarodowej w zakresie wymiany danych osobowych pasażerów. Określa również administracyjne kary pieniężne za naruszenie przepisów ustawy w związku z niedopełnieniem obowiązku przekazywania danych właściwym organom, a kompetencję do ich wymierzania przyznaje Komendantowi Głównemu Straży Granicznej.

3.2.5. Inne akty prawne o charakterze szczegółowym dotyczące ochrony danych osobowych

Ochrona danych osobowych jest uregulowana w wielu różnych aktach prawa krajowego i międzynarodowego dotyczących wyłącznie tej problematyki. Dokonany w pracy przegląd aktów uwzględnił tylko niektóre z nich. Celem rozważań było ukazanie ich różnorodności. Dlatego też omówiono akty wiążące i niewiążące; krajowe i międzynarodowe; przyjmowane przez państwa, organizacje międzynarodowe i organizacje ponadnarodowe. Istnieją ponadto specyficzne akty regulujące ochronę danych osobowych w kościołach i związkach lub wspólnotach wyznaniowych, do których wydania upoważnia art. 91 RODO. Wykazują one odmienności względem regulacji o charakterze ogólnym[168].

Oprócz wymienionych i omówionych w tej części pracy aktów normatywnych ochrona danych osobowych jest ponadto regulowana w in-

[168] Jednym z nich jest dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim wydany przez Konferencję Episkopatu Polski, w dniu 13 marca 2018 r., podczas 378. Zebrania Plenarnego w Warszawie, na podstawie kan. 455 Kodeksu Prawa Kanonicznego, w związku z art. 18 Statutu Konferencji Episkopatu Polski, po uzyskaniu specjalnego zezwolenia Stolicy Apostolskiej z dnia 3 czerwca 2017 r. (https://episkopat.pl/wp-content/uploads/2018/04/13.3.2018.PL_.Dekret-ogolny-o-ochronie-danych-osobowych.pdf, [dostęp 19.07.2018]).

nych aktach prawa krajowego[169], a także rezolucjach, zaleceniach i rekomendacjach Rady Europy[170], wiążących i niewiążących aktach prawa wtórnego Unii Europejskiej[171] i aktach innych organizacji, w tym działających na rzecz ochrony praw człowieka[172].

Akty te zawierają najczęściej szczegółowe przepisy dotyczące przetwarzania i ochrony danych osobowych w określonych sektorach lub w związku z podejmowaniem określonych działań. Uwzględniają specyfikę przetwarzania danych i związane z nim zagrożenia.

[169] Są nimi np.: rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 maja 2018 r. w sprawie przetwarzania informacji przez Służbę Ochrony Państwa (Dz. U. poz. 1069); rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 maja 2018 r. w sprawie przetwarzania informacji przez Służbę Ochrony Państwa (Dz. U. poz. 1069) i rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 lipca 2016 r. w sprawie przetwarzania informacji przez Policję (Dz. U. poz. 1091 ze zm.).

[170] Są nimi np.: rezolucja (73) 22 z dnia 26 września 1973 r. o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze prywatnym; rekomendacja CM/REC (2015) 5 Komitetu Ministrów dla Państw Członkowskich z dnia 1 kwietnia 2015 r. na temat ochrony danych osobowych wykorzystywanych dla celów zatrudnienia; rekomendacja z dnia 23 listopada 2010 r. w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili; rekomendacja R(91) 10 z dnia 9 września 1991 r. dotycząca ochrony danych osobowych przekazywanych osobom trzecim przez instytucje publiczne.; rekomendacja R (85)20 Komitetu Ministrów dla Państw Członkowskich w sprawie ochrony danych osobowych używanych dla celów marketingu bezpośredniego, Rady Europy „Ochrona Danych Osobowych Wykorzystywanych dla potrzeb marketingu bezpośredniego" z dnia 25 października 1985 r.

[171] Są nimi np.: rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz. Urz. UE L 8 z dnia 12.01.2001 r., s. 1 ze zm.) i przepisy wykonawcze do tego rozporządzenia; rozporządzenie Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej (Dz. Urz. UE L z dnia 26.06.2013 r., Nr 173, s. 2); zalecenie Komisji (UE) z dnia 10 października 2014 r. w sprawie szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych (Dz. Urz. UE L 300 z 18.10.2014 r., s. 63).

[172] Zob. wyliczenie i omówienie aktów dot. ochrony danych osobowych: J. Barta, P. Fajgielski. R. Markiewicz, *Ochrona danych osobowych*, Wolters Kluwer SA, Warszawa 2015, wyd. 6, s. 48–56, 74–78 i 80–85.

Dokonana w nich modyfikacja zasad ogólnych dotyczących m.in. zakresu i sposobu przetwarzania danych oraz praw osób, których dane dotyczą, wynika niejednokrotnie ze stwierdzonej w tych przypadkach nadrzędności interesu publicznego nad interesem jednostki. Z uwagi na konieczność zapewnienia porządku i bezpieczeństwa publicznego lub inne prawnie doniosłe interesy publiczne dopuszcza się ingerencję w sferę prywatności osób, których dane dotyczą, oraz ogranicza się zakres przyznanych im praw. Dopuszczalność wprowadzania tych ograniczeń wynika m.in. z przepisu art. 23 RODO.

Osoby, których dane dotyczą, godzą się najczęściej świadomie i dobrowolnie na ograniczanie ich praw (np. pasażerowie linii lotniczych, z uwagi na zapewnienie ochrony przed atakami terrorystycznymi). W niektórych przypadkach zakres ograniczeń i sposób ich wprowadzania budzi jednak uzasadnione wątpliwości. W tych przypadkach na straży realizacji praw osób, których dane dotyczą, powinny stać sądy i organy administracji publicznej. Sytuacja komplikuje się jednak, gdy naruszycielem praw tych osób są organy administracji publicznej – poprzez działanie niezgodne z prawem lub niewłaściwe implementowanie określonych regulacji. W tym przypadku pozycja prawna osób, których dane dotyczą, ulega znacznemu osłabieniu.

Rozdział III

Zasady ochrony danych osobowych

(Maciej Błażewski)

1. Zasady ochrony danych osobowych jako zasady prawa

Zasada prawa stanowi szczególnego rodzaju normę prawną, która umożliwia prawidłową interpretację przepisów prawnych. Ma ona wyjątkowe znaczenie w procesie stanowienia oraz stosowania prawa. Zasadę prawa powinien uwzględnić prawodawca, tworząc przepisy prawa. Ma ona także znaczenie dla podmiotów stosujących te przepisy w praktyce[173]. Zasady prawa są normami prawnymi wymagającymi konkretyzacji przez inne normy[174]. Jednocześnie zasady określają kierunek ich wykładni[175].

Nauka prawa wyróżnia zasady o charakterze dyrektywalnym oraz normatywnym. Zasady dyrektywalne są wyrażone wprost w przepisach

[173] Zob. S. Wronkowska, *System prawny a porządek prawny i ład społeczny*, [w:] S. Wronkowska, Z. Ziembiński (red.), *Zarys teorii prawa*, Wydawnictwo Ars boni et aequi, Poznań 1997, s. 188. Problematykę zasad prawa, jako norm prawnych o podstawowym znaczeniu, porusza także J. Zimmermann, *Prawo administracyjne*, Wolters Kluwer, Warszawa 2014, s. 128. Na znaczenie zasad prawa dla interpretacji przepisów prawa wskazuje także E. Ura, *Prawo administracyjne*, LexisNexis, Warszawa 2010, s. 92–93.

[174] Zob. H. Maurer, *Ogólne prawa administracyjne*, (tłum. i red.) K. Nowacki, Kolonia Limited, Wrocław 2003, s. 63.

[175] Zob. J. Zimmermann, *Motywy decyzji administracyjnej i jej uzasadnienie*, Wydawnictwo Prawnicze, Warszawa 1981, s. 58; E. Ura, *op. cit.*, s. 92–93.

prawa, a zasady opisowe wymagają ich wyartykułowania przez naukę prawa oraz orzecznictwo[176]. Podział ten przekłada się także na zróżnicowanie siły oddziaływania tych dwóch rodzajów zasad prawa na stosowanie przepisów prawa. Zasady dyrektywalne bardziej oddziaływają na podmioty stosujące prawo, właśnie ze względu na ich wyraźne określone w regulacjach prawa. Zasady opisowe obowiązują jedynie, gdy są powszechnie akceptowalne, co oznacza, że podmiot stosujący te zasady powinien wpierw je zaakceptować[177]. Z tej przyczyny zasady ochrony danych osobowych, które mają dyrektywalny charakter, znacząco oddziaływają na wykładnię przepisów dotyczących ochrony danych osobowych. Zasady ochrony danych osobowych mające opisowy charakter także mają szczególne znaczenie w toku wykładni przepisów prawa, ze względu na ich powszechną akceptację.

Zasady prawa ochrony danych odnoszą się do przepisów prawnych związanych z przetwarzaniem i ochroną danych osobowych[178]. Prawodawca europejski w celu ułatwienia ich określenia wyodrębnił je wprost w przepisach prawa zawartych w rozporządzeniu 2016/679. Mają one zatem dyrektywalny charakter[179]. Wprowadzenie jednolitego katalogu zasad ma na celu określenie ram ochrony danych[180].

[176] Zob. A. Bałaban, L. Dubel, L. Leszczyński, *Zasady tworzenia prawa*, UMCS, Lublin 1986, s. 24; L. Leszczyński, *Wykładnia systemowo-aksjologiczna*, [w:] R. Hauser, Z. Niewiadomski, A. Wróbel (red.), *System praw administracyjnego. Wykładnia w prawie administracyjnym. Tom 4*, C.H. Beck, Warszawa 2012, s. 238.

[177] Problematykę znaczenia zasad dyrektywalnych oraz zasad opisowych przedstawiają m.in. S. Wronkowska, M. Zieliński, Z. Ziembiński, *Zasady prawa. Zagadnienia podstawowe*, Wydawnictwo Prawnicze, Warszawa 1974, s. 28–29; J. Zimmermann, *Motywy decyzji…*, s. 57; M. Zieliński, *Wykładnia prawa. Zasady, reguły, wskazówki*, LexisNexis, Warszawa 2010, s. 35.

[178] W świetle motywu 26 zd. 1 RODO zasady ochrony danych dotyczą wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych.

[179] Problematykę zasad o dyrektywalnym charakterze przedstawia S. Wronkowska, *op. cit*., s. 187.

[180] M. Dominiak, M. Gawroński, *Zasady przetwarzania danych osobowych*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018, s. 64.

Zasadami prawa ochrony danych są:

1. Zasada legalności.
2. Zasada rzetelności.
3. Zasada *privacy by design*.
4. Zasada *privacy by default*.
5. Zasada przejrzystości.
6. Zasada minimalizacji danych osobowych.
7. Zasada prawidłowości.
8. Zasada integralności i poufności.
9. Zasada ograniczenia celu przetwarzania danych.
10. Zasada ograniczenia przechowywania.
11. Zasada rozliczalności.

Zasady ochrony danych są ze sobą wzajemnie powiązane. Żadna z nich nie może być stosowana z pominięciem innych zasad[181]. Ze względu na swój zakres pierwotnymi, a zarazem nadrzędnymi zasadami są zasady legalności oraz zasada rzetelności[182]. Pozostałe zasady są względem siebie równe, choć mogą odpowiadać różnym obszarom procesu przetwarzania danych osobowych.

2. Zasada legalności

Zasada legalności wyrażona wyraźnie w art. 5 ust. 1 lit. a rozporządzenia 2016/679, w świetle którego dane osobowe muszą być przetwarzane zgodnie z prawem. Ma ona charakter pierwotny i nadrzędny wobec pozostałych zasad ochrony danych[183]. Należy ujmować ją szeroko, co oznacza,

[181] *Ibidem*, s. 66.

[182] P. Drobek, *Komentarz do art. 5*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 327; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*, [w:] P. Litewski (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 258.

[183] P. Drobek, *Komentarz do art. 5*..., s. 327.

że ma ona nadrzędny charakter względem pozostałych zasad ochrony danych osobowych[184]. Nakłada wymóg przestrzegania w toku procesu przetwarzania danych przepisów prawa, niezależnie od ich charakteru oraz rodzaju aktu normatywnego powszechnie obowiązującego, w którym przepisy te są wyrażone[185]. Podstawy prawne dla przetwarzania danych osobowych zostały częściowo wyrażone w art. 6 oraz art. 9 rozporządzenia 2016/679. Przepisy te, jako podstawa prawna przetwarzania, są uzupełnione przez inne regulacje zarówno tego rozporządzenia, jak i innych aktów szczególnych dotyczących ochrony danych osobowych[186]. Przepisy uzupełniające podstawę prawną regulują m.in. sposoby przetwarzania oraz zabezpieczenia danych osobowych[187].

3. Zasada rzetelności

Zasada rzetelności, podobnie jak poprzednia zasada, została w sposób wyraźny wyrażona w art. 5 ust. 1 lit. a rozporządzenia 2016/679, w myśl którego dane osobowe muszą być przetwarzane rzetelnie. Zasada ta oznacza obowiązek uwzględnienia interesów i rozsądnych oczekiwań osób, których dane dotyczą[188], a są wyrażone w ich prawach i wolnościach[189]. Administrator oraz podmiot przetwarzający wypełniają wymóg rzetelności, jeżeli przetwarzają dane osobowe zgodnie z zasadami współżycia

[184] D. Lubasz, M. Kwiatkowska-Cylke, *Zasady przetwarzania danych osobowych*, [w:] D. Lubasz (red.), *RODO w e-commerce*, Warszawa 2018, s. 51. Na szeroki zakres zastosowania tej zasady wskazują także P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5...*, s. 258.

[185] Jak słusznie zauważają P. Litwiński, P. Barta oraz M. Kawecki, aktualna jest teza wcześniej wyrażana w nauce prawa, że zasada legalności odnosi się do norm prawa materialnego oraz procesowego, wyrażonych w aktach ustawowych oraz aktach wykonawczych. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5...*, s. 258.

[186] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 51; M. Dominiak, M. Gawroński, *op. cit.*, s. 66–67.

[187] M. Dominiak, M. Gawroński, *op. cit.*, s. 67; P. Drobek, *Komentarz do art. 5...,* s. 326.

[188] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5...*, s. 258–259; M. Dominiak, M. Gawroński, *op. cit.*, s. 67.

[189] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 52.

społecznego oraz regułami uczciwości[190]. Rzetelność jest zachowana, gdy przetwarzanie danych odbywa się w zgodzie z powszechnie aprobowanymi normami społecznymi. Wymóg rzetelności obejmuje spełnienie norm prawnych oraz pozaprawnych[191].

Zasada ta stanowi podstawę sformułowania pozostałych zasad prawa ochrony danych[192] i bezpośrednich obowiązków podmiotów procesu przetwarzania. Wymóg zachowania rzetelności oznacza obowiązek administratora wyważenia swojego interesu z interesem osób, których dane dotyczą[193]. Przykładem jest obowiązek podania osobie, której dane dotyczą, informacji niezbędnych do rzetelnego przetwarzania, zarówno w przypadku, gdy dane te pozyska od tej osoby, jak i z innego źródła[194]. Administrator powinien też zapewnić aktualność przetwarzanych danych[195]. Uwzględnienie wymogu rzetelności ma także na celu zapewnienie bezpieczeństwa procesu przetwarzania danych osobowych[196].

4. Zasada *privacy by design*

Zasada *privacy by design* jest związana z prewencyjnym charakterem publicznoprawnych regulacji ochrony danych, które mają zapobiegać powstaniu naruszeń w ich przetwarzaniu. Umożliwia ona zapewnienie odpowied-

[190] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*..., s. 259.

[191] P. Drobek, *Komentarz do art. 5*..., s. 327. Odmienne stanowisko wyraża A. Krasuski, którego zdaniem zasada rzetelności odnosi się jedynie do stosowania przepisów prawa. Zob. A. Krasuski, *Ochrona danych osobowych* …, s. 189.

[192] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*..., s. 258. Podobnie uważają D. Lubasz, M. Kwiatkowska-Cylke, którzy podkreślają nadrzędność zasady rzetelności wobec pozostałych zasad ochrony danych. Zob. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 51. Zob. też. P. Drobek, *Komentarz do art. 5...,* s. 327.

[193] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 52; P. Drobek*, Komentarz do art. 5...,* s. 327.

[194] Artykuł 13 ust. 2 oraz art. 14 RODO.

[195] Zob. też A. Stępień, P. Biały, *Bezpieczeństwo danych osobowych zgodnie z RODO*, Wydawnictwo Wiedza i Praktyka, Warszawa 2017, s. 23.

[196] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 52.

niej ochrony danych osobowych przez cały proces ich przetwarzania[197]. Zasada ta ma charakter opisowy, lecz jest możliwa do określenia na podstawie interpretacji regulacji wyrażonej w art. 25 rozporządzenia 2016/679[198]. Powinna być stosowana zarówno w bezpośrednim związku z ochroną danych, jak i pośrednio, jak w przypadku zamówień publicznych, które powinny uwzględniać stosowanie tej zasady[199]. Ma ona na celu, aby administrator już na etapie projektowania procesu przetwarzania, określił i wdrożył środki techniczne i organizacyjne niezbędne do zapewnienia ochrony danych[200]. Dotyczy ona wprowadzania nowego projektu przetwarzania oraz zmiany już istniejącego procesu przetwarzania[201].

Wypełnienie zasady *privacy by design* obejmuje dwa rodzaje czynności, wzajemnie ze sobą związanych, które powinien podjąć administrator: analizę ryzyka oraz wdrożenie odpowiednich środków technicznych i organizacyjnych. Analiza ryzyka, która może obejmować m.in. ocenę skutków, ma na celu wybranie środków zabezpieczeń wobec planowanych operacji przetwarzania, które będą optymalne względem ryzyka naruszenia ochrony danych[202]. Analiza powinna dotyczyć indywidualnego projektu przetwarzania, z tej przyczyny wymagane środki techniczne i organizacyjne mogą być każdorazowo inne[203]. Środki te powinny umożliwić

[197] A. Stępień, P. Biały, *op. cit*., s. 19; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 25*, [w:] P. Litewski (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 455. Na prewencyjny i proaktywny charakter tej zasady wskazują także D. Lubasz, K. Witkowska-Nowakowska, *Komentarz do art. 25*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2018, s. 601.

[198] M. Susałko, *Ochrona danych w fazie projektowania i domyślna ochrona danych*, [w:] D. Lubasz (red.), *RODO w e-commerce*, Warszawa 2018, s. 162.

[199] W świetle motywu 78 *in fine* RODO zasada uwzględniania ochrony danych w fazie projektowania powinna być brana pod uwagę w przetargach publicznych.

[200] A. Stępień, P. Biały, *op. cit*., s. 18. Zob. też D. Lubasz, K. Witkowska-Nowakowska, *op. cit*., s. 604–605.

[201] M. Susałko, *op. cit*., s. 163, 164.

[202] Zob. A. Stępień, P. Biały, *op. cit*., s. 19.

[203] M. Susałko, *op. cit*., s. 164.

zmniejszenie lub eliminację wykrytego ryzyka[204]. Powinny uwzględniać stan wiedzy technicznej, koszt wdrażania a także charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania[205]. Środkami tymi mogą być pseudonimizacja[206], minimalizacja przetwarzania danych osobowych; zapewnienie przejrzystości obejmujące funkcję i przetwarzanie danych osobowych; integracja niezbędnych zabezpieczeń, umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych oraz umożliwienie administratorowi tworzenia i doskonalenia zabezpieczeń[207].

Administrator może wykazać spełnienie tego obowiązku za pomocą certyfikatu wydanego przez Prezesa Urzędu lub podmiot certyfikowany[208] lub wykazać poprzez przyjęcie wewnętrznej polityki ochrony danych oraz przyjęcie na ich podstawie odpowiednich środków technicznych i organizacyjnych[209].

5. Zasada *privacy by default*

Zasada *privacy by default* oznacza obowiązek domyślnej ochrony danych osobowych. Zasada ta, podobnie jak zasada *privacy by design*, ma opisowy charakter, jednakże można ją wyprowadzić na podstawie wykładni treści art. 25 rozporządzenia 2016/679. Zasada ta jest ściśle związana z możliwością przetwarzania wyłącznie danych osobowych, które są nie-

[204] Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 25...,* s. 458–459.

[205] Artykuł 25 ust. 1 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 25...*, s. 457–458.

[206] Artykuł 25 ust. 1 RODO; motyw 78 zd. 3 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 25...*, s. 458.

[207] Motyw 78 zd. 3 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 25...*, s. 458; D. Lubasz, K. Witkowska-Nowakowska, *op. cit.*, s. 600.

[208] Artykuł 25 ust. 3 RODO. Zob. A. Stępień, P. Biały, *op. cit.*, s. 19.

[209] Motyw 78 zd. 2 RODO.

zbędne dla osiągnięcia każdego konkretnego celu przetwarzania[210]. Domyślne przetwarzanie wprowadzane jest ze względu na ilość zbieranych danych osobowych, zakres ich przetwarzania, okres ich przechowywania oraz ich dostępności[211]. W tym celu administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne[212]. Środki te powinny w szczególności zapewnić, aby dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych[213], co oznacza, że osoba, której dane dotyczą, może w każdej chwili zrezygnować z domyślnej ochrony swojej prywatności[214]. Szczególne znaczenie ma ta zasada w przypadku przetwarzania za pomocą systemów teleinformatycznych umożliwiających bieżącą interakcję z osobą, której te dane dotyczą[215]. Użytkownicy tych systemów z zasady nie zmieniają ich ustawień, z tego powodu ochrona powinna mieć domyślny charakter[216]. Domyślna ochrona danych osobowych powinna być wprowadzona już na etapie projektowania procesu przetwarzania. Z tej przyczyny realizacja zasady *privacy be default* jest silnie związana z zasadą *privacy by design*[217]. Wymóg uwzględnienia zasady domyślnej ochrony jest także pośrednio stosowany w przypadku zamówień publicznych, jeżeli dotyczą one pośrednio ochrony danych osobowych[218], a także powinien być uwzględniony w wiążących regułach korporacyjnych[219].

[210] Artykuł 25 ust. 2 zd. 1 RODO.

[211] Artykuł 25 ust. 2 zd. 2 RODO. Zob. D. Lubasz, K. Witkowska-Nowakowska, *op. cit.*, s. 609.

[212] Artykuł 25 ust. 2 zd. 1 RODO. Zob. A. Stępień, P. Biały, *op. cit.*, s. 25.

[213] Artykuł 25 ust. 2 zd. 3 RODO.

[214] A. Stępień, P. Biały, *op. cit.*, s. 25.

[215] *Ibidem*, s. 25.

[216] M. Susałko, *op. cit.*, s. 168.

[217] *Ibidem*, s. 169.

[218] W świetle motywu 78 *in fine* RODO zasada uwzględniania ochrony danych w fazie projektowania powinna być brana pod uwagę w przetargach publicznych.

[219] Artykuł 47 ust. 1 lit. d RODO.

6. Zasada przejrzystości

Zasada przejrzystości ma dyrektywalny charakter. Jest wyrażona w art. 5 ust. 1 lit. a rozporządzenia 2016/679, w świetle którego dane osobowe muszą być przetwarzane w sposób przejrzysty dla osoby, której dane dotyczą. Oznacza ona, że administrator powinien podejmować swoje działania w sposób przejrzysty i klarowny[220]. Jednakże odnosi się głównie do sfery informowania lub udostępniania informacji osobom, których dane dotyczą. Dane osobowe powinny być bowiem przetwarzane w sposób przejrzysty dla tych osób[221]. Przejrzystość odnosi się do całego procesu przetwarzania, w tym zbierania, wykorzystywania oraz przeglądania[222]. Zasada przejrzystości zakłada także stosowanie dostępnej i zrozumiałej formy dla podmiotu informowanego[223]. Przepisy prawa pozostawiają administratorowi swobodę w wyborze formy informowania, która może mieć charakter pisemny lub elektroniczny, a na żądanie osoby, której dane dotyczą, administrator powinien przekazać te informacje ustnie[224]. Forma powinna uwzględniać czytelność, umiejscowienie, wielkość przekazu informacji, a forma elektroniczna powinna uwzględniać konieczność kliknięcia przeczytania tej informacji[225]. Informacja może mieć także częściowo charakter graficzny, który w sposób widoczny, zrozumiały i czytelny przedstawia sens przetwarzania, a jeżeli informacja jest przedstawiana za pomocą elektronicznych znaków graficznych, powinny one nadawać się

[220] A. Stępień, P. Biały, *op. cit*., s. 23. Jak słusznie wskazuje P. Drobek, przetwarzanie powinno odbywać się w sposób transparentny względem osób, których dane osobowe są przetwarzane. P. Drobek, *Komentarz do art. 5*..., s. 328.

[221] Artykuł 5 ust. 1 lit. a RODO. Zob. P. Drobek, *Komentarz do art. 5*..., s. 328.

[222] Motyw 39 zd. 2 RODO. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 52.

[223] W świetle motywu 39 zd. 3 RODO zasada przejrzystości oznacza, że wszelkie informacje i komunikaty związane z przetwarzaniem danych osobowych powinny być łatwo dostępne i zrozumiałe. Zob. też A. Stępień, P. Biały, *op. cit*., s. 23.

[224] Artykuł 12 ust. 1 zd. 2–3 RODO. Zob. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 54.

[225] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 54.

do odczytu maszynowego[226]. Znaki graficzne powinny być jednak ustandaryzowane w całej Unii Europejskiej[227].

Zasada przejrzystości jest wypełniana przez obowiązki informacyjne administratora oraz podmiotu przetwarzającego[228]. Administrator powinien podać osobie, której dane dotyczą, informacje niezbędne do zapewnienia przejrzystości przetwarzania, zarówno w przypadku, gdy dane te pozyska od tej osoby, jak i z innego źródła[229]. Informacje te powinny być dostępne dla osoby, której dane dotyczą, oraz zrozumiałe. Informacje są zrozumiałe, gdy są formułowane jasnym i prostym językiem[230]. Celem przekazania informacji powinno być umożliwienie ich zrozumienia osobie, której dane dotyczą, a nie jedynie późniejsze wykazanie spełnienia obowiązku prawnego przed Prezesem Urzędu lub sądem[231]. Administrator powinien w tym celu zastosować środki umożliwiające przekazanie tych informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, ze szczególnym uwzględnieniem specyfiki grup odbiorców, np. ich młodego wieku[232]. Jasny i prosty język oznacza sformułowania semantycznie proste i jednoznaczne, przy ograniczeniu do minimum pojęć technicznych[233]. Osoba, której dane dotyczą, powinna zostać poinformowana o tożsamości administratora, celach przetwarzania, a także o ryzyku, zasadach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobo-

[226] Motyw 60 zd. 5–6 RODO. Zob. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 54.

[227] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 54–55.

[228] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5...*, s. 259; A. Krasuski, *Ochrona danych osobowych…*, s. 189.

[229] Artykuł 13 ust. 2 oraz art. 14 RODO.

[230] Motyw 39 zd. 3 RODO.

[231] P. Drobek, *Komentarz do art. 5...*, s. 328.

[232] Artykuł 12 ust. 1zd. 1 RODO. Jak słusznie zauważają A. Stępień i P. Biały, przepisy prawa nakładają szczególny wymóg zapewnienia przejrzystości w toku procesu przetwarzania danych osobowych dzieci. Zob. A. Stępień, P. Biały, *op. cit*., s. 23. Zob. też. P. Drobek, *Komentarz do art. 5...*, s. 328–329.

[233] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 55.

wych oraz sposobach wykonywania praw przysługujących im w związku z takim przetwarzaniem[234].

7. Zasada minimalizacji danych osobowych

Zgodnie z zasadą minimalizacji danych osobowych administrator powinien przetwarzać jedynie dane osobowe, które są niezbędne dla realizacji celu przetwarzania[235]. Jest ona zatem ściśle związana z zasadą ograniczenia celu przetwarzania danych[236]. W świetle tej zasady dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Zasada minimalizacja danych ma charakter dyrektywny, wyrażona wprost w art. 5 ust. 1 lit. c rozporządzenia 2016/679, w świetle którego dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Zasada minimalizacji danych została wyrażona także w motywie 39 zd. 7 RODO, zgodnie z którym dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane[237]. Wprowadza ona ilościowe ograniczenie przetwarzanych danych[238]. Administrator powinien uwzględnić tę zasadę

[234] Motyw 39 zd. 4–5 RODO. Zob. też A. Stępień, P. Biały, *op. cit*., s. 23. Jak podkreślają D. Lubasz i M. Kwiatkowska-Cylke, zasada przejrzystości odnosi się do obowiązku zapewnienia celu, zakresu i kontekstu przetwarzania danych osobowych. Zob. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 52.

[235] Zasada minimalizacji danych osobowych jest bliska treściowo zasadzie adekwatności wyrażonej w art. 26 ust. 1 pkt 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 ze zm.), zgodnie z którym dane powinny były być adekwatne w stosunku do celów, w jakich są przetwarzane. Problematykę zasady adekwatności analizuje A. Kamińska-Pietnoczko, *Dane osobowe w zatrudnieniu*, „Monitor Prawa Pracy" 2015, Nr 1, s. 13. Zob. też J. Łuczak, *Ochrona danych osobowych jako element zarządzania bezpieczeństwem informacji*, „Studia Oeconomica Posnaniensia" 2016, Vol. 4, No. 12, s. 63.

[236] M. Dominiak, M. Gawroński, *op. cit*., s. 70.

[237] Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*..., s. 263.

[238] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 60.

już w etapie projektowania systemu ochrony danych[239]. Minimalizacja danych jest szczególnym zabezpieczeniem w przypadku przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych[240]. Zastosowanie minimalizacji danych wymagane jest m.in. w wiążących regułach korporacyjnych[241].

Zasada minimalizacji odnosi się zarówno do gromadzenia, przetwarzania, jak i archiwizowania danych osobowych. Administrator nie powinien pozyskiwać danych osobowych, które są zbędne z uwagi na cel ich przetwarzania[242]. Nie jest dopuszczalne gromadzenie ich „na zapas"[243]. Powinien on także, w toku procesu przetwarzania, udostępniać te dane jedynie podmiotom, których działania są konieczne dla celu przetwarzania. Zakres dostępnych danych dla takiego podmiotu powinien być określony np. w udzielonym mu upoważnieniu[244]. Jednocześnie administrator ma obowiązek usunąć te dane, jeżeli cel ich przetwarzania został osiągnięty[245].

Wymóg minimalizacji danych ma charakter względny. Przepisy szczególne nakładają częściowo m.in. obowiązek archiwizacji danych[246]. Przepisy te określają katalog danych, które podlegają przetwarzaniu. Wyłączają indywidulane określenie zakresu niezbędnych danych do przetwarzania, ponieważ wprowadzają taki katalog normą o charakterze generalnym i abstrakcyjnym, a więc skierowaną do niezidentyfikowanych adresatów, którzy znajdują się w określonym typie sytuacji. W świetle roz-

[239] Artykuł 25 ust. 1 RODO; motyw 78 zd. 3 w zw. z motywem 78 zd. 2 RODO. Zob. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 60. Jak słusznie podkreślają M. Dominiak oraz M. Gawroński, administrator powinien uwzględnić wymóg minimalizacji danych osobowych najpóźniej w chwili gromadzenia tych danych. M. Dominiak, M. Gawroński, *op. cit.*, s. 70.

[240] Artykuł 89 ust. 1 zd. 1–2 RODO; motyw 156 zd. 2 w zw. z motywem 156 zd. 1 RODO.

[241] Artykuł 47 ust. 2 lit. d RODO.

[242] A. Stępień, P. Biały, *op. cit.*, s. 24; M. Dominiak, M. Gawroński, *op. cit.*, s. 70–71; A. Krasuski, *Ochrona danych osobowych…*, s. 193.

[243] A. Stępień, P. Biały, *op. cit.*, s. 24; D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 60.

[244] A. Stępień, P. Biały, *op. cit.*, s. 24.

[245] *Ibidem*.

[246] *Ibidem*.

porządzenia 2016/679 katalogi danych podlegających przetwarzaniu na podstawie norm ustawowych są dopuszczalne, jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej[247].

8. Zasada prawidłowości

W świetle zasady prawidłowości przetwarzane dane osobowe powinny być prawidłowe oraz aktualne w świetle celów ich przetwarzania[248]. Zasada ta ma charakter dyrektywalny, została wprost wyrażona w art. 5 ust. 1 lit. d rozporządzenia 2016/679, w myśl którego dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Zgodnie z tym przepisem należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Dane nieprawidłowe powinny zostać zatem usunięte lub sprostowane przez administratora z jego inicjatywy lub na żądanie osoby, której dane dotyczą[249].

Administrator ma obowiązek wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę czynników powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów[250], w tym weryfikację źródeł gromadzenia tych danych[251], przegląd zbioru danych[252] oraz ich aktualizację[253]. Powinien również pod-

[247] Motyw 45 zd. 1 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*..., s. 263–264.

[248] Artykuł 5 ust. 1 lit. d RODO. Zob. A. Stępień, P. Biały, *op. cit*., s. 24; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*..., s. 264; D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 59; M. Dominiak, M. Gawroński, *op. cit*., s. 72; A. Krasuski, *Ochrona danych osobowych…*, s. 195.

[249] Artykuł 5 ust. 1 lit. d RODO. A. Stępień, P. Biały, *op. cit*., s. 24.

[250] Motyw 71 zd. 6 RODO.

[251] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*..., s. 264–265.

[252] M. Dominiak, M. Gawroński, *op. cit*., s. 72; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*..., s. 265.

[253] M. Dominiak, M. Gawroński, *op. cit*., s. 72.

jąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe[254].

Osoba, której dane dotyczą, ma prawo żądać od administratora ograniczenia przetwarzania, gdy kwestionuje prawidłowość danych osobowych, na okres pozwalający administratorowi sprawdzić ich prawidłowość[255]. Osoba ta może także żądać sprostowania dotyczących jej danych osobowych, które są nieprawidłowe[256]. Administrator powinien po sprawdzeniu danych osobowych przekazać informacje tej osobie, czy i w jakim zakresie dane zostały sprostowane lub usunięte[257].

9. Zasada integralności i poufności

Zasada integralności i poufności ma dyrektywalny charakter. Jej podstawą jest art. 5 ust. 1 lit. f rozporządzenia 2016/679, w świetle którego dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych[258]. Poufność informacji oznacza zachowanie ich w tajemnicy, z wyłączeniem uprawnionych podmiotów, a integralność, że dane są spójnie i niezmienione w sposób nieuprawnio-

[254] Motyw 39 zd. 11 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5...*, s. 266.

[255] Artykuł 18 ust. 1 lit. a RODO.

[256] Artykuł 16 ust. 1 RODO.

[257] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 59.

[258] Zasada integralności i poufności oznacza nałożenie obowiązku stosowania odpowiednich środków technicznych i organizacyjnych, które zapewniają bezpieczeństwo danych osobowych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (art. 5 ust. 1 lit. f RODO). Zob. A. Stępień, P. Biały, *op. cit.*, s. 21; D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 63; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5...*, s. 267; A. Krasuski, *Ochrona danych osobowych...*, s. 196. Środki te mają na celu zapewnić także bezpieczeństwo przed nieuprawnionym do nich dostępem (motyw 39 *in fine* RODO). Zob. A. Stępień, P. Biały, *op. cit.*, s. 21.

ny[259]. Wypełnienie tej zasady jest zatem ściśle związane z zabezpieczeniem danych osobowych[260], zarówno przetwarzanych drogą analogową, jak i elektroniczną[261].

Zapewnienie poufności jest wyrażone m.in. w wypełnieniu obowiązku zachowania tajemnicy. Przepisy prawa nakładają na podmioty uczestniczące w procesie przetwarzania, w tym na inspektora ochrony danych oraz członków i personel Prezesa Urzędu, obowiązek zachowania tajemnicy oraz poufności związanej z wykonywaniem ich zadań[262]. Jeżeli tajemnica ma charakter zawodowy, wówczas odnosi się także względem osoby, której dane dotyczą, a wówczas wyłącza ona obowiązek podania jej informacji o pozyskaniu jej danych osobowych z innego źródła[263].

Administrator lub podmiot przetwarzający powinien wdrożyć odpowiednie środki techniczne i organizacyjne posiadające zdolność do ciągłego zapewnienia poufności i integralności systemów i usług przetwarzania[264]. Środki te mają na celu zapewnić bezpieczeństwo przetwarzania

[259] A. Stępień, P. Biały, *op. cit*., s. 20; P. Drobek, *Komentarz do art. 5*..., s. 340; M. Dominiak, M. Gawroński, *op. cit*., s. 77.

[260] A. Stępień, P. Biały, *op. cit*., s. 20; M. Dominiak, M. Gawroński, *op. cit*., s. 76.

[261] Rozporządzenie 2016/679 w motywie 49 wskazuje zakres niezbędnych zabezpieczeń w przypadku elektronicznego przetwarzania danych. Jak słusznie zauważył A. Krasuski, zapewnienie bezpieczeństwa przetwarzania nie ogranicza się jedynie do zabezpieczeń, lecz powinno być pojmowane znacznie szerzej, a odpowiadać realnym zagrożeniom związanym z ryzykiem naruszenia ochrony danych osobowych. Zob. A. Krasuski, *Ochrona danych osobowych*..., s. 196–197.

Należy podkreślić, że wymogi dotyczące zapewnienia bezpieczeństwa, w tym dotyczące elektronicznego przetwarzania, są określone w przepisach szczególnych. Zob. M. Błażewski, *Zasada zapewnienia bezpieczeństwa w e-administracji*, „Folia Iuridica Universitatis Wratislaviensis" 2017, vol. 6 (1), s. 111–115; M. Błażewski, *Płaszczyzny administracji elektronicznej*, Acta Universitatis Wratislaviensis, Prawo 2017, Nr 323, s. 19; M. Błażewski, *Wartości w e-administracji i ich wyważenie*, [w:] J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I*, Wolters Kluwer, Warszawa 2017, s. 204–205.

[262] Zgodnie z art. 38 ust. 5 RODO inspektor ochrony danych jest obowiązany zachować tajemnicę i poufność w związku z wykonywaniem swoich zadań. W świetle art. 54 ust. 2 RODO członek oraz personel Prezesa Urzędu podlegają obowiązkowi zachowania tajemnicy służbowej odnoszącej się do poufnych informacji, które uzyskał podczas wykonywania zadań lub swoich uprawnień.

[263] Artykuł 14 ust. 5 lit. d RODO.

[264] Artykuł 32 ust. 1 lit. b RODO. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 63.

danych osobowych[265]. Wybór środków może być dokonany na podstawie oceny skutków przetwarzania danych osobowych, które pozwalają określić ryzyko ich naruszenia, a także stałą kontrolę zagrożeń[266]. Środkami tymi są m.in.: pseudonimizacja i szyfrowanie danych osobowych; zapewnienie systemom i usługom przetwarzania ciągłej poufności, integralności, dostępności i odporności; zapewnienie zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania[267].

10. Zasada ograniczenia celu przetwarzania danych

Zasada ograniczenia celu obejmuje dwa podstawowe obowiązki: prawidłowe określenie celu przetwarzania danych osobowych oraz wykorzystanie tych danych zgodnie z tymi celami lub celami powiązanymi[268]. Zasada ta ma dyrektywalny charakter. Jest wyrażona w art. 5 ust. 1 lit. b rozporządzenia 2016/679, w świetle którego dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami, lecz dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań nauko-

[265] A. Stępień, P. Biały, *op. cit.*, s. 21.

[266] *Ibidem*; D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 64; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 32*, [w:] P. Litewski (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 503.

[267] Art. 32 ust. 1 lit. a–d RODO. Jak słusznie podkreślają D. Lubasz oraz M. Kwiatkowska-Cylke, katalog ten ma charakter przykładowy. Zob. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 63. Zgodnie z motywem 83 zd. 1–2 RODO szyfrowanie stanowi środek minimalizujący ryzyko przetwarzania niezgodnego z prawem, poprzez zapewnienie odpowiedniego poziomu poufności.

[268] D. Lubasz oraz M. Kwiatkowska-Cylke podkreślają, że zasada ograniczenia celu odnosi się do prawidłowego określenia celu oraz przetwarzania danych jedynie zgodnie z tym celem. Zob. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 56–57. Podobnie P. Drobek, *Komentarz do art. 5...*, s. 330.

wych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami.

Zasada ograniczenia celu odnosi się zatem do całego procesu przetwarzania, zarówno do jego początkowego etapu, gdy określany jest jego cel, jak i do kolejnych jego etapów, gdy dane są już przetwarzane. Zgodnie z zasadą ograniczenia celu, przetwarzanie danych osobowych powinno odbywać się z zasady w celu pierwotnym, na który wyraziła wcześniej zgodę osoba, której dane dotyczą, lub który jest realizowany na innej podstawie prawnej[269], a także w celu związanym z celem pierwotnym[270].

Nowy cel powinien być zatem zgodny z celem pierwotnym[271]. Zasada ta nie oznacza zakazu przetwarzania danych w innym celu niż pierwotny[272]. Na takie rozumienie tej zasady wskazuje także prawo administratora do dalszego przetwarzania pomimo realizacji pierwotnego celu, jeżeli dalsze przetwarzanie odbywa się w celach archiwalnych w interesie publicznym, celach badań naukowych, historycznych lub statystycznych[273]. Zmiana celu przetwarzania wymaga odrębnej podstawy prawnej względem pierwotnego celu. Podstawą mogą być przepisy szczególne, zarówno prawa Unii Europejskiej, jak i prawa polskiego, jeżeli regulują one wykonanie zadania publicznego[274]. Administrator powinien poinformować osobę, której dane dotyczą, o zamiarze przetwarzania w celu innym niż w celu pierwotnym[275].

[269] Artykuł 5 ust. 1 lit. b RODO. Zob. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 58.

[270] Motyw 50 zd. 1 RODO.

[271] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5...*, s. 261.

[272] *Ibidem*. Zob. też M. Dominiak, M. Gawroński, *op. cit.*, s. 69.

[273] Artykuł 5 ust. 1 lit. b *in fine* RODO. Zob. A. Stępień, P. Biały, *op. cit.*, s. 23. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit.*, s. 59.

[274] Motyw 50 zd. 2–3 RODO. Zob. A. Stępień, P. Biały, *op. cit.*, s. 23.

[275] Motyw 61 zd. 3 RODO.

11. Zasada ograniczenia przechowywania

Zasada ograniczenia przechowywania odnosi się do czasu przechowywania danych osobowych, który powinien być ograniczony do okresu niezbędnego dla realizacji celów, dla których dane te są przetwarzane[276]. Jest to zasada dyrektywalna, wyrażona w art. 5 ust. 1 lit. e rozporządzenia 2016/679, w świetle którego dane osobowe muszą 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, jednakże dane osobowe można przechowywać przez okres dłuższy, jeżeli będą przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą.

Nie jest zatem możliwe ich przechowywanie w nieskończoność[277]. Administrator powinien określić termin usunięcia tych danych, aby zapobiec ich przechowywaniu przez okres dłuższy niż jest niezbędne[278]. Czas przechowywania powinien być uwarunkowany jego celem[279]. Na określenie czasu mogą mieć wpływ przepisy prawa regulujące stosunek prawny pomiędzy administratorem a osobą, której dane dotyczą[280]. Zasada ta ma względny charakter, ponieważ dane te można przechowywać pomi-

[276] Artykuł 5 ust. 1 lit. e RODO. D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 61; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*..., s. 266.

[277] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*..., s. 266; P. Drobek, *Komentarz do art. 5*..., s. 340.

[278] Motyw 39 zd. 10 RODO. Zob. A. Stępień, P. Biały, *op. cit*., s. 25. Jak słusznie podkreślają M. Dominiak i M. Gawroński, administrator powinien nie tylko określić czas przetwarzania, ale także poinformować o tym osobę, której dane dotyczą. Zob. M. Dominiak, M. Gawroński, *op. cit*., s. 73; P. Drobek, *Komentarz do art. 5*..., s. 339; A. Krasuski, *Ochrona danych osobowych*..., s. 196.

[279] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 61; M. Dominiak, M. Gawroński, *op. cit*., s. 73.

[280] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 61–62.

mo upływu tego okresu, jeżeli będą przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub statystycznych. Warunkiem jest zastosowanie odpowiednich środków technicznych i organizacyjnych w celu ochrony praw i wolności osób, których dane dotyczą[281]. Administrator może także przechowywać te dane w innych celach, pod warunkiem że przestaną one umożliwiać identyfikację osoby, której dane dotyczą. Środkiem służącym uniemożliwieniu tej identyfikacji jest anonimizacja[282].

12. Zasada rozliczalności

Zasada rozliczalności ma dyrektywalny charakter, jest wyrażona art. 5 ust. 2 rozporządzenia 2016/679, zgodnie z którym administrator jest odpowiedzialny za przestrzeganie wymogów związanych z pozostałymi zasadami ochrony danych osobowych i musi być w stanie wykazać ich przestrzeganie. Zasada rozliczalności odnosi się do podjęcia przez administratora odpowiedzialności za zapewnienie ochrony danych, a także do jego obowiązku wykazania, że przestrzega on pozostałych zasad ochrony danych w toku procesu przetwarzania[283]. Należy zatem zasadę tę odnieść do pozostałych zasad wyrażonych w rozporządzeniu 2016/679[284].

Zasada rozliczalności jest skutkiem pozostawienia administratorowi swobody w wyborze tych środków. Z tą swobodą jest ściśle związa-

[281] Artykuł 5 ust. 1 lit. e RODO. Zob. A. Stępień, P. Biały, *op. cit*., s. 25; D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 62; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5...*, s. 267.

[282] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5...*, s. 266.

[283] W świetle zasady rzetelności wyrażonej art. 5 ust. 2 RODO administrator powinien być w stanie wykazać przestrzeganie pozostałych zasad prawa ochrony danych. Jak słusznie podkreśla P. Drobek, zasada rozliczalności obejmuje podjęcie odpowiednich środków służących zapewnieniu ochrony danych osobowych oraz późniejszą możliwość wykazania tych działań. Zob. P. Drobek*, Komentarz do art. 5...*, s. 342–343.

[284] A. Stępień, P. Biały, *op. cit*., s. 22; D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 64. Zdaniem P. Drobka zasada rozliczalności ma zapewnić większą skuteczność pozostałych zasad ochrony danych. P. Drobek, *Komentarz do art. 5...*, s. 343.

na odpowiedzialność administratora za zapewnienie ochrony danych[285]. Powinien wdrożyć środki, które umożliwią mu wypełnienie obowiązku ochrony danych w świetle rozporządzenia 2016/679 oraz wykazanie, że tym samym zapewnia odpowiednią ochronę[286]. W tym celu administrator powinien weryfikować i aktualizować stosowane środki[287].

Administrator danych powinien móc także wykazać względem Prezesa Urzędu oraz osoby, której te dane dotyczą, że wypełnia przepisy ochrony danych zarówno planując, jak i wykonując pozostałe czynności przetwarzania[288]. Administrator może wykonać ten obowiązek, gdy wdroży odpowiedni system ochrony danych, obejmujący środki techniczne i organizacyjne[289]. Administrator wykazuje przestrzeganie przepisów o ochronie danych osobowych za pomocą dokumentacji opisującej przyjęte środki, a także wypełnienie innych obowiązków związanych z procesem przetwarzania, w tym odpowiedniego wyboru podmiotu przetwarzającego, prawidłowego pozyskiwania zgody na przetwarzanie, wypełnienia obowiązku informacyjnego, wykonania oceny skutków ochrony danych, terminowego rozpatrywania wniosków osób, których dane dotyczą[290].

[285] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 5*..., s. 268; M. Dominiak, M. Gawroński, *op. cit*., s. 80; P. Drobek*, Komentarz do art. 5*..., s. 342.

[286] W świetle art. 24 ust. 1 RODO administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem 2016/679 i aby móc to wykazać. Zob. P. Drobek*, Komentarz do art. 5*..., s. 343–344.

[287] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 65.

[288] A. Stępień, P. Biały, *op. cit*., s. 22; D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 64.

[289] D. Lubasz, M. Kwiatkowska-Cylke, *op. cit*., s. 64.

[290] *Ibidem*, s. 65–66.

Rozdział IV

Podmioty procesu przetwarzania

(Maciej Błażewski)

1. Wyodrębnienie grup podmiotów procesu przetwarzania

Proces przetwarzania danych osobowych obejmuje relacje pomiędzy jego podmiotami, reprezentującymi różne interesy, wobec których przepisy prawa określają odmienne uprawnienia, obowiązki lub zadania. Należy wyróżnić trzy grupy podmiotów, ze względu na podstawowy interes, który reprezentują w toku procesu przetwarzania.

W pierwszej grupie mieści się jedynie osoba, której dane są przetwarzane. Osoba ta reprezentuje wyłącznie swój interes jednostkowy, wyrażony w przepisach prawa.

Druga grupa obejmuje administratora, podmiot przetwarzający oraz inspektora ochrony danych. Grupa ta nie jest jednorodna. Podstawowym interesem, który reprezentują podmiot przetwarzający oraz inspektor ochrony danych, jest interes publiczny. Prawodawca nałożył na te podmioty, ze względu na ich szczególną wiedzę i kwalifikacje, wiele obowiązków o charakterze publicznoprawnym w celu zapewnienia prawidłowego przebiegu procesu przetwarzania. Jednakże podmiot przetwarzający oraz inspektor ochrony danych są powołani przez administratora, aby umożliwić mu wykonanie czynności przetwarzania. Z tej przyczyny pod-

mioty te wraz z samym administratorem reprezentują także interes jednostkowy administratora.

Do trzeciej grupy należą Prezes Urzędu Ochrony Danych Osobowych, mający status organu nadzorczego według rozporządzenia 2016/679, oraz podmiot certyfikujący. Działania tych podmiotów w toku procesu projektowania nakierowane są na wykonanie interesu publicznego. Ich podstawowym celem jest zapobiegnięcie naruszeniom ochrony danych osobowych.

Regulacje odnoszące się do podmiotów oraz relacji pomiędzy nimi stanowią kontynuacje przepisów poprzednich, wyrażonych w dyrektywie 95/46/WE. W świetle postanowień tej dyrektywy podmiotami tymi były osoba, której dane dotyczą, administrator danych, przetwarzający oraz organ nadzorczy[291].

Analiza każdego z tych podmiotów pozwoli określić ich miejsce oraz znaczenie w procesie przetwarzania. Z tej przyczyny wyjaśnienie ich statusu konieczne jest w początkowej części tego opracowania.

2. Osoba, której dane dotyczą

Osoba, której dane dotyczą, jest podmiotem, jej dane osobowe podlegają ochronie na podstawie rozporządzenia 2016/679 oraz ustawy o ochronie danych osobowych. Jest osobą fizyczną, której dane są przetwarzane bez względu na obywatelstwo oraz miejsce zamieszkania[292]. W świetle przepisów Kodeksu cywilnego osobę fizyczną można rozumieć jako każdego człowieka od chwili urodzenia[293]. Podmiot ten posiada status osoby, której dane dotyczą, bez względu na swój wiek lub zakres zdolności do czynności prawnych. Przepisy rozporządzenia 2016/679 mają bowiem

[291] Artykuł 2 lit. d–f oraz art. 28 dyrektywy 95/46/WE.

[292] Motyw 14 zd. 1 RODO.

[293] Artykuł 8 § 1 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2018 r., poz. 1025 ze zm.), dalej KC.

na celu ochronę prywatności każdej osoby fizycznej. Ochrona obejmuje środki pośrednie, niewymagające udziału w ich stosowaniu osoby, której dane dotyczą, oraz środki bezpośrednie, które osoba może zastosować za pośrednictwem innego podmiotu reprezentującego jej interesy. Rozporządzenie 2016/679 wyraźnie wskazuje, że osobą, której dane dotyczą, nie jest osoba zmarła, ponieważ dane takiej osoby nie podlegają ochronie[294]. W świetle tego rozporządzenia osoba taka powinna być zidentyfikowana lub możliwa do zidentyfikowania na podstawie zebranych danych osobowych[295].

3. Administrator danych

Administratorem danych jest podmiot samodzielnie określający cel oraz sposób przetwarzania danych osobowych[296], który ma faktyczny wpływ na proces przetwarzania[297]. Jeżeli cele i sposoby przetwarzania określa dwa lub więcej podmiotów, posiadają one status współadministratorów[298]. Przepisy prawa nie wymagają od tego podmiotu szczególnej formy lub statusu. Może nim być osoba fizyczna lub osoba prawna, w tym osoba

[294] Motyw 27 RODO.

[295] Artykuł 4 pkt 1 RODO; motyw 26 zd. 1 RODO.

[296] Artykuł 4 pkt 7 RODO. Zob. M. Gawroński, K. Kloc, M. Wojtas, *Administrator i podmiot przetwarzający*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018, s. 117; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4…*, s. 219–220. Nauka prawa na gruncie dawnych przepisów o ochronie danych, wyrażonych w u.o.d.o.97, wyróżniała administratora danych osobowych, decydującego o celach i środkach przetwarzania danych, oraz administrującego danymi osobowymi, który realnie zarządza procesem przetwarzania. B. Konieczna-Drzewiecka, A. Zubrycka, *Tajemnica upoważnionego do przetwarzania danych osobowych*, „Monitor Prawniczy" 2015, Nr 21, s. 1174.

[297] A. Krasuski, *Podstawy prawne przetwarzania danych objętych tajemnicą telekomunikacyjną*, „Przegląd Ustawodawstwa Gospodarczego" 2016, Nr 8, s. 3–4.

[298] Artykuł 26 ust. 1 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 26*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 462; K. Witkowska-Nowakowska*, Komentarz do art. 26*, [w:] E. Bielak-Jomaa, D. Lubasz (red*.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 613.

prawna będąca podmiotem publicznym[299]. Status administratora może być także określony przez przepisy prawa Unii Europejskiej lub prawa państwa członkowskiego wprost lub poprzez określenie kryteriów jego wyznaczenia, jeżeli przepisy te określają cele i sposoby przetwarzania tych danych osobowych[300].

Administrator danych, jak również współadministrator, został obowiązany do zapewnienia przestrzegania przepisów prawa dotyczących przetwarzania danych osobowych[301]. Wykonanie tego obowiązku obejmuje zastosowanie odpowiednich środków organizacyjno-technicznych służących realizacji tych przepisów. Środki te powinny być poddawane przez niego przeglądom i aktualizacji, tak aby ochrona danych była skuteczna[302]. Administrator samodzielnie określa, jakie środki powinny być stosowane przy zapewnieniu ochrony danych osobowych. Ponosi on jednak odpowiedzialność za przestrzeganie regulacji dotyczących ochrony danych[303]. Szczególne zasady odpowiedzialności dotyczą także współadministratorów. Są one określne przez nich samych, chyba że przepisy pra-

[299] W świetle art. 4 pkt 7 RODO administratorem danych może być osoba fizyczna, osoba prawna, organ publiczny, jednostka lub inny podmiot. Zob. M. Gawroński, K. Kloc, M. Wojtas, *op. cit*., s. 116–117; K. Witkowska-Nowakowska, *Komentarz do art. 4*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 211; A. Krasuski, *Ochrona danych osobowych…*, s. 134. Podobne wnioski były wywodzone na podstawie starego stanu prawnego wyrażonego w u.o.d.o.97. Zob. M. Czelny, *Ochrona danych osobowych w działalności Kościoła Katolickiego w Polsce*, „Studia z Prawa Wyznaniowego" 2011, T. 14, s. 242. Administrator jest najważniejszym podmiotem procesu przetwarzania. Należy wskazać konkretny podmiot, który posiada status administratora, ze względu na jego obowiązki w procesie przetwarzania. M. Tarnawa-Zajączkowska, *Zmiana ustawy o ochronie danych osobowych. Administrator danych osobowych jako podmiot zbiorowy*, „Casus" 2016, Nr 2, s. 46, 48.

[300] Art. 4 pkt 7 RODO. Zob. K. Witkowska-Nowakowska, *Komentarz do art. 4.*.., s. 211; A. Krasuski, *Ochrona danych osobowych…*, s. 134–135.

[301] W myśl art. 5 ust. 2 w zw. z art. 5 ust. 1 RODO administrator jest odpowiedzialny za przestrzeganie przepisów dotyczących ochrony danych osobowych. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4.*.., s. 225.

[302] Art. 24 ust. 1 RODO. Zob. M. Gawroński, K. Kloc, M. Wojtas, *op. cit*., s. 119.

[303] Artykuł 5 ust. 2 w zw. z art. 5 ust. 1 RODO. Zob. M. Gawroński, K. Kloc, M. Wojtas, *op. cit*., s. 118–119; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4.*.., s. 219–220.

wa w sposób szczególny je określają. Uzgodnienia współadministratorów powinny obejmować przejrzyste zasady podziału tej odpowiedzialności[304], a także w sposób należyty odzwierciedlać zakresy ich obowiązków oraz relacje pomiędzy nimi a osobami, których dane dotyczą[305]. Uzgodnienia te mają względny charakter wobec tych osób, ponieważ mogą one wykonywać przysługujące im prawa związane z ochroną ich danych, samodzielnie wobec każdego z administratorów[306].

4. Podmiot przetwarzający

Podmiotem przetwarzającym jest podmiot, niezależny od swojej formy prawnej lub statusu, który prowadzi przetwarzanie danych osobowych w imieniu i na polecenie administratora na podstawie umowy lub innego instrumentu prawnego[307]. Podmiot ten powinien realizować wyłącznie cele wskazane przez administratora[308].

Administrator powinien wybrać podmiot przetwarzający, który zapewnia gwarancję ochrony danych osobowych, mając wiedzę fachową oraz wiarygodność. Podmiot przetwarzający powinien mieć także zasoby umożliwiające wdrożenie odpowiednich środków technicznych i organizacyjnych i tym samym pozwalające spełnić w toku przetwarzania wymogi rozporządzenia 2016/679 oraz zapewnić ochronę praw osób, których dane dotyczą[309]. Podmiot przetwarzający może wykazać zastosowanie tych

[304] Artykuł 26 ust. 1 zd. 2 RODO. Zob. K. Witkowska-Nowakowska, *Komentarz do art. 26*..., s. 620.

[305] Artykuł 26 ust. 2 zd. 1 RODO. Należy także zauważyć, że w świetle art. 26 ust. 2 zd. 2 RODO uzgodnienia powinny być udostępniane podmiotom, których dane dotyczą.

[306] Artykuł 26 ust. 3 RODO.

[307] Artykuł 28 ust. 1 w zw. z art. 28 ust. 3 zd. 1 RODO; art. 29 RODO; art. 4 pkt 8 RODO. Zob. M. Gawroński, K. Kloc, M. Wojtas, *op. cit.*, s. 121; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4.*.., s. 226.

[308] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4.*.., s. 226.

[309] Artykuł 28 ust. 1 RODO, motyw 81 zd. 1 RODO. Zob. M. Gawroński, K. Kloc, M. Wojtas, *op. cit.*, s. 122.

gwarancji m.in. poprzez wdrożenie zatwierdzonego kodeksu postępowania lub certyfikatu, które stanowią pośredni środek ochrony danych[310].

Umowa lub inny instrument prawny stanowiący podstawę stosunku prawnego pomiędzy administratorem, a podmiotem przetwarzającym określa przedmiot, czas, charakter i cele przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa administratora, jak również zadania i obowiązki podmiotu przetwarzającego z uwzględnieniem kontekstu przetwarzania i ryzyka naruszenia praw lub wolności osoby, której dane dotyczą[311]. Umowa ta może być przygotowana indywidualnie lub z zastosowaniem standardowych klauzul umownych[312]. Umowa lub inny instrument prawny może mieć formę pisemną lub elektroniczną[313].

Przepisy prawa uszczegółowiają elementy umowy lub innego instrumentu prawnego poprzez wskazanie obligatoryjnych obowiązków podmiotu przetwarzającego[314]. Obowiązkami tymi są: wykonywanie czynności przetwarzania jedynie na udokumentowane polecenie administratora; zapewnienie zachowania tajemnicy w toku przetwarzania[315]; wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających odpowiedni stopień bezpieczeństwa wobec ryzyka naruszenia praw i wolności osób fizycznych[316]; zapewnienie przestrzegania warunków korzysta-

[310] Artykuł 28 ust. 5 w zw. z art. 28 ust. 1 RODO.

[311] Artykuł 28 ust. 3 zd. 1 RODO; motyw 81 zd. 3 RODO. Szerzej problematykę umowy z podmiotem przetwarzającym przedstawiają: M. Gawroński, K. Kloc, M. Wojtas, *op. cit*., s. 122–125.

[312] W świetle motywu 81 zd. 4 RODO umowa pomiędzy administratorem a podmiotem przetwarzającym może opierać się na standardowych klauzulach umownych, jeżeli zostały one przyjęte bezpośrednio przez Komisję Europejską lub zostały przyjęte przez Prezesa Urzędu zgodnie z mechanizmem spójności, a następnie zostały przyjęte przez Komisję Europejską. Zgodnie z art. 28 ust. 6 w zw. z art. 28 ust. 7 oraz art. 28 ust. 8 RODO umowa lub inny instrument prawny mogą opierać się, w całości lub częściowo, na standardowych klauzulach umownych określonych przez Prezesa Urzędu lub Komisję Europejską.

[313] Artykuł 28 ust. 9 w zw. z art. 28 ust. 3–4 RODO.

[314] M. Gawroński, K. Kloc, M. Wojtas, *op. cit*., s. 121, 125–126.

[315] Artykuł 28 ust. 3 lit. a–b RODO.

[316] Artykuł 28 ust. 3 lit. c w zw. z art. 32 ust. 1 RODO.

nia z usług innego podmiotu przetwarzającego[317]; pomoc administratorowi w wypełnieniu jego obowiązku odpowiedzi na żądania osoby, której dane dotyczą, w zakresie realizacji jej praw poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych[318]; pomoc administratorowi w zgłoszeniu naruszenia ochrony danych osobowych Prezesowi Urzędu, zawiadomieniu osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, przygotowania oceny skutków ochrony danych, w podejmowaniu czynności związanych z uprzednią konsultacją[319]; udostępnienie administratorowi wszelkich informacji niezbędnych do wykazania spełnienia swoich obowiązków oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich[320].

Podmiot przetwarzający po zakończeniu świadczenia usługi przetwarzania jest także obowiązany do usunięcia lub zwrócenia administratorowi, w zależności od jego decyzji, wszelkich danych osobowych oraz usunięcia ich kopii, chyba że przepisy prawa stanowią inaczej[321].

Podmiot przetwarzający może korzystać z usług innego podmiotu przetwarzającego w celu wykonania swoich obowiązków, jeżeli uzyska zgodę administratora. Zgoda powinna być wyrażona w formie pisemnej i mieć charakter szczegółowy lub ogólny[322]. W przypadku wyrażenia zgody ogólnej administrator ma możliwość monitorowania działań podmiotu przetwarzającego. Administrator powinien mieć możliwość wyrażenia sprzeciwu wobec zmian dotyczących dokonania lub zastąpienia innych podmiotów przetwarzających, by tym samym móc wpłynąć na skład podmiotowy osób uczestniczących w procesie przetwarzania[323].

[317] Artykuł 28 ust. 3 lit. d RODO.
[318] Artykuł 28 ust. 3 lit. e RODO.
[319] Artykuł 28 ust. 3 lit. f w zw. z art. 32–36 RODO; motyw 95 RODO.
[320] Artykuł 28 ust. 3 lit. h RODO.
[321] Artykuł 28 ust. 3 lit. g RODO.
[322] Artykuł 28 ust. 2 zd. 1 RODO.
[323] Artykuł 28 ust. 2 zd. 2 RODO.

Także inny podmiot działający z upoważnienia podmiotu przetwarzającego, jest uprawniony do przetwarzania danych osobowych wyłącznie na polecenie administratora lub na podstawie przepisów prawa[324].

5. Inspektor ochrony danych

Inspektora ochrony danych wyznacza administrator danych lub podmiot przetwarzający[325]. Inspektor ten jest z zasady wyznaczony fakultatywnie, a jedynie w szczególnych przypadkach ma obligatoryjny charakter[326].

Podmioty te mogą wyznaczyć inspektora ochrona danych bez względu zakres i rodzaj swojej struktury organizacyjnej, a także przetwarzania ochrony danych.

Administrator danych lub podmiot przetwarzający mają obowiązek wyznaczenia inspektora ochrony danych, gdy będzie zachodzić choć jedna z poniższych sytuacji, wśród których należy wyróżnić:

1) przetwarzanie danych odbywa się przez organ administracji publicznej lub inny podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
2) główna działalność administratora danych lub podmiotu przetwarzającego polega na operacjach przetwarzania wymagających, na dużą skalę, regularnego i systematycznego monitorowania osób, których dane dotyczą[327];
3) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kate-

[324] Artykuł 29 RODO.

[325] Artykuł 37 ust. 1 RODO.

[326] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 37*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 556.

[327] Artykuł 37 ust. 1 lit. a–b RODO. Zob. A. Stępień, P. Biały, *op. cit*., s. 39–40; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 37...*, s. 556–561.

gorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa[328].

Inspektor ochrony danych może być wyznaczony dla grupy administratorów danych lub podmiotów przetwarzających, które są podmiotami prywatnymi lub podmiotami publicznymi[329].

Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych[330].

Przepisy prawa wyróżniają trzy cechy, jakie powinien spełniać inspektor ochrony danych osobowych: kompetencyjność, niezależność oraz fachowość[331].

Pierwsza cecha, jaką jest kompetencyjność, oznacza, że inspektor powinien być wyposażony w prawa wobec innych podmiotów wewnątrz struktury organizacyjnej administratora danych lub podmiotu przetwarzającego, które skutecznie będą umożliwiały mu wykonywanie jego obowiązków. W tym celu inspektorowi zostało nadane prawo właściwego i niezwłocznego włączenia się we wszystkie sprawy dotyczące ochrony danych w związku z prowadzeniem działalności administratora danych lub podmiotu przetwarzającego[332].

Przepisy prawa wymagają także w tym celu zapewnienia inspektorowi ochrony danych niezależności od pomiotów, których działania ana-

[328] Artykuł 37 ust. 1 lit. c RODO. Zob. więcej A. Stępień, P. Biały, *op. cit*., s. 40; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 37...*, s. 561–562.

[329] W świetle art. 37 ust. 2 RODO grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, a myśl art. 37 ust. 3 RODO podobnie: grupa podmiotów publicznych, w tym organów administracji publicznej, może wyznaczyć jednego inspektora.

[330] Artykuł 37 ust. 3 RODO.

[331] Zdaniem K. Wygody wymogi zawarte w rozporządzeniu 2016/679 dotyczące wyboru inspektora ochrony danych mają charakter merytoryczny. K. Wygoda, *Administrator bezpieczeństwa informacji a inspektor ochrony danych na tle regulacji krajowych i unijnych – wybrane zagadnienia*, „Przegląd Prawa i Administracji" 2016, Nr 105, s. 232.

[332] Artykuł 38 ust. 1 RODO. Zob. M. Kibil, M. Gawroński, *Inspektor ochrony danych (IOD)*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018, s. 364–365.

lizuje. Gwarancją niezależności jest m.in. zakaz przekazywania inspektorowi instrukcji dotyczących wykonywania przez niego zadań[333] oraz wyłączenie możliwości wykonywania innych zadań i obowiązków, które mogłyby przyczynić się do powstania konfliktu interesów[334].

Trzecim elementem gwarantującym skuteczne wykonanie funkcji inspektora ochrony danych jest jego fachowość. Przepisy prawa wskazują, że inspektor ochrony danych powinien posiadać odpowiednią wiedzę[335] oraz umiejętności umożliwiające mu efektywne wykonanie jego zadań. Wiedza fachowa powinna dotyczyć prawa i praktyk w dziedzinie ochrony danych[336], a poziom wiedzy odpowiadać rodzajowi operacji przetwarzania chronionych danych osobowych[337].

Zadania inspektora ochrony danych są wyznaczone w przepisach prawa albo przez administratora danych lub podmiot przetwarzający, w tym poprzez zaakceptowanie przez te podmioty wiążących reguł korporacyjnych zatwierdzonych przez właściwy organ nadzorczy[338]. Wykonanie tych zadań ma m.in. na celu zapewnienie skutecznej ochrony danych osobowych przez administratora danych lub podmiot przetwarzający, co świadczy o pomocniczym charakterze inspektora ochrony danych wobec tych podmiotów. Inspektor, wykonując te zadania, ma także na celu umożliwienie realizacji organom nadzorczym swoich kompetencji oraz osobom

[333] W świetle art. 38 ust. 3 zd. 1 RODO, administrator danych oraz podmiot przetwarzający mają obowiązek zapewnienia, aby wobec inspektora ochrony danych nie były kierowane instrukcje dotyczące wykonywania jego zadań. Zob. M. Kibil, M. Gawroński, *op. cit.*, s. 367–368.

[334] W świetle wykładni *a contrario* art. 38 ust. 6 RODO inne zadania i obowiązki inspektora ochrony danych nie mogą przyczyniać się do powstania konfliktu interesu w związku z wykonywaniem zadań i obowiązków dotyczących ochrony danych osobowych.

[335] Artykuł 37 ust. 5 RODO. Zob. K. Wygoda, *Administrator bezpieczeństwa informacji...*, s. 234.

[336] Motyw 97 RODO; art. 37 ust. 5 RODO. Zob. A. Stępień, P. Biały, *op. cit.*, s. 40; M. Kibil, M. Gawroński, *op. cit.*, s. 363–364.

[337] W świetle motywu 97 RODO niezbędny poziom wiedzy fachowej wymaganej od inspektora ochrony danych powinien uwzględniać rodzaj prowadzonych operacji przetwarzania danych osobowych oraz ich ochrony.

[338] Artykuł 47 ust. 2 lit. h w zw. art. 47 ust. 1 RODO.

fizycznym realizacji praw związanych z ochroną ich danych osobowych. Zadania inspektora ochrony danych można podzielić ze względu na ich kategorię na zadania o charakterze: informacyjnym, kontrolnym, edukacyjnym, konsultacyjnym oraz kontaktowym.

Zadania inspektora o charakterze informacyjnym obejmują czynności skierowane do podmiotów wewnętrznych i zewnętrznych. Obowiązek informacyjny wobec podmiotów wewnętrznych obejmuje informowanie administratora danych, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach dotyczących ochrony tych danych, które są wyrażone w przepisach prawa[339]. Obowiązek informacyjny wobec podmiotów zewnętrznych obejmuje informowanie organu nadzorującego oraz osób fizycznych, których dane są przetwarzane. Inspektor ochrony danych pełni funkcję punktu kontaktowego dla organu nadzorczego w celu bieżącego informowania o przetwarzaniu danych[340]. Osoby fizyczne, jako podmioty zewnętrzne, także mają prawo uzyskać bieżącą informację na temat procesu przetwarzania ich danych osobowych[341].

Z zadaniami informacyjnymi związane są także zadania edukacyjne, które są skierowane do podmiotów wewnętrznych i dotyczą zagadnień ogólnych procesu przetwarzania danych osobowych. Inspektor ochrony danych powinien w tym celu podejmować działania zwiększające świadomość personelu uczestniczącego w operacjach przetwarzania, w tym poprzez prowadzenie szkoleń[342].

Kolejne zadania mające na celu przekazywanie informacji mają charakter konsultacyjną. Inspektor ochrony danych ma obowiązek doradzania administratorowi danych, podmiotowi przetwarzającemu oraz pracownikom, którzy przetwarzają dane osobowe, w sprawie ich obowiązków

[339] W świetle art. 39 ust. 1 pkt a RODO informacje o przepisach prawa dotyczą regulacji Unii Europejskiej oraz państw członkowskich.

[340] Artykuł 39 ust. 1 lit. e RODO.

[341] Artykuł 38 ust. 4 RODO.

[342] Artykuł 39 ust. 1 lit. b RODO.

związanych z przetwarzaniem tych danych[343]. Inspektor powinien także zapewnić administratorowi danych konsultacje w trakcie przygotowania oceny skutków dla ochrony danych[344].

Inspektor ochrony danych ma także obowiązek podejmowania czynności kontrolnych obejmujących monitorowanie przestrzegania przepisów prawa oraz polityk w sprawie ochrony danych osobowych[345], wykonania oceny skutków ochrony danych[346], a także prowadzenie związanych z tym audytów[347].

Jednym z podstawowych zadań inspektora ochrony danych jest również zapewnienie współpracy z osobami fizycznymi, w związku z przetwarzaniem ich danych osobowych[348], oraz z organem nadzorczym[349]. W celu ułatwienia wykonania inspektorowi zadania kontrolnego administrator danych powinien udostępniać jego dane kontaktowe osobom, których dane są przetwarzane[350], organowi nadzorczemu[351], a także zamieścić je w rejestrze czynności przetwarzania danych osobowych[352].

[343] Artykuł 39 ust. 1 lit. a RODO.

[344] Artykuł 35 ust. 2 w zw. z art. 35 ust. 1 RODO.

[345] Artykuł 39 ust. 1 lit. b RODO.

[346] Artykuł 39 ust. 1 lit. c RODO.

[347] Artykuł 39 ust. 1 lit. b RODO.

[348] W świetle art. 38 ust. 4 RODO inspektor ochrony danych powinien zapewnić osobom fizycznym, których dane dotyczą, możliwość kontaktu we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykorzystaniem ich praw.

[349] Artykuł 39 ust. 1 lit. d RODO.

[350] Administrator danych, podczas przekazywania danych osobowych bezpośrednio od osoby fizycznej, powinien podać jej m.in. informację dotyczącą danych kontaktowych inspektora ochrony danych (art. 13 ust. 1 lit. b RODO). Administrator danych powinien przekazać tej osobie dane kontaktowe także w przypadku, gdy pozyskał dane osobowe z innego źródła (art. 14 ust. 1 lit. b RODO).

[351] W świetle art. 36 ust. 3 lit. d RODO administrator danych powinien przekazać organowi nadzorczemu dane kontaktowe inspektora ochrony danych w związku z konsultacjami dotyczącymi stosowania środków minimalizujących ryzyko związane z przetwarzaniem danych osobowych.

[352] Zgodnie z art. 30 ust. 1 lit. a oraz art. 3 ust. 2 lit. a RODO administrator danych oraz podmiot przetwarzający powinni zamieścić w rejestrze czynności przetwarzania danych osobowych dane kontaktowe inspektora ochrony danych.

6. Organ nadzorczy

Prezes Urzędu Ochrony Danych Osobowych, dalej nazywany Prezesem Urzędu, jest organem nadzorczym właściwym w sprawach związanych z ochroną danych osobowych na terytorium Polski[353]. Zadania Prezesa Urzędu skierowane są na ochronę podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem ochrony danych oraz ułatwieniem swobodnego przepływu tych danych w Unii Europejskiej[354]. Prezesa Urzędu powołuje i odwołuje Sejm Rzeczypospolitej Polskiej za zgodą Senatu Rzeczypospolitej Polskiej[355]. Prezesem Urzędu może zostać jedynie osoba posiadające kwalifikacje, doświadczenie i umiejętności, zwłaszcza w dziedzinie ochrony danych osobowych, umożliwiające mu wypełnienie jego obowiązków i uprawnień[356].

Organ ten jest niezależny wobec innych podmiotów publicznych[357]. Przepisy prawa w tym celu: określają, że Prezes Urzędu, wykonując swo-

[353] W świetle art. 4 pkt 21 RODO organ nadzorczy jest niezależnym organem publicznym ustanowionym przez państwo członkowskie. W myśl art. 34 ust. 2 u.o.d.o. Prezes Urzędu Ochrony Danych Osobowych jest organem nadzorczym w rozumieniu RODO. Art. 7 ust. 1 u.o.d.o. wprowadza domniemanie kompetencji Prezesa Urzędu w sprawach nieuregulowanych w u.o.d.o. Zgodnie z art. 34 ust. 1 u.o.d.o. Prezes Urzędu jest organem właściwym w sprawie ochrony danych osobowych. Zgodnie z motywem 122 zd. 1 RODO organ nadzorczy jest właściwy do wykonywania uprawnień i zadań powierzonych na podstawie rozporządzenia 2016/679, na terytorium państwa członkowskiego, przez które został utworzony.

[354] Artykuł 51 ust. 1 RODO. Zgodnie z motywem 123 zd. 1 RODO Prezes Urzędu jako organ nadzorczy monitoruje stosowanie rozporządzenia 2016/679 oraz przyczynia się do jego spójnego stosowania w całej Unii, w celu zapewnienia ochrony danych osobowych oraz swobodnego przepływu tych danych na rynku wewnętrznym.

[355] Artykuł 34 ust. 3 u.o.d.o. W świetle art. 4 pkt 21 RODO organ nadzorczy jest ustanawiany przez państwo członkowskie. Przepis ten stanowi wykonanie regulacji art. 53 ust. 1 RODO, w świetle którego państwo członkowskie powinno zapewnić, aby każdy członek ich organów nadzorczych był powoływany w drodze przejrzystej procedury np. przez parlament.

[356] Artykuł 53 ust. 2 RODO. Wymagania te zostały wyszczególnione w art. 34 ust. 4 u.o.d.o., w świetle którego na stanowisko Prezesa Urzędu może być powołana osoba, która spełnia łącznie przesłanki: posiadanie obywatelstwa polskiego, wyższego wykształcenia, nieposzkalowanej opinii, wyróżnianie się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych, korzystaniem z pełni praw publicznych, a także nieskazanie prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe.

[357] W świetle art. 52 ust. 1 RODO organ nadzorczy powinien w sposób niezależny wypełniać swoje zadania i wykonywać swoje uprawnienia zawarte w RODO. Zgodnie z motywem 117

je zadania, podlega jedynie ustawom[358], i wskazują kadencyjność jego funkcji[359]. Niezależność Prezesa Urzędu ma zapewnić także obowiązek powstrzymania się od wszelkich czynności sprzecznych ze swoimi obowiązkami, w tym podejmowania zajęć zarobkowych lub niezarobkowych sprzecznych z tymi obowiązkami[360]. Jednocześnie Prezes Urzędu podczas wypełniania swoich zadań i uprawnień pozostaje wolny od bezpośrednich i pośrednich wpływów zewnętrznych, nie może realizować niczyich instrukcji[361]. W celu prawidłowego wykonania swoich zadań Prezes Urzędu powinien mieć zapewnione możliwości kadrowe, techniczne, organizacyjne i finansowe[362]. Niezależność Prezesa Urzędu ma jednak czę-

zd. 1 RODO Prezes Urzędu jako organ nadzorczy powinien być uprawniony do wykonywania swoich zadań i uprawnień w sposób całkowicie niezależny.

[358] Artykuł 34 ust. 5 u.o.d.o.

[359] W świetle art. 34 ust. 6–7 u.o.d.o. kadencja Prezesa Urzędu trwa 4 lata, a jednocześnie ograniczono liczbę kadencji do dwóch. W świetle art. 34 ust. 9 u.o.d.o. prawodawca ograniczył przesłanki odwołania Prezesa Urzędu przed upływem kadencji do: zrzeczenia się stanowiska, powstania trwałej niezdolności do pełnienia obowiązków na skutek choroby stwierdzonej orzeczeniem lekarskim, sprzeniewierzenia się ślubowaniu, skazaniu prawomocnym wyrokiem sądu za popełnienie umyślnego przestępstwa lub umyślnego przestępstwa skarbowego oraz pozbawienia praw publicznych. Przepis ten stanowi wykonanie regulacji art. 53 ust. 4 RODO: piastun organu nadzoru może zostać odwołany ze stanowiska jedynie wówczas, gdy dopuścił się poważnego uchybienia lub przestał spełniać warunki niezbędne do pełnienia obowiązków.

[360] Artykuł 52 ust. 3 RODO. Zgodnie z art. 37 ust. 1 u.o.d.o. Prezes Urzędu oraz jego zastępcy nie mogą zajmować innego stanowiska, z wyjątkiem stanowiska dydaktycznego, naukowo-dydaktycznego lub naukowego w szkole wyższej, Polskiej Akademii Nauk, instytucie badawczym lub innej jednostce naukowej. W świetle tego przepisu Prezes Urzędu nie powinien także wykonywać innych zajęć zarobkowych lub niezarobkowych sprzecznych ze swoimi obowiązkami. W myśl art. 37 ust. 2 u.o.d.o. Prezes Urzędu oraz jego zastępcy nie mogą także należeć do partii politycznej, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością tego urzędu. W myśl motywu 121 zd. 2 RODO Prezes Urzędu jako organ nadzorczy powinien działać uczciwie, powstrzymywać się od czynności niezgodnych z jego obowiązkami oraz nie podejmować zajęć zarobkowych i niezarobkowych niezgodnych z tymi obowiązkami.

[361] Artykuł 52 ust. 2 RODO. Zob. P. Litwiński, P. Barta, *Komentarz do art. 52*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 669–670.

[362] W świetle art. 52 ust. 4 RODO państwa członkowskie mają obowiązek zapewnienia organowi nadzorczemu odpowiednich zasobów kadrowych, technicznych i finansowych, oraz pomieszczeń i infrastruktury niezbędnych do skutecznego wypełniania jego zadań i wykony-

ściowo względny charakter, podlega on bowiem kontroli finansowej oraz kontroli sądowej[363].

Można wyróżnić kilka grup zadań Prezesa Urzędu, do których zaliczają się zadania: informacyjne; związane ze stosowaniem środków ochrony; mające na celu rozpoczęcie i prowadzenie współpracy z innymi organami oraz związane z prowadzeniem postępowań.

Zadania informacyjne mają charakter indywidualny oraz generalny. Indywidualne zadania informacyjne, które są skierowane wobec indywidualnego adresata, obejmują udzielenie informacji na żądanie osoby, której dane dotyczą, o wykonywaniu praw przysługujących jej na mocy rozporządzenia 2016/679[364], a także konsultacje z administratorem w sprawie ograniczenia wysokiego ryzyka ochrony danych[365]. Generalnymi zadaniami informacyjnymi, skierowanymi wobec niezidentyfikowanych adresatów lub grupy indywidulanych adresatów, są: upowszechnienie w społeczeństwie wiedzy o ochronie danych, w tym uświadamianie ryzyka, zasad, zabezpieczeń i praw związanych z przetwarzaniem tych danych[366]; upowszechnienie wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy rozporządzenia 2016/679[367]. Zadania informacyjne o charakterze generalnym mają na

wania jego uprawnień, w tym w zakresie wzajemnej pomocy, współpracy i uczestnictwa w pracach Europejskiej Rady Ochrony Danych. Zgodnie z art. 52 ust. 5 RODO państwo członkowskie ma także obowiązek zapewnić organowi nadzorczemu własnego personelu, wybranego przez piastuna tego organu, działającego pod wyłącznym swoim kierownictwem. W świetle motywu 120 RODO Prezes Urzędu jako organ nadzorczy powinien być wyposażony w zasoby finansowe i kadrowe, pomieszczenia i infrastrukturę niezbędne do skutecznego wykonywania zadań, a także dysponować odrębnym, publicznym budżetem rocznym. Zgodnie z motywem 121 zd. 3 RODO Prezes Urzędu jako organ nadzorczy powinien dysponować pracownikiem personalnym działającym pod jego wyłącznym kierownictwem.

[363] W świetle motywu 118 RODO Prezes Urzędu jako organ nadzorczy powinien podlegać mechanizmowi kontroli lub monitorowania pod kątem wydatków oraz kontroli sądowej. Zob. P. Litwiński, P. Barta, *Komentarz do art. 52*..., s. 670.

[364] Artykuł 57 ust. 1 lit. e RODO.

[365] Artykuł 36 ust. 1 RODO.

[366] Artykuł 57 ust. 1 lit. b RODO; motyw 122 zd. 3 RODO.

[367] Artykuł 57 ust. 1 lit. d RODO.

celu efektywne stosowanie przepisów o ochronie danych. Przykładem ich wykonania jest m.in. upowszechnienie wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków ochrony danych[368], wykazu rodzajów operacji przetwarzania danych osobowych niewymagających oceny skutków[369]oraz udostępnienia na stronie podmiotowej BIP Prezesa Urzędu standardowych klauzul umownych, zatwierdzonych kodeksów postępowania, przyjętych standardowych klauzul ochrony danych oraz rekomendacje określające środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych[370].

Zadania Prezesa Urzędu są również związane ze stosowaniem środków ochrony; a w tym zakresie przyjmuje on standardowe klauzule umowne[371]; ustanawia i prowadzi wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków ochrony danych[372]; udziela zaleceń dotyczących operacji przetwarzania[373]; zachęca do sporządzania kodeksów postępowania, wydaje opinie na ich temat oraz zatwierdza te kodeksy, w których znajdują się odpowiednie zabezpieczenia[374]; zachęca do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń z tej dziedziny, a także zatwierdza kryteria certyfikacji[375]; dokonuje okresowego przeglądu udzielonych certyfikacji[376]; opracowuje i publikuje wymogi akredytacji podmiotu monitorującego ko-

[368] Artykuł 54 ust. 1 pkt 1 u.o.d.o. w zw. z art. 35 ust. 4 RODO.

[369] Artykuł 54 ust. 1 pkt 2 u.o.d.o. w zw. z art. 35 ust. 5 RODO.

[370] Artykuł 53 ust. 1 u.o.d.o.

[371] Artykuł 57 ust. 1 lit. j w zw. z art. 28 ust. 8 i art. 46 ust. 2 lit. d RODO.

[372] Artykuł 57 ust. 1 lit. k w zw. z art. 35 ust. 4 RODO.

[373] Artykuł 57 ust. 1 lit. l w zw. z art. 36 ust. 2 RODO.

[374] Artykuł 57 ust. 1 lit. m w zw. z art. 40 ust. 1 oraz art. 40 ust. 5 RODO. W świetle art. 40 ust. 1 RODO Prezes Urzędu zachęca do sporządzania kodeksów postępowania, a w myśl art. 40 ust. 5 zd. 2 RODO organ ten wydaje opinię o zgodności kodeksu, jego zmianie i rozszerzenia z rozporządzeniem 2016/679, a także zatwierdza taki projekt kodeksu, jego zmianę lub rozszerzenie.

[375] Artykuł 57 ust. 1 lit. n w zw. z art. 42 ust. 5 RODO.

[376] Artykuł 57 ust. 1 lit. o w zw. z art. 42 ust. 7 RODO.

deksy postępowania oraz podmiotu certyfikującego[377]; akredytuje podmiot monitorujący kodeksy postępowania oraz podmiot certyfikujący[378]; wydaje zezwolenia na klauzule umowne i przepisy stanowiące odpowiednie zabezpieczenia gwarantujące przekazywanie danych osobowych poza Unię Europejską[379]; zatwierdza wiążące reguły korporacyjne[380].

Prezes Urzędu wykonuje także zadania mające na celu rozpoczęcie i prowadzenie współpracy m.in. z innymi organami nadzorczymi w pozostałych państwach członkowskich[381], organami i władzami Rzeczpospolitej Polskiej[382] oraz organami Unii Europejskiej[383].

Do zadań Prezesa Urzędu należy także prowadzenie postępowań, w tym związanych z rozpatrzeniem skarg wniesionych przez osobę, której dane dotyczą[384], oraz wszczętych na podstawie informacji otrzymanych od innych organów administracji publicznej, w tym od organów nadzorczych z innych państw członkowskich[385]. Prezes Urzędu prowadzi postępowanie nadzorcze zgodnie z regulacjami Kodeksu postępowania administra-

[377] Artykuł 57 ust. 1 lit. p w zw. z art. 41 oraz art. 43 RODO.

[378] Artykuł 57 ust. 1 lit. q w zw. z art. 41 oraz art. 43 RODO.

[379] Artykuł 57 ust. 1 lit. r w zw. z art. 46 ust. 3 RODO.

[380] Artykuł 57 ust. 1 lit. s w zw. z art. 47 RODO.

[381] W świetle art. 57 ust. 1 lit. g RODO Prezes Urzędu współpracuje z innymi organami nadzorczymi w celu zapewnienia spójnego stosowania i egzekwowania rozporządzenia 2016/679. W świetle art. 59 ust. 1 u.o.d.o. Prezes Urzędu współpracuje z niezależnymi organami nadzorczymi w sprawach ochrony danych osobowych. W świetle motywu 123 zd. 2 RODO Prezes Urzędu powinien współpracować z innymi organami nadzorczymi oraz Komisją Europejską, nawet wówczas, gdy nie ma zawartej umowy o wzajemnej pomocy lub współpracy pomiędzy państwami członkowskimi.

[382] Zgodnie z art. 57 ust. 1 lit. c RODO Prezes Urzędu doradza, zgodnie z prawem państwa polskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem. Zgodnie z art. 52 ust. 1 u.o.d.o. Prezes Urzędu może kierować m.in. do organów państwowych, organów samorządu terytorialnego wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych.

[383] W myśl art. 57 ust. 1 lit. t RODO Prezes Urzędu bierze udział w pracach Europejskiej Rady Ochrony Danych. Zgodnie z art. 51 ust. 2 zd. 2 RODO Prezes Urzędu ma obowiązek współpracy z innymi organami nadzorczymi w państwach członkowskich oraz z Komisją Europejską.

[384] Artykuł 57 ust. 1 lit. f RODO; motyw 122 zd. 3 RODO.

[385] Artykuł 57 ust. 1 lit. h RODO.

cyjnego[386]. Ustawa o ochronie danych osobowych wprowadza jednakże częściowe odrębności, szczególnie w zakresie postępowania dowodowego, związanego z ponoszeniem kosztów tłumaczenia dokumentacji na język polski[387] oraz prowadzeniem postępowania kontrolnego, jeżeli zajdzie konieczność uzupełnienia dowodów[388]. Organ ten ma także z zasady prawo dostępu do informacji objętych tajemnicą prawnie chronioną, także objętych tajemnicą przedsiębiorstwa[389].

Przepisy prawa wprowadzają również inne zadania Prezesa Urzędu, do jakich należą m.in.[390]: monitoring rozwoju nowych technologii informacyjno-komunikacyjnych i praktyk handlowych[391]; prowadzenie wewnętrznego rejestru naruszeń rozporządzenia 2016/679 i zastosowania uprawnień przez Prezesa Urzędu[392].

Prezes Urzędu w celu wykonywania tych zadań wykonuje czynności kontrolne nad procesem przetwarzania danych osobowych[393]. Prawa tego organu związane z prowadzeniem kontroli obejmują głównie prawo do uzyskania informacji m.in. od administratora lub podmiotu przetwarzającego. Prawa te wynikają wprost z rozporządzenia 2016/679 lub wymagają konkretyzacji ze strony Prezesa Urzędu. Prawem wynikającym wprost z roz-

[386] Artykuł 60 w zw. z art. 7 ust. 1 u.o.d.o.

[387] W świetle art. 63 u.o.d.o. Prezes Urzędu może żądać od strony przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez stronę na jej koszt.

[388] Artykuł 68 ust. 1 u.o.d.o.

[389] Artykuł 64 u.o.d.o. W świetle art. 65 ust. 1–3 u.o.d.o. strona postępowania nadzorczego jest obowiązana do przedstawienia Prezesowi Urzędu wersji dokumentu niezawierającego informacji objętych zastrzeżeniem tajemnicy przedsiębiorstwa, jeżeli strona złożyła takie zastrzeżenie, a Prezes Urzędu, w drodze decyzji, nie uchylił tego zastrzeżenia.

[390] Wymienione zadania nie są wszystkimi zadaniami Prezesa Urzędu, na co wskazuje otwarty charakter ich katalogu. Zob. art. 57 ust. 1 lit. v RODO.

[391] Artykuł 57 ust. 1 lit. i RODO.

[392] Artykuł 57 ust. 1 lit. u w zw. z art. 58 ust. 2 RODO.

[393] Jak zauważyła M. Sakowska-Baryła, w toku analizy starych przepisów dotyczących ochrony danych wyrażonych w u.o.d.o.97, skutkiem kontroli sprawowanej przez Generalnego Inspektora Ochrony Danych Osobowych (organ, który jest poprzednikiem Prezesa Urzędu), może być władcza ingerencja w proces przetwarzania danych osobowych. M. Sakowska-Baryła, *Kontrolowanie przez GIODO przetwarzania danych osobowych*, „Kontrola Państwowa" 2016, Nr 2, s. 28.

porządzenia 2016/679 jest uzyskanie informacji na podstawie zgłoszenia naruszenia ochrony danych osobowych[394]. Prawa wymagające konkretyzacji przez Prezesa Urzędu obejmują m.in.: prawo żądania udostępnienia rejestru czynności przetwarzania danych osobowych[395]; prawo dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych; prawo dostępu do informacji objętych tajemnicą prawnie chronioną[396] oraz dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych temu organowi do realizacji swoich zadań[397]. Prezes Urzędu jest też uprawniony do prowadzenia postępowań w formie audytów ochrony danych[398]; dokonywania przeglądu udzielonych certyfikacji pod kątem wypełniania kryteriów certyfikacji przez administratora lub podmiot przetwarzający[399]. Istotnym elementem kontroli jest przedstawianie jej wyników podmiotowi kontrolowanemu. W tym celu Prezesowi Urzędu nadano uprawnienie do zawiadamiania administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia rozporządzenia 2016/679[400].

7. Podmiot certyfikujący

Przepisy prawa wyróżniają także podmiot pośrednio związany z przetwarzaniem danych osobowych, a bezpośrednio związany z zapewnieniem stosowania zasad ich stosowania. Jest nim podmiot certyfikujący.

Podmiot certyfikujący może równolegle wobec Prezesa Urzędu Ochrony Danych Osobowych podejmować certyfikację świadczącą o zgodności

394 Artykuł 33 ust. 1 RODO.
395 Artykuł 30 ust. 4 RODO.
396 Artykuł 64 u.o.d.o.
397 Artykuł 58 ust. 1 lit. a oraz lit. e RODO.
398 Artykuł 58 ust. 1 lit. b RODO.
399 Artykuł 58 ust. 1 lit. c w zw. z art. 42 ust. 7 RODO.
400 Artykuł 58 ust. 1 lit. d RODO.

operacji przetwarzania z przepisami rozporządzenia 2016/679[401]. Certyfikat jest środkiem pośrednim ochrony danych osobowych. Podmiot certyfikujący powinien dysponować odpowiednim poziomem wiedzy fachowej dotyczącej ochrony danych[402], co potwierdza jego akredytacja wydana przez Polskie Centrum Akredytacji[403]. Akredytacja jest wydawana na wniosek przyszłego podmiotu certyfikującego[404], na podstawie kryteriów akredytacji zatwierdzonych przez Prezesa Urzędu lub Europejską Radę Ochrony Danych, udostępnionych na stronie podmiotowej Prezesa Urzędu w Biuletynie Informacji Publicznej[405], a jej udzielenie jest potwierdzone certyfikatem akredytacji zgodnie z wymogami ustawy o systemach oceny zgodności i nadzoru rynku[406]. Podmiot wnioskujący o udzielenie akredytacji powinien spełnić również inne warunki, wśród których należy wyróżnić: wykazanie swojej niezależności i wiedzy fachowej; zobowiązanie się do przestrzegania kryteriów certyfikacji; dysponowanie m.in. procedurami wydawania, okresowego przeglądu i cofania certyfikacji, a także przejrzy-

[401] W świetle art. 15 ust. 1 u.o.d.o. certyfikacji może dokonać Prezes Urzędu Ochrony Danych Osobowych lub podmiot certyfikujący. Przepis ten odpowiada treści art. 42 ust. 5 RODO: certyfikacji dokonują podmioty certyfikujące lub organ nadzorczy. Jak słusznie podkreślają P. Makowski, P. Drobek oraz K. Witkowska-Nowakowska, wprowadzone zostały dwa modele certyfikacji, jeden podejmowany przez podmiot certyfikujący, a drugi podejmowany przez organ nadzorczy. Zob. P. Makowski, P. Drobek, K. Witkowska-Nowakowska, *Komentarz do art. 43*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 850. Problematykę prowadzenia certyfikacji przez organ nadzorczy przedstawiają P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 43*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 618.

[402] Artykuł 43 ust. 1 RODO.

[403] Zgodnie z art. 43 ust. 1 *in fine* RODO państwa członkowskie zapewniają akredytację podmiotów certyfikowanych przez organ nadzorczy lub krajową jednostkę akredytacyjną. Polski prawodawca implementując ten przepis, w art. 12 ust. 1 u.o.d.o. wskazał, że akredytację wykonuje Polskie Centrum Akredytacji.

[404] Artykuł 23 ust. 1–4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2017 r., poz. 1398 ze zm.), dalej u.s.o.z.

[405] Artykuł 43 ust. 3 zd. 1 RODO w zw. z art. 13 u.o.d.o. W świetle art. 43 ust. 6 zd. 1–2 w zw. z art. 43 ust. 3 RODO Prezes Urzędu powinien podać w łatwo dostępny sposób do publicznej wiadomości kryteria akredytacji oraz przekazać je Europejskiej Radzie Ochrony Danych.

[406] Artykuł 24 ust. 1 u.s.o.z.

stymi procedurami i strukturami, umożliwiającymi rozpatrzenie skargi na naruszenie warunków certyfikacji przez administratora lub podmiot przetwarzający lub na sposób wdrożenia certyfikacji przez te podmioty; oraz wykazanie Prezesowi Urzędu, że jego zadania i obowiązki nie powodują konfliktu interesów w związku z prowadzeniem przez ten podmiot innej działalności niż certyfikacja[407]. Podmiot certyfikujący powinien spełniać warunki akredytacji przez cały okres jej ważności, który wynosi do pięciu lat[408]. W przypadku naruszenia tych warunków Polskie Centrum Akredytacji może cofnąć akredytację[409]. Centrum to ma obowiązek informowania Prezesa Urzędu o udzieleniu akredytacji oraz jej cofnięciu[410].

[407] Artykuł 43 ust. 2 RODO. Problematykę konfliktu interesów w związku z działalnością podmiotu certyfikującego oraz jego niezależności przedstawiają P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 43…*, s. 619. Zob. też P. Makowski, P. Drobek, K. Witkowska-Nowakowska, *op. cit.*, s. 851–854.

[408] Artykuł 24 ust. 3 u.s.o.z. W świetle art. 24 ust. 2 pkt 5 u.s.o.z. okres ważności certyfikacji jest określony w certyfikacie akredytacji. Zgodnie z art. 43 ust. 4 zd. 2 RODO akredytacja może być udzielona na okres do 5 lat, z możliwością jej przedłużenia na tych samych warunkach.

[409] Artykuł 24 ust. 4 u.s.o.z. W świetle art. 43 ust. 7 RODO cofnięcie akredytacji może nastąpić wówczas, gdy podmiot certyfikujący nie spełnia lub przestał spełniać warunki akredytacji lub jeżeli działania podejmowane przez ten podmiot naruszają przepisy rozporządzenia 2016/679.

[410] Artykuł 14 ust. 1–4 u.o.d.o.

Rozdział V

Pośrednie środki prawne ochrony danych osobowych

(Maciej Błażewski)

1. Rodzaje pośrednich środków prawnych ochrony danych osobowych

Pośrednie środki prawne ochrony danych osobowych są środkami prawnymi *sensu largo*. Środki te stosowane są przez administratora oraz podmiot przetwarzający. W grupie pośrednich środków prawnych można wyróżnić środki techniczne i organizacyjne, środki informacyjne, ocenę skutków przetwarzania danych osobowych wraz z konsultacjami z Prezesem Urzędu, rejestry dotyczące czynności przetwarzania, certyfikat, wiążące reguły korporacyjne oraz kodeks postępowania opracowany przez zrzeszenie lub podmiot reprezentujący administratorów lub podmioty przetwarzające.

2. Środki techniczne i organizacyjne

Administrator oraz podmiot przetwarzający mają obowiązek zapewnić bezpieczeństwo przetwarzania danych osobowych poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych, przed oraz

w trakcie przetwarzania. Środki techniczne mogą mieć charakter materialny, odnoszący się do pomieszczeń, gdzie przetwarzane są dane, oraz charakter informatyczny, w przypadku przetwarzania za pomocą systemów informatycznych. Środki organizacyjne mogą dotyczyć wewnętrznych norm prawnych oraz polityk bezpieczeństwa[411].

Podmioty te posiadają swobodę w wyborze środków technicznych i organizacyjnych, ponosząc jednocześnie odpowiedzialność za dokonany wybór. Przy dokonaniu wyboru podmioty te powinny uwzględniać zarówno uwarunkowania przetwarzania, jak i rodzaje ryzyka związanego z przetwarzaniem. Do uwarunkowań przetwarzania, wpływających na wybór środków, należą: stopień bezpieczeństwa względem naruszenia praw i wolności osób fizycznych, stan wiedzy technicznej, koszt wdrożenia tych środków, a także cechy przetwarzania, takie jak jego charakter, zakres, kontekst i cele[412]. Ryzykiem warunkującym wybór jest przypadkowe lub niezgodne z prawem zniszczenie, utrata, modyfikacja, nieuprawnione ujawnienie lub nieuprawniony dostęp do przetwarzanych danych osobowych[413].

Rozporządzenie 2016/679 wymienienia jedynie przykładowe środki techniczne i organizacyjne[414], którymi są m.in.:

1) pseudonimizacja i szyfrowanie danych osobowych;
2) posiadanie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

[411] R. Walasek, *Systemy bezpieczeństwa informacji w przedsiębiorstwach logistycznych – wyniki badania*, „Nauki o zarządzaniu. Management Sciences" 2016, Nr 1, s. 157.

[412] Artykuł 32 ust. 1 RODO. Zob. D. Lubasz, *Komentarz do art. 32*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 692, 694–698.

[413] Artykuł 32 ust. 2 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 32*..., s. 501–502; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 24*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 448–449.

[414] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 32*..., s. 502.

3) posiadanie zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania[415];
5) zapewnienie rzeczywistej podległości osób upoważnionych do zapewnienia przetwarzania[416].

Środkami technicznymi i organizacyjnymi mogą być także: umowy administratora z innymi podmiotami uczestniczącymi w procesie przetwarzania, wprowadzenie wymogu minimalizacji wobec przetwarzania danych, szczególnych wymogów w związku z przekazaniem danych do państw trzecich, polityki bezpieczeństwa danych[417], system bezpieczeństwa informacji[418], jak również ścisłego podziału organizacyjnego z odpowiednim wyróżnieniem odpowiedzialności za czynności podejmowane w procesie przetwarzania[419].

Administrator powinien móc wykazać stosowanie właściwych środków technicznych i organizacyjnych ze względu na ryzyka dla konkretne-

[415] Artykuł 32 ust. 1 RODO. Zgodnie z art. 32 ust. 3 RODO administrator lub podmiot przetwarzający może wykazać, że wywiązał się z obowiązków określonych w punktach 1–4 poprzez zastosowanie zatwierdzonego kodeksu postępowania lub certyfikatu. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 32*..., s. 502–503; D. Lubasz*, Komentarz do art. 32...,* s. 699–704.

[416] W świetle art. 32 ust. 4 RODO administrator oraz podmiot przetwarzający mają obowiązek zapewnić, aby każda osoba fizyczna działająca z ich upoważnienia, która ma dostęp do danych osobowych, przetwarzała je jedynie na polecenie administratora, chyba że wymóg przetwarzania wynika z przepisów szczególnych. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 32*..., s. 503, 504.

[417] A.P. Czarnowski, M. Gawroński, *Bezpieczeństwo danych w świetle RODO – analiza ryzyka i adekwatności środków*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018, s. 278–279. Politykę bezpieczeństwa jako przykład środka ochrony danych przedstawiają także: R. Walasek, *op. cit*., s. 157; M. Beskosty, *Zarządzanie bezpieczeństwem informacji*, Studia nad Bezpieczeństwem 2017, Nr 2, s. 165–166; J. Chmura, *Wartość informacji i jej bezpieczeństwo w gospodarce opartej na wiedzy*, Journal of Modern Science" 2016, Nr 3, s. 312.

[418] R. Walasek, *op. cit*., s. 157.

[419] J. Łuczak, *Ochrona danych osobowych*..., s. 69.

go procesu przetwarzania. Odpowiada to wymogom zasady rozliczalności. Ułatwieniem dla wypełnienia tego obowiązku jest możliwość stosowania zatwierdzonych kodeksów postępowania lub uzyskania certyfikatów[420].

3. Środki informacyjne

Środki informacyjne mogą mieć charakter prewencyjny, gdy dotyczą przyszłego lub bieżącego procesu przetwarzania danych osobowych, jak również charakter następczy, gdy dotyczą naruszeń przepisów prawa. Adresatem informacji może być osoba, której dane dotyczą, oraz Prezes Urzędu. Przekazanie informacji osobie, której dane dotyczą, ma na celu zagwarantowanie jej wypełnienia uprawnień kontrolnych[421]. Przekazanie informacji Prezesowi Urzędu służy wykonaniu jego zadań.

Prewencyjny charakter ma m.in. obowiązek informacyjny administratora wobec osoby, której dane dotyczą. Obowiązek ten ma miejsce niezależnie, czy dane osobowe zostały pozyskane od tej osoby, czy też z innego źródła[422]. Należy jednak podkreślić, że przepisy prawa różnicują zakres tego obowiązku z zależności od źródła pochodzenia danych. Informacje kierowane do osoby, której dane dotyczą, powinny być przekazane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, z zastosowaniem jasnego i prostego języka[423]. Informacje te nie powinny zatem być przygotowane z użyciem hermetycznego języka prawniczego[424].

[420] Artykuł 32 ust. 3 RODO. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 32…*, s. 503–504; D. Lubasz, *Komentarz do art. 32…,* s. 705.

[421] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 364–365.

[422] Artykuły. 13–14 RODO.

[423] Artykuł 12 ust. 1 RODO. Zob. J. Łuczak, *Komentarz do art. 13*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 486; J. Łuczak, *Komentarz do art. 14*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 506.

[424] J. Łuczak, *Komentarz do art. 13.*.., s. 486.

Administrator ma obowiązek, niezależnie od źródła pochodzenia danych, przekazania informacji obejmujących: określenie tożsamości i danych kontaktowych administratora (np. adresu jego siedziby)[425]; cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania zgodną z wymaganiami rozporządzenia 2016/679[426]; informacje o odbiorcach danych osobowych, jeżeli można określić konkretnych odbiorców, lub o istniejących kategoriach odbiorców[427]; a gdy ma to zastosowanie – także określenie tożsamości i danych kontaktowych przedstawiciela administratora[428]; dane kontaktowe inspektora ochrony danych, jeżeli został on ustanowiony[429]; informacje związane z przekazaniem danych osobowych do państwa trzeciego lub organizacji międzynarodowej[430]. Obowiązek poinformowania osoby, której dane dotyczą, jeżeli osoba ta podała te dane, obejmuje wskazanie, jakie prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią stanowią podstawę przetwarzania[431], a jeżeli dane pochodziły z innego źródła, obowiązek ten dotyczy także przekazania informacji o kategoriach danych osobowych[432].

Administrator ma także obowiązek podania osobie, której dane dotyczą, niezależnie od źródła pochodzenia danych, informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, w tym infor-

[425] Artykuły 13 ust. 1 lit. a oraz art. 14 ust. 1 lit. a RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13.*.., s. 366; J. Łuczak, *Komentarz do art. 13.*.., s. 482.

[426] Artykuły 13 ust. 1 lit. c oraz art. 14 ust. 1 lit. c RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13.*.., s. 366–367; J. Łuczak, *Komentarz do art. 13.*.., s. 482.

[427] Artykuły 13 ust. 1 lit. e oraz art. 14 ust. 1 lit. e RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13.*.., s. 367; J. Łuczak, *Komentarz do art. 13.*.., s. 482–483.

[428] Artykuły 13 ust. 1 lit. a oraz art. 14 ust. 1 lit. a RODO.

[429] Artykuły 13 ust. 1 lit. b oraz art. 14 ust. 1 lit. b RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13.*.., s. 366; J. Łuczak, *Komentarz do art. 13.*.., s. 483.

[430] Artykuły 13 ust. 1 lit. f oraz art. 14 ust. 1 lit. f RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13.*.., s. 368.

[431] Artykuł 13 ust. 1 lit. d w zw. z art. 6 ust. 1 lit. f RODO. Jak wskazują P. Litwiński, P. Barta oraz M. Kawecki, prawnie realizowane interesy obejmują m.in. działania marketingowego administratora, ochronę przed oszustwami lub dochodzenie roszczeń w postępowaniu sądowym. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13.*.., s. 367.

[432] Artykuł 14 ust. 1 lit. d RODO.

macje o: okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu[433]; prawie wniesienia skargi do organu nadzorczego[434]; zautomatyzowanym podejmowaniu decyzji[435] oraz o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania i o prawie do wniesienia sprzeciwu wobec przetwarzania, o prawie do przenoszenia danych[436] oraz o ewentualnej możliwości cofnięcia zgody na przetwarzanie[437].

Administrator powinien także poinformować osobę, której dane dotyczą, o planowej zmianie celu przetwarzania, jak również o innych zmianach związanych z przetwarzaniem danych, będących konsekwencją zmiany celu, takich jak zmiana okresu przetwarzania[438].

Przepisy jedynie częściowo różnicują zakres informacji, w zależności od źródła danych osobowych. Jeżeli dane pochodzą od osoby, której one dotyczą, informacje prawe powinny także wskazywać podstawę prawną pobrania danych osobowych[439]. W przypadku, gdy dane pochodzą z innego źródła, osoba, której dane dotyczą, powinna być poinformo-

[433] Artykuły 13 ust. 2 lit. a oraz art. 14 ust. 2 lit. a RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13.*.., s. 369.

[434] Artykuły 13 ust. 2 lit. d oraz art. 14 ust. 2 lit. e RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13.*.., s. 370.

[435] Artykuły 13 ust. 2 lit. f oraz art. 14 ust. 2 lit. g RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13.*.., s. 371–373; J. Łuczak, *Komentarz do art. 13.*.., s. 483–485.

[436] Artykuły 13 ust. 2 lit. b oraz art. 14 ust. 2 lit. c RODO.

[437] Zgodnie z art. 13 ust. 2 lit. c oraz art. 14 ust. 2 lit. d w zw. z art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO, jeżeli przetwarzanie danych odbywa się na podstawie zgody, osoba, której dane dotyczą, powinna być poinformowana o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

[438] Zgodnie z art. 13 ust. 3 oraz art. 14 ust. 4 RODO obowiązek poinformowania o zmianie celu powinien zostać wykonany przed jego zmianą. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 13.*.., s. 375.

[439] W świetle art. 13 ust. 2 lit. e RODO osoba, której dane dotyczą, jeżeli jest źródłem tych danych, powinna być poinformowana, czy podstawą prawną pobrania tych danych jest ustawa, umowa lub inne zobowiązanie, i jakie są ewentualne konsekwencje niepodania danych.

wana o źródle pochodzenia danych osobowych[440] oraz, czy podstawą ich przetwarzania są prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią[441].

Przepisy prawa określają również czas wykonania obowiązku informacyjnego przez administratora, gdy źródłem danych jest osoba, której one dotyczą. Czas przekazania informacji zależy od celu ich pozyskania. Zasadą jest, że informacje o pozyskaniu danych powinny zostać podane w rozsądnym terminie po ich pozyskaniu, ale nie później niż w ciągu miesiąca, przy uwzględnieniu konkretnych okoliczności ich przetwarzania[442]. Wyjątkowo obowiązek informacyjny powinien zostać wykonany najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą, lub pierwszym ujawnieniu tych danych innemu odbiorcy[443], a w przypadku zmiany celu ich przetwarzania przed taką zmianą[444].

Obowiązek informacyjny jest wyłączony, niezależnie od źródła pochodzenia danych osobowych, jeżeli osoba, której dane dotyczą, dysponuje tymi informacjami[445]. Przepisy prawa wyłączają ten obowiązek w przypadku, gdy dane osobowe nie pochodzą od osoby, której one dotyczą, gdy udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku[446]; pozyskiwanie lub ujaw-

[440] Artykuł 14 ust. 2 lit. f RODO

[441] Artykuł 14 ust. 2 lit. b w zw. z art. 6 ust. 1 lit. f RODO.

[442] Artykuł 14 ust. 3 lit. a RODO.

[443] Zgodnie z art. 14 ust. 3 lit. b RODO obowiązek komunikacyjny powinien być wykonany przy pierwszej komunikacji, jeżeli celem ich pozyskania jest komunikacja z osobą, której dane dotyczą, a w świetle art. 14 ust. 3 lit. c RODO obowiązek ten należy wykonać najpóźniej przy pierwszym ujawnieniu danych osobowych innemu odbiorcy, jeżeli taki był cel ich pozyskania. Zob. J. Łuczak, *Komentarz do art. 14.…*, s. 500–501.

[444] Artykuł 13 ust. 3 RODO.

[445] Artykuły 13 ust. 4 w zw. z art. 13 ust. 1–3 oraz art. 14 ust. 5 lit. a w zw. z art. 14 ust. 1 RODO. Zob. J. Łuczak, *Komentarz do art. 13.…*, s. 488.

[446] Artykuł 14 ust. 5 lit. b RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 14*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 385–386.

nianie jest wyraźnie uregulowane przez przepisy prawa[447] albo gdy dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej, przewidzianym w tych przypisach[448].

Drugi rodzaj środków informacyjnych, które mają charakter następczy, obejmuje obowiązek przekazanie informacji o nieprawidłowości w przetwarzaniu Prezesowi Urzędu lub osobom, których dane dotyczą. Przepisy prawa różnicują obowiązek stosowania tych środków w zależności od rodzaju naruszenia oraz adresata informacji. Należy wyróżnić dwa środki informacyjne: zgłoszenie naruszenia ochrony danych[449] oraz zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych[450].

Zgłoszenie Prezesowi Urzędu naruszenia danych osobowych jest dokonywane przez administratora lub przez podmiot przetwarzający administratorowi[451].

Zgłoszenie Prezesowi Urzędu powinno zostać przekazane, jeżeli naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych. Zgłoszenie powinno zawierać przynajmniej: opis charakteru naruszenia ochrony danych osobowych; imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego; opis możliwych konsekwencji naruszenia ochrony danych osobowych; opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych[452]. Zgłoszenie może zawierać także

[447] Artykuł 14 ust. 5 lit. c RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 14…*, s. 386–388.

[448] Art. 14 ust. 5 lit. d RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 14…*, s. 388–389.

[449] Artykuł 33 RODO. Zdaniem M. Tarnawy-Zajączkowskiej, regulacje zawarte w rozporządzeniu 2016/679, w tym dotyczące zgłoszenia naruszenia ochrony danych, porządkują obowiązki administratora, tym samym wprowadzając spójne mechanizmy ochrony danych osobowych. M. Tarnawa-Zajączkowska, *Rewolucje w ochronie danych osobowych – gdzie ich szukać?*, „Casus" 2017, Nr 4, s. 43.

[450] Artykuł 34 RODO.

[451] Artykuł 33 ust. 1–2 RODO.

[452] Artykuł 33 ust. 3 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 33*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwa-*

inne informacje, o ile podmiot zgłaszający uzna, że będą one przydatne do wyjaśnienia okoliczności naruszenia[453]. Ze względu na potrzebę szybkiego wykonania zadań przez Prezesa Urzędu przepisy prawa określają czas zgłoszenia mu naruszenia ochrony danych osobowych[454].

Zgłoszenie administratorowi powinien wnieść podmiot przetwarzający, jeżeli stwierdzi naruszenie ochrony danych osobowych[455]. Ma to na celu umożliwienie administratorowi analizę ryzyka oraz zastosowanie odpowiednich środków zapewniających bezpieczeństwo. Zgłoszenie powinno być przekazane administratorowi bez zbędnej zwłoki[456].

Administrator powinien zawiadomić osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych[457]. Zawiadomienie powinno być sporządzone jasnym i prostym językiem, zawierać opis charakteru naruszenia ochrony danych osobowych oraz określać imię, nazwisko i dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej

rzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz, Warszawa 2018, s. 514–515; W. Chomiczewski, *Komentarz do art. 33*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 714.

[453] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 33.*.., s. 515; W. Chomiczewski, *Komentarz do art. 33.*.., s.. 715.

[454] Zgodnie z art. 33 ust. 1 zd. 1 RODO administrator powinien zgłosić naruszenia ochrony danych osobowych Prezesowi Urzędu w terminie 72 godzin po stwierdzeniu tego naruszenia, które skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Czas zgłoszenia ma jednak względny charakter. W świetle art. 33 ust. 4 RODO informacje te mogą być zgłaszane sukcesywnie, lecz bez zbędnej zwłoki, jeżeli nie można ich udzielić w tym samym czasie. W myśl art. 33 ust. 1 zd. 2 RODO zgłoszenie przekazane Prezesowi Urzędu po upływie 72 godzin od naruszenia powinno obejmować także wyjaśnienie przyczyn opóźnienia.

[455] Artykuł 33 ust. 2 RODO.

[456] Artykuł 33 ust. 2 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 33.*.., s. 514–515.

[457] Artykuł 34 ust. 1 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 34*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 518–519; W. Chomiczewski, *Komentarz do art. 34*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 720–721.

informacji; opis możliwych konsekwencji naruszenia ochrony danych osobowych, a także opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych[458]. Zawiadomienie powinno być przekazane bez zbędnej zwłoki[459]. Obowiązek administratora związany z przekazaniem zawiadomienia ma względny charakter, także w przypadku powstania wysokiego naruszenia praw lub wolności osób fizycznych. Wymóg ten nie dotyczy sytuacji, gdy administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony, takie jak szyfrowanie, a środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, oraz zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą[460]. Administrator nie musi wykonywać tego obowiązku również wówczas, gdy wymagałby on niewspółmiernie dużego wysiłku[461]. Prezes Urzędu może zweryfikować, czy miał miejsce szczególny przypadek wyłączający obowiązek przekazania tego zawiadomienia[462]. Jeżeli Prezes Urzędu stwierdzi, że nie miał miejsce taki przypadek, może on nakazać administratorowi przekazać zawiadomienie o naruszeniu ochrony danych[463].

Środkiem informacyjnym jest też publiczny komunikat lub podobny środek, za pomocą którego administrator może powiadomić osobę, której dane dotyczą, że doszło do naruszenia danych osobowych w sposób mogący spowodować wysokie naruszenie jej praw lub wolności. Admini-

[458] Artykuł 34 ust. 2 w zw. z art. 33 ust. 3 lit. b–d RODO.

[459] Artykuł 34 ust. 1 RODO.

[460] Artykuł 34 ust. 3 lit. a–b RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 34.*.., s. 520–521; W. Chomiczewski, *Komentarz do art. 34.*.., s. 724–725.

[461] Artykuł 34 ust. 3 lit. c zd. 1 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 34.*.., s. 521; W. Chomiczewski, *Komentarz do art. 34.*.., s. 725–726.

[462] Zgodnie z art. 34 ust. 4 RODO Prezes Urzędu może zażądać od administratora lub może stwierdzić, że został spełniony jeden z warunków wyłączenia obowiązku przekazania zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

[463] Artykuł 58 ust. 2 lit. e w zw. z art. 34 ust. 4 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 34.*.., s. 521–522; W. Chomiczewski, *Komentarz do art. 34.*.., s. 726–727.

strator może zastosować ten środek w zastępstwie zawiadomienia osoby, której dane dotyczą, jeżeli zawiadomienie takie wymagałoby niewspółmiernie dużego wysiłku[464].

4. Ocena skutków przetwarzania danych osobowych wraz z konsultacjami z Prezesem Urzędu Ochrony Danych Osobowych

Środkiem ochrony danych, wykonywanym przez administratora lub podmiot przetwarzający wobec planowanego przetwarzania danych, jest ocena skutków ochrony danych oraz konsultacje z Prezesem Urzędu. Ocenę skutków dotyczący planowanych operacji przetwarzania ochrony danych osobowych wykonuje administrator przed rozpoczęciem przetwarzania[465]. Pojedyncza ocena skutków może być wykonana wobec podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem[466]. Ocena skutków oznacza analizę ryzyka połączoną ze wskazaniem działań, które mogą wykluczyć powstanie naruszeń ochrony danych[467].

Ocena skutków jest wymagana, jeżeli przetwarzanie będzie mogło spowodować wysokie ryzyko naruszenia praw lub wolności osób fi-

[464] Artykuł 34 ust. 3 lit. c RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 34.…*, s. 521.

[465] Artykuł 35 ust. 1 zd. 1 RODO. Zob. A. Stępień, P. Biały, *op. cit*., s. 34; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 35*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 531; K. Witkowska-Nowakowska*, Komentarz do art. 35*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 738.

[466] Artykuł 35 ust. 1 zd. 2 RODO. W świetle motywu 92 RODO pojedyncza ocena skutków może nastąpić szczególnie, gdy grupa administratorów lub podmiotów przetwarzających zamierza stworzyć wspólną aplikację, platformę lub środowisko przetwarzania. Jak słusznie podkreślają P. Litwiński, P. Barta oraz M. Kawecki, obowiązek prowadzenia oceny skutków powinien być określony każdorazowo dla konkretnej operacji przetwarzania danych. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 35...*, s. 526.

[467] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 35...*, s. 529; K. Witkowska-Nowakowska*, Komentarz do art. 35...*, s. 737.

zycznych, ze względu na charakter, zakres, kontekst i cele przetwarzania oraz źródła ryzyka[468]. Przetwarzanie powinno odbywać się zgodnie z oceną skutków[469]. Obowiązek przeprowadzenia oceny skutków ma miejsce w szczególności, gdy dotyczy: zautomatyzowanej, systematycznej i kompleksowej oceny czynników związanych z osobą fizyczną, obejmującą np. profilowanie, oraz stanowiącą podstawę decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych oraz systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie[470]. Ocena skutków jest zatem z zasady związana z przetwarzaniem danych osobowych z użyciem nowych technologii[471]. Jednakże przetwarzanie innymi metodami także może wymagać przeprowadzenia oceny skutków[472].

W celu ułatwienia administratorowi ustalenia, czy w jego przypadku konieczne jest przeprowadzenie oceny skutków, Prezes Urzędu ma obowiązek określić i ogłosić w komunikacie wykaz rodzajów operacji prze-

[468] Artykuł 35 ust. 1 RODO; motyw 90 zd. 1 RODO. W świetle motywu 90 zd. 1 w zw. z motywem 89 zd. 3 RODO ocena skutków ma na celu analizę prawdopodobieństwa i powagi ryzyka naruszenia praw i wolności osoby fizycznej w związku z przetwarzaniem danych, które jej dotyczą. Zob. A. Stępień, P. Biały, *op. cit*., s. 34. Jak słusznie podkreślają P. Naklicka oraz A. Gawron, ocena skutków przetwarzania danych stanowi sformalizowaną analizę ryzyka, podejmowaną w przypadkach, gdy wstępnie określono, że będzie miało miejsce wysokie ryzyko w związku z przetwarzaniem danych. Zob. P. Naklicka, A. Gawron, *Rodosłowniczek, czyli omówienie podstawowych pojęć RODO wraz z przykładami*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018, s. 55.

[469] W świetle art. 35 ust. 11 RODO administrator danych powinien przeprowadzić przegląd w celu sprawdzenia zgodności przetwarzania z oceną skutków. Zgodnie z tym przepisem przegląd powinien mieć miejsce, przynajmniej gdy nastąpi zmiana ryzyka wynikającego z operacji przetworzenia.

[470] Artykuł 35 ust. 3 RODO, motyw 91 RODO. Zob. A. Stępień, P. Biały, *op. cit*., s. 34–35.

[471] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 35...*, s. 526.

[472] Zdaniem K. Witkowskiej-Nowakowskiej przepisy prawa dotyczące oceny skutków są neutralne technologicznie. K. Witkowska-Nowakowska, *Komentarz do art. 35...*, s. 730.

twarzania danych osobowych wymagających oceny skutków[473] oraz wykaz rodzajów operacji przetwarzania danych osobowych niewymagających oceny skutków[474]. Komunikaty te są publikowane w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski"[475].

Administrator, wykonując ocenę skutków, konsultuje się z inspektorem ochrony danych, jeżeli wcześniej go wyznaczył[476], oraz zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania[477].

Administrator powinien opisać w ocenie skutków przetwarzanie poprzez wskazanie: systematycznego opisu planowanych operacji przetwarzania, celów przetwarzania oraz prawnie uzasadnionych interesów realizowanych przez administratora; oceny niezbędności i proporcjonalności operacji przetwarzania w stosunku do jego celów; oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą[478]. W ocenie skutków administrator powinien także wskazać środki planowane w celu zaradzenia ryzyku obejmujące zabezpieczenia, a także środki i mechanizmy bezpieczeństwa zapewniające minimalizację tego ryzyka oraz ochronę danych osobowych w sposób zgodny z przepisami rozporządze-

[473] Artykuł 54 ust. 1 pkt 1 u.o.d.o. w zw. z art. 35 ust. 4 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 35*..., s. 536–537; K. Witkowska-Nowakowska, *Komentarz do art. 35*..., s. 742.

[474] Artykuł 54 ust. 1 pkt 2 u.o.d.o. w zw. z art. 35 ust. 5 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 35*..., s. 537–538; K. Witkowska-Nowakowska, *Komentarz do art. 35*..., s. 743.

[475] Artykuł 54 ust. 2 u.o.d.o. W świetle art. 35 ust. 4 zd. 2 oraz art. 35 ust. 5 zd. 2 RODO Prezes Urzędu przekazuje te wykazy Europejskiej Radzie Ochrony Danych.

[476] Artykuł 35 ust. 2 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 35*..., s. 534. W świetle art. 39 ust. 1 lit. c RODO inspektor ochrony danych na żądanie administratora ma obowiązek udzielić zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania. Jak słusznie wskazują A. Stępień oraz P. Biały, znaczenie inspektora ochrony danych w związku z oceną skutków ma minimalny charakter. A. Stępień, P. Biały, *op. cit*., s. 34.

[477] W świetle art. 35 ust. 9 RODO administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, w sposób nienaruszający interesów handlowych lub interesów publicznych lub bezpieczeństwa operacji przetwarzania. Zob. K. Witkowska-Nowakowska, *Komentarz do art. 35*..., s. 752–753.

[478] Artykuł 35 ust. 7 lit. a–c RODO. Zob. więcej A. Stępień, P. Biały, *op. cit*., s. 35.

nia 2016/679. Środki te powinny uwzględniać prawa i prawnie uzasadnione interesy osób, których dane dotyczą, i innych osób, których sprawa dotyczy[479]. Ocena skutków powinna uwzględniać też przestrzeganie zatwierdzonego kodeksu postępowania, jeśli kodeks ten ma w tym przypadku zastosowanie[480].

Konsekwencją oceny skutków może być powstanie obowiązku administratora do konsultacji z Prezesem Urzędu, jeżeli ocena skutków wykaże, że przetwarzanie spowodowałoby powstanie wysokiego ryzyka, gdyby administrator nie zastosował w celu jego zminimalizowania środków ponadstandardowych z punktu widzenia dostępnych technologii i kosztów wdrożenia[481]. Ryzyko takie może być spowodowane rodzajem, zakresem lub częstotliwością przetwarzania, które skutkują w konsekwencji powstaniem szkody lub ingerencją w prawa i wolności osoby fizycznej[482].

Konsultacje powinny nastąpić przed rozpoczęciem przetwarzania[483], na wniosek administratora[484]. Wniosek powinien spełniać wymogi podania określone w Kodeksie postępowania administracyjnego, w tym określać wskazanie wnioskodawcy, jego adres i żądanie[485], a także wymogi formy wniesienia podania[486].

Administrator we wniosku o przeprowadzenie konsultacji powinien przedstawić Prezesowi Urzędu informacje o planowanym przetwarzaniu,

[479] Artykuł 35 ust. 7 lit. d RODO, motyw 90 zd. 2 RODO.

[480] Artykuł 35 ust. 8 RODO.

[481] Artykuł 36 ust. 1 RODO, motyw 94 zd. 1 RODO. Zob. A. Stępień, P. Biały, *op. cit*., s. 36; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 36*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 549; K. Witkowska-Nowakowska, *Komentarz do art. 36*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 758.

[482] Motyw 94 zd. 2 RODO.

[483] Artykuł 36 ust. 1 RODO.

[484] Artykuł 57 ust. 1 u.o.d.o., motyw 94 zd. 3 RODO.

[485] Artykuł 63 § 2 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2017 r., poz. 1257 ze zm.), dalej k.p.a.

[486] Artykuł 63 § 1, 3–3b k.p.a.

obejmujące określenie: obowiązków administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu; celów i sposobów zamierzonego przetwarzania; środków i zabezpieczeń mających chronić prawa i wolności osób, których dane dotyczą; danych kontaktowych inspektora ochrony danych; oceny skutków dla ochrony danych oraz wszelkie inne informacje, których zażąda od niego Prezes Urzędu[487]. Jeżeli wniosek ten nie spełnia tych kryteriów, Prezes Urzędu informuje administratora o nieudzieleniu konsultacji oraz wskazuje przyczyny ich nieudzielenia[488].

Prezes Urzędu w związku z konsultacjami może udzielić administratorowi lub podmiotowi przetwarzającemu pisemnego zalecenia lub może zastosować środek nadzoru, jeżeli przetwarzanie skutkowałoby naruszeniem rozporządzenia 2016/679, a administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko[489]. Prezes Urzędu udziela zalecenia lub stosuje środek nadzoru w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje, który może być przedłużony o sześć tygodni ze względu na złożony charakter zamierzonego przetwarzania[490].

Administrator jest obowiązany przestrzegać zaleceń określonych w ocenie skutków oraz w konsultacjach z Prezesem Urzędu. Jeżeli ustanowiony został podmiot przetwarzający, powinien on pomagać admiratorowi w wykonaniu tych obowiązków[491]. Zalecenia nie wyłączają prawa administratora do samodzielnego określenia stosowanych środków technicznych i organizacyjnych. Z samodzielnością administratora jest jed-

[487] Artykuł 36 ust. 3 RODO; motyw 94 zd. 5 RODO. Zob. A. Stępień, P. Biały, *op. cit.*, s. 36; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 36*..., s. 550–551.

[488] Artykuł 57 ust. 3 u.o.d.o.

[489] Artykuł 36 ust. 2 zd. 1 RODO.

[490] Artykuł 36 ust. 2 zd. 1–2 RODO. W myśl art. 36 ust. 2 zd. 3 RODO Prezes Urzędu powinien poinformować administratora lub podmiot przetwarzający o przedłużeniu tego terminu oraz podać przyczyny tego opóźnienia. Zgodnie z art. 36 ust. 2 zd. 4 RODO bieg tego terminu może być zawieszony do czasu, gdy Prezes Urzędu uzyska wszelkie informacje, których zażądał do celów konsultacji. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 36*..., s. 552.

[491] Motyw 95 RODO.

nak związana jego odpowiedzialność za zapewnienie prawidłowej ochrony danych w procesie ich przetwarzania[492].

5. Rejestrowanie czynności przetwarzania

Środkami prawnymi *sensu largo* o charakterze pośrednim, umożliwiającymi Prezesowi Urzędu kontrolę procesu przetwarzania, są rejestr czynności przetwarzania danych osobowych prowadzony przez administratora lub jego przedstawiciela oraz rejestr wszystkich kategorii czynności przetwarzania prowadzony przez podmiot przetwarzający lub jego przedstawiciela[493]. Prowadzenie rejestrów ma umożliwić administratorowi wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z przepisami prawa, w zgodzie z zasadą rozliczalności[494].

Prowadzenie rejestrów jest obowiązkowe, gdy: administrator zatrudnia minimum 250 osób; przetwarzanie może powodować ryzyko naruszenia praw i wolności osób, które ich dotyczą; przetwarzanie nie ma charakteru sporadycznego; przetwarzanie obejmuje dane wrażliwe lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych[495]. Rejestry dotyczące przetwarzania danych osobowych mogą być prowadzone

[492] A. Stępień, P. Biały, *op. cit*., s. 35.

[493] Artykuł 30 ust. 1–2 RODO; motyw 82 zd. 1 RODO. Zob. więcej P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 30*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 492–493, 497–498; D. Lubasz, *Komentarz do art. 30*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 678.

[494] D. Lubasz, *Komentarz do art. 30*..., s. 663; P. Naklicka, A. Gawron, *op. cit*., s. 61–62; K. Kloc, *Rejestrowanie czynności przetwarzania danych*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018, s. 137.

[495] Artykuł 30 ust. 5 RODO. W świetle motywu 13 zd. 3 RODO wyłączenie obowiązku prowadzenia rejestru czynności przetwarzania wobec podmiotów zatrudniających mniej niż 250 pracowników jest spowodowane uwzględnieniem szczególnej sytuacji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

w formie pisemnej lub elektronicznej[496]. Powinny być udostępnione Prezesowi Urzędu na jego żądanie w celu umożliwienia temu organowi monitorowania operacji przetwarzania, prowadzonych odpowiednio przez administratora oraz podmiot przetwarzający[497].

Przepisy prawa częściowo różnicują zakres informacji, które rejestry powinny zawierać, w zależności od podmiotu, który je prowadzi. Rejestr zawiera bowiem informacje o czynnościach przetwarzania, za które każdy z tych podmiotów jest odpowiedzialny[498]. W rejestrze prowadzonym zarówno przez administratora, jak i podmiot przetwarzający, zamieszcza się: imię i nazwisko lub nazwę oraz dane kontaktowe odpowiednio administratora lub wszystkich współadministratorów podmiotu przetwarzającego lub podmiotów przetwarzających; przedstawiciela administratora lub podmiotu przetwarzającego; inspektora ochrony danych[499]; jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa[500]; a gdy ma to zastosowanie, informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej[501]. Rejestr czynności przetwarzania danych osobowych prowadzony przez administratora powinien zawierać także: cele przetwarzania; opis kategorii osób, których dane dotyczą; opis kategorii danych osobowych; kategorie odbiorców danych osobowych; a jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych[502]. Rejestr prowadzony przez

[496] Art. 30 ust. 3 RODO. Zob. więcej P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 30...*, s. 496–497; D. Lubasz, *Komentarz do art. 30...*, s. 676–678; K. Kloc, *op. cit.*, s. 147.

[497] Artykuł 30 ust. 4 RODO; motyw 82 zd. 2 RODO.

[498] Motyw 82 zd. 1 RODO. Zob. D. Lubasz, *Komentarz do art. 30...*, s. 674.

[499] Artykuły 30 ust. 1 lit. a oraz art. 30 ust. 2 lit. a RODO. Zob. D. Lubasz, *Komentarz do art. 30...*, s. 668–669.

[500] Artykuły 30 ust. 1 lit. g oraz art. 30 ust. 2 lit. d RODO. D. Lubasz, *Komentarz do art. 30...*, s. 673.

[501] Artykuły 30 ust. 1 lit. e oraz art. 30 ust. 2 lit. c RODO.

[502] Artykuł 30 ust. 1 lit. b–d, f RODO. Zob. D. Lubasz, *Komentarz do art. 30...*, s. 669–671, 672.

podmiot przetwarzający powinien zawierać także kategorie przetwarzań dokonywanych w imieniu każdego z administratorów[503].

6. Certyfikat

Środkiem prawnym *sensu largo* o charakterze pośrednim jest także certyfikat świadczący, że operacje przetwarzania prowadzone przez administratora lub podmiot przetwarzający są zgodne z przepisami rozporządzenia 2016/679[504]. Certyfikat stanowi gwarancję, że wdrożono odpowiednie środki techniczne i organizacyjne zapewniające wykonanie wymogów określonych w tym rozporządzeniu[505]. Wydanie certyfikatu nie wpływa na zmianę praw i obowiązków tych podmiotów związanych z przetwarzaniem danych osobowych, a także nie wpływa na zakres zadań i uprawnień Prezesa Urzędu Ochrony Danych Osobowych[506].

Certyfikacja ma dobrowolny charakter[507]. Prezes Urzędu Ochrony Danych Osobowych lub podmiot certyfikujący dokonują jej na wniosek administratora, podmiotu przetwarzającego, producenta albo podmiotu wprowadzającego usługę lub produkt na rynek[508]. Podmioty te składają wniosek o certyfikację, w formie papierowej lub elektronicznej, który obejmuje informacje o nich i ich działalności oraz potwierdza spełnienie kryteriów cer-

[503] Artykuł 30 ust. 2 lit. b RODO.

[504] Artykuł 42 ust. 1 zd. 1 RODO.

[505] Artykuły 28 ust. 5 w zw. z art. 28 ust. 1 oraz art. 28 ust. 4 RODO. W świetle motywu 100 RODO mechanizm certyfikacji ma na celu zwiększenie przejrzystości i poprawy przestrzegania rozporządzenia 2016/679, a w konsekwencji umożliwienia szybkości oceny stopnia ochrony danych. Zob. P. Makowski, P. Drobek, *Komentarz do art. 42*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 840.

[506] Artykuł 42 ust. 4 RODO.

[507] Artykuł 42 ust. 3 RODO. Zob. A. Krasuski, *Ochrona danych osobowych…*, s. 307; P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 42*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 612; P. Makowski, P. Drobek, *Komentarz do art. 42…,* s. 842–843.

[508] Artykuł 15 ust. 1 u.o.d.o.

tyfikacji[509]. Wniosek powinien zawierać także dokumenty potwierdzające spełnienie kryteriów certyfikacji albo ich kopie, a jeżeli certyfikacji dokonuje Prezes Urzędu, wnioskodawca powinien przedstawić również dowód wniesienia opłaty za czynności związane z certyfikacją[510].

Proces certyfikacji powinien trwać nie dłużej niż 3 miesiące od dnia złożenia wniosku o wydanie certyfikatu[511]. Proces certyfikacji prowadzi Prezes Urzędu albo podmiot certyfikujący[512]. Jeżeli proces ten prowadzi podmiot certyfikujący, ponosi on odpowiedzialność za podjęcie właściwej oceny w stosunku do wnioskodawcy, przed udzieleniem certyfikacji[513].

Prezes Urzędu pozostawia bez rozpoznania wniosek niezawierający danych podmiotu ubiegającego się o certyfikację[514], a wzywa do uzupełnienia wniosku, jeżeli nie zawiera on: informacji potwierdzających spełnienie kryteriów certyfikacji, wskazania zakresu wnioskowanej certyfikacji[515], dokumentów lub ich kopii potwierdzających spełnienie kryteriów certyfikacji, dowodu wniesienia opłaty za czynności związane z certyfikacją lub odpowiednią formę[516]. Skutkiem nieuzupełnienia wniosku w ter-

[509] Zgodnie z art. 17 ust. 1 u.o.d.o. podmiot wnioskujący o certyfikację powinien złożyć wniosek zawierający nazwę podmiotu ubiegającego się o certyfikację albo jego imię i nazwisko oraz wskazanie adresu jego siedziby, adresu miejsca prowadzenia działalności gospodarczej albo adresu zamieszkania; informacje potwierdzające spełnianie kryteriów certyfikacji; wskazanie zakresu wnioskowanej certyfikacji. W świetle art. 17 ust. 3 u.o.d.o. wniosek o certyfikację może być złożony pisemnie w postaci papierowej opatrzonej własnoręcznym podpisem albo w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a jeżeli wniosek kieruje się do Prezesa Urzędu Ochrony Danych Osobowych może być także złożony w postaci elektronicznej opatrzony podpisem potwierdzonym profilem zaufanym ePUAP.

[510] Artykuł 17 ust. 2 w zw. z art. 26 u.o.d.o.

[511] Artykuł 18 ust. 1 u.o.d.o.

[512] Zgodnie z art. 15 ust. 1 u.o.d.o. oraz art. 42 ust. 5 RODO certyfikacji dokonuje Prezes Urzędu lub podmiot certyfikujący.

[513] Artykuł 43 ust. 4 zd. 1 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 43*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz,* Warszawa 2018, s. 617; P. Makowski, P. Drobek, K. Witkowska-Nowakowska, *op. cit.*, s. 854.

[514] Artykuł 18 ust. 2 w zw. z art. 17 ust. 1 pkt 1 u.o.d.o.

[515] Artykuł 18 ust. 2 w zw. z art. 17 ust. 1 pkt 2-3 u.o.d.o.

[516] Artykuł 18 ust. 2 w zw. z art. 17 ust. 2-3 u.o.d.o.

minie 7 dni od dnia doręczenia wezwania jest pozostawienie wniosku bez rozpoznania[517].

Proces certyfikacji prowadzony przez Prezesa Urzędu jest odpłatny. Prezes Urzędu podbiera opłatę za czynności związane z certyfikacją, która stanowi dochód budżetu państwa[518]. Wysokość opłaty powinna odpowiadać przewidywalnym kosztom poniesionym z tytułu wykonywania czynności związanych z certyfikacją, przy czym określając jej wysokość, pod uwagę powinny być brane: zakres certyfikacji, przewidywany przebieg i długość postępowania certyfikującego oraz koszt pracy pracownika wykonującego czynności związane z certyfikacją[519].

Prezes Urzędu, jeżeli przeprowadza proces certyfikacji, jest uprawniony do przeprowadzenia czynności sprawdzających u wnioskodawcy w celu oceny, czy spełnia on kryteria certyfikacji[520]. Czynności te mogą być wykonane po zawiadomieniu o nich wnioskodawcy[521]. Kryteria certyfikacji, które powinien przestrzegać wnioskodawca, są zatwierdzane przez Prezesa Urzędu oraz Europejską Radę Ochrony Danych, a następnie są one udostępnione na stronie podmiotowej Prezesa Urzędu w Biuletynie Informacji Publicznej[522].

Pozytywne zakończenie procesu certyfikacji ma miejsce w przypadku wydania certyfikatu. Jest on dokumentem potwierdzającym certyfikację[523], zawierającym informacje dotyczące podmiotów procesu certyfikacji (wnioskodawcy oraz podmiotu certyfikującego lub Prezesa Urzędu), zakresu obo-

[517] Artykuł 18 ust. 2 u.o.d.o.

[518] Artykuł 26 ust. 1 w zw. z art. 26 ust. 5 u.o.d.o.

[519] Artykuł 26 ust. 1 w zw. z art. 26 ust. 2 u.o.d.o.

[520] Artykuł 24 ust. 1 u.o.d.o.

[521] Artykuł 24 ust. 2 u.o.d.o.

[522] Artykuł 16 u.o.d.o. w zw z art. 42 ust. 5 RODO. W świetle art. 43 ust. 6 zd. 1-2 w zw. z art. 42 ust. 5 RODO, Prezes Urzędu powinien podać w łatwo dostępny sposób do publicznej wiadomości kryteria certyfikacji, oraz przekazać je Europejskiej Radzie Ochrony Danych.

[523] Artykuł 21 ust. 1 u.o.d.o.

wiązywania certyfikatu oraz informacje o certyfikacie[524]. Jeżeli certyfikację wykonuje podmiot certyfikujący, o zamiarze jej dokonania informuje Prezesa Urzędu[525]. Podmiot certyfikujący lub Prezes Urzędu zawiadamia wnioskodawcę o dokonaniu certyfikacji[526]. Jeżeli certyfikacji dokonuje podmiot certyfikujący, powinien on przekazać Prezesowi Urzędu dane podmiotu, któremu udzielono certyfikacji[527]. Prezes Urzędu powinien wpisać do wykazu udostępnionego na swojej stronie podmiotowej w BIP podmiot, który otrzymał certyfikację. Wpis, który ma informacyjny charakter, powinien być wprowadzony niezwłocznie po dokonaniu certyfikacji albo otrzymaniu od podmiotu certyfikującego informacji o dokonaniu certyfikacji[528].

Proces certyfikacji kończy się negatywnie odmową wydania certyfikatu, jeżeli podmiot certyfikujący lub Prezes Urzędu stwierdzi, że wnioskodawca nie spełnia kryteriów certyfikacji[529]. Prezes Urzędu odmawia certyfikacji w drodze decyzji administracyjnej[530]. Podmiot certyfikujący odmawia certyfikacji w drodze czynności materialno-technicznej, a wcześniej informuje Prezesa Urzędu o planowanej odmowie[531]. Pod-

[524] W myśl art. 21 ust. 2 u.o.d.o., certyfikat powinien zawierać co najmniej: oznaczenie podmiotu, który otrzymał certyfikat; nazwę podmiotu dokonującego certyfikacji oraz wskazanie adresu jego siedziby; numer lub oznaczenie certyfikatu; zakres, w tym okres, na jaki została dokonana certyfikacja; datę wydania i podpis podmiotu dokonującego certyfikacji lub osoby przez niego upoważnionej.

[525] Artykuł 19 u.o.d.o.

[526] Artykuł 18 ust. 1 u.o.d.o.

[527] Artykuły 23 ust. 1 u.o.d.o. oraz art. 43 ust. 5 RODO.

[528] Artykuł 23 ust. 2–4. u.o.d.o. Na informacyjny charakter wpisu do wykazu podmiotów, którym udzielono certyfikacji oraz cofnięto certyfikację, wskazuje treść przepisów u.o.d.o. dotyczących wydania i cofnięcia certyfikatu. Wydanie oraz cofnięcie certyfikatu stanowi o powstaniu lub wyeliminowaniu jednostkowego i konkretnego domniemania, że administrator lub podmiot przetwarzający wykonuje operacje przetwarzania w sposób zgodny z przepisami RODO.

[529] Artykuł 20 ust. 1 u.o.d.o.

[530] Artykuł 20 ust. 2 u.o.d.o.

[531] Artykuł 19 u.o.d.o. Na formę czynności materialno-technicznej odmowy certyfikacji przez podmiot certyfikujący świadczy wykładnia *a contrario* art. 20 ust. 2 u.o.d.o. Przepis ten wyraźnie wskazuje, że Prezes Urzędu odmawia dokonania certyfikacji w drodze decyzji. Przepisy prawa nie wskazują jednocześnie na formę certyfikacji dokonanej przez podmiot certyfikujący, stąd wydaje się, że decyzja administracyjna jako odmowa dokonania certyfikacji jest właściwa jedynie dla działania Prezesa Urzędu. Należy także podkreślić, że podmiot certyfi-

miot certyfikujący lub Prezes Urzędu w zależności, który z tych podmiotów prowadzi proces certyfikacji, zawiadamia wnioskodawcę o odmowie dokonania certyfikacji[532].

Przepisy prawa nakładają na podmiot certyfikujący obowiązek przekazania informacji Prezesowi Urzędu o sposobie zakończenia procesu certyfikacji, tak aby mógł on w razie potrzeby zastosować środki nadzoru wobec wnioskodawcy, które obejmują: nakazanie podmiotowi certyfikującemu cofnięcie certyfikacji lub nakazanie mu nieudzielenia certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane[533].

Podmiot, który otrzymał certyfikat, powinien spełniać kryteria certyfikacji obowiązujące na dzień wydania certyfikatu przez cały okres jego ważności[534]. Podmiot certyfikujący oraz Prezes Urzędu sprawują nadzór nad działalnością związaną z certyfikatem[535]. Prezes Urzędu jest uprawniony, po dokonaniu certyfikacji, do przeprowadzenia czynności sprawdzających u podmiotu, który otrzymał certyfikat, czy nadal spełnia on kryteria certyfikacji[536]. Czynności te mogą być wykonane po zawiadomieniu o nich tego podmiotu[537].

Jeżeli podmiot certyfikujący lub Prezes Urzędu stwierdzi, że podmiot, któremu udzielono certyfikacji, nie spełnia lub przestał spełniać kryteria certyfikacji, cofa certyfikację[538]. Prezes Urzędu cofa certyfikację

kujący jest podmiotem prawa prywatnego, realizującym sprywatyzowane zadania publiczne, dlatego nadanie temu podmiotowi kompetencji do wydania decyzji administracyjnej powinno być wyraźnie wyartykułowane w treści przepisów prawa.

[532] Artykuł 18 ust. 1 u.o.d.o.

[533] Artykuł 43 ust. 1 w zw. z art. 58 ust. 2 lit. h RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 42*..., s. 612–613.

[534] Artykuł 22 ust. 1 u.o.d.o.

[535] Zgodnie z art. 58 ust. 1 lit. c RODO Prezes Urzędu przeprowadza przegląd udzielonych certyfikacja. W świetle art. 42 ust. 7 zd. 2 RODO podmiot certyfikujący oraz Prezes Urzędu powinni cofnąć certyfikację, jeżeli nie zostały spełnione lub przestały być spełniane jej kryteria.

[536] Artykuł 24 ust. 1 u.o.d.o.

[537] Artykuł 24 ust. 2 u.o.d.o.

[538] Artykuł 22 ust. 2 u.o.d.o.

w drodze decyzji administracyjnej[539]. Podmiot certyfikujący ma obowiązek przekazać Prezesowi Urzędu dane podmiotu, któremu cofnął certyfikację, wraz ze wskazaniem przyczyny tego cofnięcia[540]. Należy zaznaczyć, że podmiot certyfikujący jest odpowiedzialny za podjęcie właściwej oceny, której skutkiem było cofnięcie certyfikacji[541].

7. Wiążące reguły korporacyjne

Wiążące reguły korporacyjne są środkami prawnymi *sensu largo* o charakterze pośrednim mającym zrekompensować niski stopień ochrony danych w państwach trzecich, w których występuje część czynności procesu przetwarzania[542]. Stanowią one szczególnego rodzaju politykę ochrony danych, obowiązującą w związku z procesem przetwarzania zachodzącym w państwie trzecim lub organizacji międzynarodowej[543]. Reguły te stanowią gwarancję przestrzegania wymagań w celu ochrony danych przez administratora oraz podmiot przetwarzający, pomimo że przewarzanie danych odbywa się w państwie trzecim lub organizacji międzynarodowej, które nie zapewniają odpowiedniego środka ochrony danych[544].

Powinny one być zatwierdzone przez Prezesa Urzędu. Reguły te obejmują członków grupy przedsiębiorstw lub przedsiębiorców, którzy prowadzą wspólną działalność gospodarczą, oraz ich pracowników. Powinny być wiążące oraz mieć zastosowanie dla każdego z tych podmio-

[539] Artykuł 22 ust. 3 u.o.d.o.

[540] Artykuły 23 ust. 1 u.o.d.o. oraz art. 43 ust. 5 RODO.

[541] Artykuł 43 ust. 4 zd. 1 RODO.

[542] Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 47*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 648.

[543] W świetle art. 4 pkt 20 RODO wiążące reguły korporacyjne powinny być stosowane, gdy administrator lub podmiot przetwarzający posiada jednostkę organizacyjną na terytorium państwa członkowskiego, lecz zachodzi jednorazowe lub wielokrotne przekazanie danych osobowych administratorowi lub podmiotowi przetwarzającemu, będącemu członkiem grupy przedsiębiorstw, a położonego w państwie trzecim.

[544] Motyw 107 zd. 1–2; motyw 108 zd. 1–2 RODO.

tów, i być przez każdego z nich egzekwowane[545]. Mają one charakter wewnętrzny lub prywatnoprawny[546]. Wiążące reguły korporacyjne powinny także w sposób wyraźny przyznać osobom, których dane dotyczą, egzekwowalne prawa związane z ich przetwarzaniem[547].

Wiążące reguły korporacyjne powinny zawierać: strukturę i dane kontaktowe; opis przekazywania danych, w tym kategorii danych osobowych, rodzaj przetwarzania i jego celów, rodzajów osób, których dane dotyczą, oraz nazw danego państwa trzeciego; określenie, zakresu związania reguł; zastosowania ogólnych zasad ochrony danych; praw osób, których dane dotyczą, w związku z przetwarzaniem oraz sposoby wykonywania tych praw; przyjęcie przez administratora lub podmiot przetwarzający, mających jednostki organizacyjnej na terytorium państwa członkowskiego, odpowiedzialności prawnej za naruszenie wiążących reguł korporacyjnych; sposób, w jaki osobom, których dane dotyczą, podaje się informacje o wiążących regułach korporacyjnych; zadania inspektora ochrony danych lub innej osoby, lub podmiotu, odpowiedzialnych za monitorowanie przestrzegania wiążących reguł korporacyjnych oraz monitorowanie szkoleń i rozpatrywanie skarg; procedury dotyczące skarg; stosowane mechanizmy zapewniające weryfikację przestrzegania wiążących reguł korporacyjnych; mechanizmy zgłaszania i rejestrowania zmian w zasadach i zgłaszania tych zmian organowi nadzorczemu; mechanizm współpracy z organem nadzorczym; mechanizm zgłaszania właściwemu organowi nadzorczemu wszelkich wymogów prawnych, którym podlega w państwie trzecim; właściwe szkolenia z zakresu ochrony danych dla personelu mającego stały lub regularny dostęp do danych osobowych[548].

[545] Artykuł 47 ust. 1 lit. a RODO; motyw 110 RODO. Zob. P. Drobek, *Komentarz do art. 47*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 881–882.

[546] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 47...*, s. 648–649.

[547] Artykuł 47 ust. 1 lit. b RODO.

[548] Artykuł 47 ust.1 lit. c w zw. z art. 47 ust. 2 RODO.

8. Kodeks postępowania

Kolejnym środkiem prawnym ochrony danych osobowych *sensu largo* o charakterze pośrednim jest kodeks postępowania, stanowiący zespół norm prawnych opracowanych przez zrzeszenie lub inne podmioty reprezentujące administratora lub podmioty przetwarzające, zatwierdzony przez organ właściwy ze względu na zakres zastosowania tego kodeksu.

Kodeks ma na celu zapewnienie stosowania rozporządzenia 2016/679, z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw[549]. Jednocześnie należy zaznaczyć, że ma on dobrowolny charakter[550]. Administrator, stosując zatwierdzony kodeks postępowania, może w ten sposób wykazać, że wywiązuje się ze swoich obowiązków określonych w tym rozporządzeniu[551]. Kodeks nie ma tylko wizerunkowego znaczenia, lecz może służyć rozstrzyganiu sporów, a także zawiera egzekwowalne normy[552]. Kodeks postępowań może zostać opracowany przez zrzeszenie i inne podmioty reprezentujące administratorów lub podmioty przetwarzające[553]. Kodeks może także obowiązywać administratorów i podmioty przetwarzające z państw trzecich lub organizacji międzynarodowych na podstawie umowy lub innego wiążącego instrumentu[554].

Kodeks ma na celu doprecyzować rozporządzenie 2016/679[555]. Powinien uwzględnić przy tym dotychczasowe dobre praktyki przetwarza-

[549] Artykuł 40 ust. 1 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 40*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Warszawa 2018, s. 597; U. Góral, P. Makowski, *Komentarz do art. 40*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 822–823.

[550] U. Góral, P. Makowski, *op. cit.*, s. 823.

[551] Motyw 81 zd. 2 RODO.

[552] U. Góral, P. Makowski, *op. cit.*, s. 820.

[553] Art. 40 ust. 2 RODO.

[554] Art. 40 ust. 3 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 40...*, s. 599–600.

[555] Art. 40 ust. 2 RODO.

nia danych osobowych[556] oraz, w szczególności, dopasować obowiązki administratorów i podmiotów przetwarzających do ryzyka naruszenia praw lub wolności osób fizycznych, jakie może powodować przetwarzanie[557]. Z tej przyczyny reguluje on: sposób rzetelnego i przejrzystego przetwarzania; określenie prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach; sposób zbierania danych osobowych; pseudonimizację danych osobowych; sposób informowania opinii publicznej i osób, których dane dotyczą; sposób wykonywania przez osoby, których dane dotyczą, przysługujących im praw; sposób informowania i ochrony dzieci oraz sposób pozyskiwania zgody osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem; środki i procedury, do których wykonania jest zobowiązany administrator; środki zapewniające bezpieczeństwo przetwarzania; sposób zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą; sposób przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych; postępowania pozasądowe oraz inne tryby rozstrzygania sporów w celu rozstrzygania sporów między administratorami a osobami, których dane dotyczą[558]. Kodeks może zawierać także wskazówki co do wdrożenia odpowiednich środków służących przestrzeganiu prawa ochrony danych oraz sposobu wykazania przestrzegania prawa przez administratora i podmiot przetwarzający[559].

Zrzeszenie lub inny podmiot reprezentujący administratorów lub podmioty przetwarzające, mający zamiar opracować kodeks postępowania, powinien przedłożyć projekt kodeksu Prezesowi Urzędu w celu jego

[556] P. Punda, A.P. Czarnowski, M. Gawroński, *Kodeksy postępowania i certyfikacja*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018, s. 165.

[557] Motyw 98 zd. 2 RODO.

[558] Artykuł 40 ust. 2 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 40...*, s. 598–599.

[559] Motyw 77 RODO.

zatwierdzenia[560]. Organ nadzorczy wydaje opinię o zgodności projektu kodeksu z rozporządzeniem 2016/679 i zatwierdza go, jeżeli uzna, że stanowi on odpowiednie zabezpieczenia[561]. Odmienna procedura występuje, gdy kodeks będzie dotyczył czynności przetwarzania prowadzonych w kilku państwach członkowskich. Prezes Urzędu powinien wówczas zwrócić się o opinię do Europejskiej Rady Ochrony Danych. Opinia ta dotyczy zgodności projektu kodeksu z rozporządzeniem 2016/679, a jeżeli ma on obowiązywać także administratorów lub podmioty przetwarzające z państw trzecich i organizacji międzynarodowych, opinia powinna określać, czy projekt kodeksu stanowi odpowiednie zabezpieczenia[562]. Europejska Rada Ochrony Danych po wyrażeniu pozytywnej opinii przedkłada ją Komisji Europejskiej[563]. Komisja może, w drodze aktu wykonawczego, stwierdzić, że zatwierdzony kodeks postępowania jest powszechnie obowiązujący w Unii Europejskiej[564], a następnie zapewnić odpowiednie upowszechnienie zatwierdzonego kodeksu[565]. Procedura ta obwiązuje także w przypadku zmiany i rozszerzenia tego kodeksu[566].

Przestrzeganie kodeksu przez obowiązanych do jego stosowania administratorów lub podmiotów przetwarzających powinno być monitorowane przez podmiot monitorujący, który został akredytowany w tym celu przez właściwy organ nadzorczy[567]. Jeżeli administrator lub podmiot

[560] Artykuł 40 ust. 5 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 40…*, s. 600–601; U. Góral, P. Makowski, *op. cit*., s. 829; P. Punda, A.P. Czarnowski, M. Gawroński, *op. cit*., s. 165.

[561] Artykuł 40 ust. 5 zd. 2 RODO.

[562] Artykuł 40 ust. 7 w zw. z art. 40 ust. 3 RODO.

[563] Artykuł 40 ust. 8 RODO.

[564] Artykuł 40 ust. 9 zd. 1 RODO.

[565] Artykuł 40 ust. 10 RODO. W świetle art. 40 ust. 11 RODO Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie zatwierdzone kodeksy podstępowania, zmiany i rozszerzenia i udostępnia je opinii publicznej za pomocą odpowiednich środków. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 40…*, s. 601–602.

[566] Artykuł 40 ust. 5; art. 40 ust. 6 w zw. z art. 40 ust. 5; art. 40 ust. 7–9; art. 40 ust. 10 w zw. z art. 40 ust. 9; art. 40 ust. 11 RODO.

[567] Artykuł 40 ust. 4 w zw. z art. 41 ust. 1 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 41*, [w:] P. Litwiński (red.), *Rozporządzenie w sprawie ochrony osób fizycz-*

przetwarzający narusza kodeks, podmiot monitorujący zawiesza lub wyklucza go spośród stosujących kodeks. Podmiot monitorujący informuje Prezesa Urzędu o tych działaniach i ich powodach[568].

nych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz, Warszawa 2018, s. 604.

[568] Art. 41 ust. 4 RODO. Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 41.*.., s. 604–605.

Rozdział VI

Bezpośrednie środki prawne ochrony danych osobowych

(Jolanta Behr)

1. Przegląd bezpośrednich środków prawnych ochrony danych osobowych

Korzystanie z bezpośrednich środków prawnych ochrony danych osobowych wymaga aktywnej postawy (działania) osoby, której dane dotyczą. Zgodnie z przyjętym w pracy podziałem, należą do nich:

- prawo do wyrażenia zgody na przetwarzanie danych osobowych i jej cofnięcie;
- prawo dostępu do danych osobowych;
- prawo do sprostowania danych osobowych;
- prawo do usunięcia danych osobowych;
- prawo do ograniczenia przetwarzania danych osobowych;
- prawo do przenoszenia danych osobowych;
- prawo do sprzeciwu wobec przetwarzania danych osobowych;
- prawo do wniesienia skargi do organu nadzorczego na administratora lub podmiot przetwarzający dane osobowe;
- prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu;

– prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu;
– prawo do odszkodowania.

2. Prawo do wyrażenia i wycofania zgody na przetwarzanie danych osobowych

2.1. Zgoda – uwagi ogólne

Przepisy art. 6 RODO i art. 23 u.o.d.o. określają przesłanki zgodności z prawem (legalności) przetwarzania danych osobowych. Co do zasady mają one równorzędny status i autonomiczny charakter. Oznacza to, że zrealizowanie którejkolwiek z nich decyduje o legalności przetwarzania[569]. Jedną z przesłanek jest zgoda osoby, której dane dotyczą[570]. Udzielenie zgody nie zawsze jest jednak wystarczające do legalnego przetwarzania. Odnosi się to np. do przetwarzania danych osobowych wrażliwych, które – w niektórych przypadkach – nie jest możliwe nawet po uzyskaniu uprzedniej zgody osoby, której dane dotyczą[571].

„Zgoda" to m.in. zezwolenie na coś, aprobata, przystanie na coś[572]. Termin „zgoda" jest stosowany w tekstach wielu aktów prawnych. W kontekście ochrony danych osobowych został on zdefiniowany w przepisie art. 7 pkt 5 u.o.d.o.97. Stanowi on, że zgodą osoby, której dane dotyczą, „jest oświadczenie woli, którego treścią jest zgoda[573] na przetwarzanie

[569] Zob. motyw 40 preambuły.

[570] Wyrok NSA z dnia 25 lipca 2017 r., sygn. I OSK 2859/16, LEX nr 2333310; wyrok WSA w Warszawie z dnia 18 października 2012 r., sygn. II SA/Wa 697/12, LEX nr 1241598; B. Kaczmarek-Templin, *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – wybrane zagadnienia*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *Polska i europejska reforma danych osobowych*, Wolters Kluwer, Warszawa 2016, s. 102–126.

[571] Zob. motyw 51 preambuły i art. 9 ust. 2 lit. a RODO.

[572] S. Skorupka, H. Auderska, Z. Łempicka (red.), *Mały słownik języka polskiego*, Państwowe Wydawnictwo Naukowe, Warszawa 1968, s. 1002.

[573] Przyjęta przez ustawodawcę definicja jest obarczona błędem *idem per idem*. W *definiensie* stosuje się bowiem wyrażenie stosowane w *definiendum* (zob. S. Lewandowski, A. Machiń-

danych osobowych tego, kto składa oświadczenie". Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Można ją odwołać w każdym czasie[574].

Poglądy przedstawicieli nauki prawa dotyczące charakteru prawnego zgody osoby, której dane dotyczą, nie są jednolite[575]. Niesporne jest jednak to, że zgoda powinna być wyraźna i konkretna[576], powinna odnosić się wyłącznie do „określonych danych oraz sprecyzowanego sposobu i celu ich przetwarzania"[577]. Należy ją udzielić odrębnie dla każdego celu przetwarzania[578].

Ustawodawca krajowy wyłącza uznanie zgody domniemanej lub dorozumianej z oświadczenia woli o innej treści. Stanowisko to różni się od definicji zgody zawartej w RODO, dopuszczającej wprost jej udziele-

ska, *Definicje*, [w:] S. Lewandowski, H. Machińska, A. Malinowski, J. Petzel, *Logika dla prawników*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2002, s. 61).

[574] Uzupełnienie definicji zgody o „prawo odwołania zgody w każdym czasie" nastąpiło w dniu 7 marca 2011 r. Zmianę wprowadzono przepisami ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz. U. Nr 229, poz. 1497). Lukę istniejącą w tym zakresie uzupełniało jednak orzecznictwo (zob. np. wyrok WSA w Warszawie z dnia 21 października 2009 r., sygn. II SA/Wa 857/09, LEX nr 573915).

[575] Wyróżnia się trzy dominujące stanowiska. Pierwsze uznaje ją za jednostronną, upoważniającą czynność prawną, do której należy stosować przepisy Kodeksu cywilnego odnoszące się do tych czynności. Drugie przyjmuje, że zgoda jest „jednostronnym, odwołalnym działaniem prawnie zbliżonym w swym charakterze do oświadczenia woli". Trzecie – nieznajdujące szerokiego poparcia – przyjmuje natomiast, że nie jest ona czynnością prawną (T. Szewc, *Zgoda na przetwarzanie danych osobowych*, „Państwo i Prawo" 2008, Nr 2, s. 87–96 i powołana tam literatura). Warto także zwrócić uwagę na stanowisko zgodnie z którym zgoda jest „nowym typem oświadczenia jednostki, odrębnym od podobnych oświadczeń, występującym wcześniej w innych dziedzinach prawa" (M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Wolters Kluwer Polska, Warszawa 2010, s. 103 i powołana tam literatura). Prezentowane poglądy tracą na znaczeniu wobec kierunku i zakresu zmian wprowadzonych w RODO, które wyznacza ogólne standardy odnoszące się do zgody.

[576] I. Kamińska, *Komentarz do art. 7*, [w:] I. Kamińska, *Ochrona danych osobowych. Komentarz*, wersja el., https://sip.lex.pl/#/commentary/587555936/353376 [dostęp 31.07.2018]; J. Barta, R. Markiewicz, *Komentarz do art. 7*, [w:] J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Zakamycze, Kraków 2001, s. 314.

[577] Wyrok NSA z dnia 10 stycznia 2013 r., sygn. I OSK 2029/11, LEX nr 1341461.

[578] Wyrok NSA z dnia 11 kwietnia 2003 r., sygn. II SA 3942/02, LEX nr 1148407.

nie również w wyniku działań konkludentnych[579]. W myśl RODO zgodą osoby, której dane dotyczą, jest dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba ta w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących jej danych osobowych[580]. Definicja ta poszerza dotychczasowe rozumienie zgody zawarte w dyrektywie 95/46/WE[581]. Uwzględnia dodatkowo jednoznaczność okazania woli i dopuszczalność wyrażenia zgody dorozumianej[582].

Zdefiniowanie zgody na poziomie ponadnarodowym – w rozporządzeniu – należy ocenić pozytywnie. Ujednolica nadawane jej znaczenie we wszystkich państwach członkowskich Unii Europejskiej. Eliminuje istniejący dotychczas problem niejednolitości regulacji prawnych w tym zakresie, osłabiający pozycję prawną osób, których dane dotyczą[583].

Gdy osoby te przemieszczały się poza granice państwa, które stale zamieszkiwały, nie posiadały niezbędnej wiedzy na temat regulacji prawnych obowiązujących na tym obszarze. Były narażone na nadużycia w zakresie niezgodnego z prawem przetwarzania ich danych osobowych i ponosiły negatywne skutki nieznajomości przepisów prawa. Ich pozycję osłabiało ponadto zróżnicowanie sposobu udzielania zgody w poszczególnych państwach członkowskich. Przyczyną tego było zdefiniowanie „zgody" w dyrektywie, która ma na celu harmonizowanie ustawodawstw – czyli ich zbliżanie – a nie ujednolicanie. W konse-

[579] D. Lubasz, *Komentarz do art. 4 pkt 11*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO ogólne rozporządzenie o ochronie danych. Komentarz*, Wolters Kluwer, Warszawa 2018, s. 243–244.

[580] Artykuł 4 pkt 11 RODO.

[581] W świetle przepisu art. 2 lit. h zgoda osoby, której dane dotyczą, to konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą, że wyraża ona przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych.

[582] D. Lubasz, *Komentarz do art. 4 pkt 11.…*, s. 243.

[583] M. Mazewski, *Prawo do wyrażenia i wycofania zgody na przetwarzanie danych*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017, s. 47–48.

kwencji pozycja prawna osób, których dane dotyczą, różniła się w poszczególnych państwach.

2.2. Warunki zgody w świetle RODO

2.2.1. Dobrowolność

Warunkiem zgody na przetwarzanie danych osobowych jest jej dobrowolność[584]. Oznacza ona istnienie rzeczywistego (realnego) wyboru, dokonywanego przez osobę udzielającą zgody oraz kontrolowanie przez nią przedmiotu i zakresu udostępnianych danych[585]. Zgoda powinna być udzielana z osobna na różne operacje przetwarzania[586] danych osobowych. Nie jest jednak błędne objęcie nią wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach[587].

Niedopuszczalne jest wywieranie jakiegokolwiek przymusu lub presji na osobę udzielającą zgody. Nie należy wprowadzać ani sugerować istnienia mechanizmów lub procedur, których zastosowanie – w przypadku nieudzielenia zgody na przetwarzanie danych lub jej cofnięcia – będzie powodowało negatywne skutki względem tej osoby. Nie należy uzależniać wykonania umowy lub świadczenia usługi od udzielenia zgody na przetwarzanie danych, gdy nie jest ono niezbędne dla ich realizacji[588]. Działaniem tym jest np. uzależnienie przeglądania treści określonej strony internetowej od udzielenia zgody na przetwarzanie danych. Następuje to na przykład, gdy

[584] Artykuł 4 pkt 11 RODO.

[585] Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, wersja el., s. 5, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 [dostęp 03.07.2018].

[586] Przetwarzaniem jest operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (art. 4 pkt 2 RODO).

[587] Motyw 32 i 43 preambuły RODO.

[588] Motyw 42 i 43 preambuły i art. 7 ust. 4 RODO.

okienko udzielenia zgody przesłania całą stronę internetową, a niewyrażenie zgody jest równoznaczne z opuszczeniem strony.

W celu uzyskania zgody nie można wykorzystywać nierówności pozycji prawnej administratora danych i osoby udzielającej zgody. RODO[589] formułuje ten zakaz przede wszystkim w odniesieniu do „organów publicznych". Są nimi wszystkie „organy sprawujące władzę ustawodawczą, wykonawczą lub sądowniczą, czy pozostawione poza trójpodziałem, a także niezależnie od posiadania właściwości [ponadnarodowej – przyp. J. B.], ogólnopaństwowej czy terytorialnie ograniczonej"[590]. Wprowadzenie omawianego zakazu ma istotne znaczenie, bowiem nierównorzędna pozycja jest w praktyce nadużywana przez te organy[591].

Przykładem nadużycia było żądanie przez organy administracji publicznej od osób, których dane dotyczą, udzielenia przez nie zgody na przetwarzanie danych osobowych, których zakres wykracza poza niezbędny do realizacji zadania publicznego. Następowało to w przypadku składania przez mieszkańców tzw. deklaracji śmieciowej[592], w której żądano podania numeru telefonu komórkowego i innych danych osobowych. Ich nieudostępnienie lub nieudzielenie zgody na ich przetwarzanie powodowało negatywne skutki względem osoby, której dane dotyczą[593]. W tym przypadku organ administracji publicznej wykorzystywał dominującą pozycję i uzależniał świadczenie usługi od udzielenia zgody na przetwarzanie danych.

[589] Motyw 43 preambuły RODO.

[590] M. Zubik, W. Sokolewicz, *Komentarz do art. 7*, [w:] L. Garlicki, M. Zubik (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Wydawnictwo Sejmowe, Warszawa 2016, wyd. II uzup., t. I, s. 245–246.

[591] Dotyczy to przede wszystkim organów administracji publicznej, które w stosunkach z administrowanymi mają względem nich nadrzędną pozycję, co wynika z charakteru stosunków administracyjnoprawnych (zob. E. Ochendowski, *op. cit*., s. 39–45).

[592] Deklaracja o wysokości opłaty za gospodarowanie odpadami komunalnymi.

[593] Zob. np. wyrok WSA w Krakowie z dnia 22 lipca 2015 r., sygn. I SA/Kr 415/15, LEX nr 1770518; uchwała KRIO w Gdańsku z dnia 18 kwietnia 2013 r., sygn. 094/g319/P/13, LEX nr 1311015; rozstrzygnięcie nadzorcze Wojewody Warmińsko-Mazurskiego z dnia 23 stycznia 2013 r., sygn. PN.4131.80.2013, LEX nr 1293260.

Nierównorzędność pozycji występuje również w relacji z innymi podmiotami, w szczególności z pracodawcami. Niektórzy z nich wywierają presję na pracownikach, żądając udzielenia przez nich zgody na pobranie i przetwarzanie dodatkowych danych osobowych, wykraczających poza zakres określony przepisami prawa. Wyrażona wówczas zgoda nie może być uznana za dobrowolną. Działanie to „narusza prawa pracownika i swobodę wyrażenia przez niego woli”[594]. Jest ono również niezgodne z przepisami prawa określającymi zakres danych osobowych pracownika gromadzonych przez pracodawcę[595].

2.2.2. Konkretność

Drugim warunkiem zgody jest jej konkretność. Zgoda jest konkretna, gdy odnosi się do określonego stanu faktycznego, obejmując tylko wybrane dane i wskazując sprecyzowany sposób oraz cel ich przetwarzania[596]. Zakres zgody powinien być ustalony w odniesieniu do zamierzonego celu przetwarzania, poza który nie powinien wykraczać. Zakazane jest gromadzenie i przetwarzanie danych osobowych, które są zbędne dla realizacji określonego zadania[597].

Cel przetwarzania powinien być prawnie uzasadniony, a udzielana zgoda powinna obejmować jeden lub większą liczbę określonych celów[598]. Jeśli operacje są współzależne i występują w ramach jednego celu, nie jest konieczne uzyskiwanie odrębnej zgody na każdą z nich. Wystarczy wówczas uzyskać zgodę „w ramach jednego celu na […] wszystkie czynności zwią-

[594] Wyrok WSA w Warszawie z dnia 18 czerwca 2010 r., sygn. II SA/Wa 151/10, LEX nr 643811.

[595] Zob. art. 22^1 k.p.; motyw 155 preambuły i art. 88 RODO.

[596] Wyrok NSA z dnia 10 stycznia 2013 r., sygn. I OSK 2029/11, LEX nr 1341461.

[597] Przykładem tego działania było żądanie przez gminy w procesie rekrutacji do publicznych żłobków i przedszkoli zaświadczenia o poddaniu dziecka obowiązkowym szczepieniom (zob. wyrok WSA w Gliwicach z dnia 26 października 2015 r., sygn. IV SA/Gl 748/15, LEX nr 1816386).

[598] Artykuł 5 ust. 1 lit. b, art. 6 ust. 1 lit. a oraz motyw 43 preambuły RODO.

zane z danym celem przetwarzania"[599]. Cele te powinny być wyraźne, uzasadnione i określone w momencie zbierania danych[600].

Cel przetwarzania powinien być aktualny. Oznacza to, że zgoda nie może być udzielana dla potencjalnych celów, „niejako «na zapas» z założeniem, że [dane – przyp. J. B.] mogą być […] ewentualnie przydatne w przyszłości"[601]. Przykładowo, jeśli kandydat w procesie rekrutacji ubiega się o określone stanowisko i wyraził zgodę na przetwarzanie jego danych osobowych na potrzeby rekrutacji na to stanowisko, wówczas po zakończeniu tej rekrutacji jego dane nie mogą być już legalnie przetwarzane w innych rekrutacjach, bowiem cel przetwarzania został zrealizowany[602].

Aby ustalić czy zgoda jest konkretna należy wziąć pod uwagę trzy kwestie. Pierwsza dotyczy realizacji zasady informowania osób, których dane dotyczą, odnośnie do celu uzasadniającego gromadzenie i przetwarzanie ich danych osobowych. Informacja powinna być jasna i jednoznaczna. Służy ona zabezpieczeniu przed nieuprawnionym naruszeniem prawa do prywatności[603]. Druga odnosi się do formułowania prośby o udzielenie zgody w sposób umożliwiający ustalenie czy jest ona udzielana dla jednego lub większej liczby celów przetwarzania. Trzecią jest jednoznaczne oddzielenie informacji dotyczących udzielenia zgody na przetwarzanie danych osobowych od innych informacji. Chodzi o to, aby osoba udzielająca zgody nie miała wątpliwości co do jej przedmiotu i zakresu. Należy jej więc udzielić precyzyjnych informacji na ten temat[604].

[599] D. Lubasz, *Komentarz do art. 4 pkt 11.*.., s. 249; Article 29 Data Protection Working Party, *op. cit.*, s. 10.

[600] Motyw 39 preambuły RODO.

[601] Wyrok WSA w Warszawie z dnia 12 lipca 2017 r., sygn. II SA/Wa 221/16, LEX nr 2113510.

[602] Zgoda może być jednak sformułowana w sposób uwzględniający różne cele przetwarzania. Może przykładowo obejmować przetwarzanie dotyczące rekrutacji na określonego rodzaju stanowiska w wyznaczonym czasie (np. wszystkie stanowiska kierownicze u danego przedsiębiorcy przez okres sześciu miesięcy od dnia wyrażenia zgody).

[603] Zob. szerzej nt. tej zasady: J.A. Cannataci, *The end of the purpose-specification principle in data protection?*, „International Review of Law, Computers & Technology" 2010, Vol. 24, Nr 1, s. 101–117.

[604] Article 29 Data Protection Working Party, *op. cit.*, s. 11–12.

Problemem praktycznym występującym w tym obszarze jest m.in. łączenie kilku celów przetwarzania w jednym punkcie zgody. Są to sytuacje, w których osoba, której dane dotyczą, nie może udzielić odrębnej zgody na każdy cel przetwarzania, ponieważ są one ujęte w jednym punkcie. Uchybienie to jest jednym z najczęściej odnotowywanych w klauzulach zgody na przetwarzanie danych osobowych w celach marketingowych proponowanych przez banki[605]. Osłabia to pozycję prawną osób, których dane dotyczą. Tworząc projekt zgody na przetwarzanie danych osobowych należy zatem dołożyć szczególnej staranności, aby zapewnić konkretność zgody i rozłączne określenie jej celów.

2.2.3. Świadomy charakter

Trzecim warunkiem zgody jest jej świadomy charakter. Oznacza to, że osoba, której dane dotyczą, powinna być zorientowana przede wszystkim w tym: jakie dane będą przetwarzane, kto będzie je przetwarzać i jaki jest cel ich przetwarzania. Jeśli dane są przetwarzane w sposób zautomatyzowany, osoba ta powinna znać również konsekwencje tej metody. Powinna mieć świadomość ryzyka związanego z przetwarzaniem jej danych, a także znać środki ochrony swoich praw. Świadomy charakter zgody łączy się ściśle z zasadą transparentności, której realizacji służy stosowanie języka prostego i dostosowanego do możliwości percepcyjnych przeciętnego odbiorcy.

W praktyce udzielana zgoda nie zawsze ma świadomy charakter. Informacje udzielane przez administratorów są niejednokrotnie trudne do zrozumienia i pozbawione przejrzystości. Są przekazywane w formie niedostosowanej do możliwości percepcyjnych adresatów oraz w nadmiernej ilości, zniechęcającej do zapoznania się z nimi. Utrudnione jest ponadto wyodrębnienie istotnych kwestii. Sformułowanie zgody na prze-

[605] *Banki błędnie formułują klauzule zgody na przetwarzanie danych osobowych w celach marketingowych*, wersja el, https://giodo.gov.pl/pl/259/10003/ [dostęp 06.07.2018].

twarzanie danych w sposób sprzeczny z przepisami RODO powoduje, że oświadczenie złożone przez osobę, której dane dotyczą, nie jest wiążące w części niezgodnej z tymi przepisami[606].

Należy odnotować, że dokonując oceny prawidłowości udzielonej zgody bada się, czy wymagane informacje zostały przekazane w sposób umożliwiający adresatom zapoznanie się z ich treścią przed wyrażeniem zgody. Bez znaczenia jest to, czy osoba wyrażająca zgodę faktycznie się z nimi zapoznała i zrozumiała ich treść. Do obowiązków administratora danych osobowych należy bowiem udowodnienie, że osoba, której dane dotyczą, udzieliła zgody niezbędnej dla określonego celu przetwarzania w wymaganym zakresie, a także, że zgoda ta jest ważna[607]. Nie weryfikuje się natomiast wiedzy osób, których dane dotyczą, i ich świadomości odnośnie do przysługujących im praw. Wprowadzenie tego mechanizmu byłoby czasochłonne i kosztowne. Ważne jest zatem przestrzeganie wyznaczonych przepisami prawa wymogów i procedur, w szczególności związanych z wyrażaniem zgody, realizacją obowiązków informacyjnych, zgodnym z prawem przetwarzaniem danych osobowych i ich właściwym przechowywaniem. Wpływają one bowiem na zwiększenie prawdopodobieństwa ochrony praw osób, których dane dotyczą.

2.2.4. Jednoznaczność

Ostatnim warunkiem ważności zgody jest jej jednoznaczność. RODO stanowi, że zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności wyrażającej –odnoszące się do określonej sytuacji – dobrowolne, świadome i jednoznaczne przyzwolenie osoby, której dane dotyczą, na przetwarzanie dotyczących jej danych osobowych[608]. Zgodą jest więc intencjonalne zachowanie osoby, której dane dotyczą, polegające na jej działaniu.

[606] Artykuł 7 ust. 2 RODO.
[607] Zob. motyw 42 preambuły i art. 7 ust. 1 RODO.
[608] Motyw 32 preambuły RODO.

Udzielenie zgody może nastąpić w formie oświadczenia lub wyraźnego działania potwierdzającego, w którym osoba przyzwala na przetwarzanie jej danych osobowych[609]. W odróżnieniu od dotychczasowych regulacji i przepisów ustawy o ochronie danych osobowych[610] RODO dopuszcza wprost udzielenie zgody dorozumianej.

Udzielenie zgody może nastąpić w formie ustnej lub pisemnej, w tym elektronicznej. Może polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, wybraniu ustawień technicznych do korzystania z usług społeczeństwa informacyjnego, złożeniu innego oświadczenia lub podjęciu innego działania wskazującego bezspornie, że określona osoba wyraża zgodę na przetwarzanie jej danych. Działanie powinno umożliwić ustalenie zakresu udzielonej zgody[611].

W niektórych przypadkach RODO wymaga, aby zgoda była „wyraźna"[612]. Oznacza to, że osoba, której dane dotyczą, powinna uzewnętrznić swoją wolę w sposób nieulegający wątpliwości. Jako że nie jest wymagane, aby „wyraźna" zgoda była udzielona na piśmie, dopuszczalne jest jej udzielenie w formie ustnego oświadczenia. Niewątpliwym ułatwieniem dla administratora danych w zakresie dowodowym byłoby jednak zastosowanie formy pisemnej. Udzielenie wyraźnej zgody może również polegać na uzupełnieniu formularza elektronicznego, wysłaniu maila określonej treści, zastosowaniu podpisu elektronicznego lub doręczeniu skanu zgody. Wprowadzenie wymogu wyraźnej zgody wyłącza jej udzielenie w sposób dorozumiany[613].

[609] Artykuł 2 pkt 11 RODO.
[610] Zob. art. 7 pkt 5 u.o.d.o.97.
[611] Motyw 32 preambuły RODO.
[612] Zob. art. 9, 22 i 49 RODO.
[613] Article 29 Data Protection Working Party, *op. cit*., s. 18–19.

2.3. Zgoda dziecka

Ze względu na niedojrzałość fizyczną i umysłową oraz mniejszą świadomość konsekwencji swoich działań dzieci[614] są narażone na zagrożenia zarówno w „świecie realnym", jak i wirtualnym[615]. Jednym z nich jest niepożądany dostęp do ich danych osobowych[616], które są wykorzystywane m.in. w celach marketingowych i do tworzenia profili osobowych lub profili użytkownika[617]. Mając to na uwadze, RODO wprowadza szczegółowe regulacje w zakresie ochrony danych osobowych dzieci.

Pierwsza wymaga, aby wszelkie informacje i komunikaty kierowane do dziecka były formułowane jasnym i prostym językiem, w sposób dla niego przystępny[618]. Powinny one uwzględniać poziom jego rozwoju.

Druga wprowadza szczególne warunki wyrażenia zgody na przetwarzanie danych osobowych dziecka. Znajduje ona zastosowanie względem usług społeczeństwa informacyjnego[619] oferowanych bezpośred-

[614] Dzieckiem jest osoba w wieku poniżej osiemnastu lat, chyba że zgodnie z przepisami prawa uzyska ona wcześniej pełnoletność (preambuła i art. 1 Konwencji o prawach dziecka przyjętej przez Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych dnia 20 listopada 1989 r., Dz. U. z 1991 r. Nr 120, poz. 526 ze zm.). Dziecko jest rozumiane jednolicie na obszarze Unii Europejskiej. Wszystkie państwa członkowskie są bowiem sygnatariuszami Konwencji (zob. wykaz państw, które ratyfikowały Konwencję, https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4&lang=en [dostęp 02.07.2018]). W Rzeczypospolitej Polskiej osobą pełnoletnią jest ponadto kobieta, która ukończyła lat szesnaście i wstąpiła w związek małżeński (zob. art. 10 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2018 r., poz. 1025) w zw. z art. 10 § 1 ustawy z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy (t.j. Dz. U. z 2017 r., poz. 682 ze zm.).

[615] Dzieci wykazują coraz większą aktywność w cyberprzestrzeni. Obecnie 1/3 użytkowników internetu to osoby, które nie ukończyły osiemnastego roku życia (M. Mecenaite, *Consent for processing children's personal data in the EU: following in US footsteps?*, „Information & Communications Technology Law" 2017, Vol. 26, Nr 2, s. 146–197).

[616] K. Broniatowski, *Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni – regulacje w prawie polskim i unijnym*, Kancelaria Senatu. Biuro Spraw Senatorskich, Warszawa 2017, s. 4–7.

[617] Motyw 38 preambuły RODO.

[618] Motyw 58 preambuły RODO.

[619] Do usługi społeczeństwa informacyjnego nawiązuje przepis art. 4 pkt 25 RODO, który odsyła w tym zakresie do dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. L

nio dziecku. Co do zasady, zgodę na przetwarzanie danych osobowych udziela dziecko, które ukończyło 16 lat[620]. Jeśli jest ono młodsze, wymagana jest zgoda lub aprobata jego rodzica lub opiekuna prawnego, który powinien działać w „najlepiej pojętym interesie dziecka"[621]. Na administratorze danych osobowych spoczywa obowiązek podjęcia „rozsądnych starań", aby zweryfikować czy określona przepisami prawa osoba wyraziła zgodę[622].

Faktyczne ustalenie osób wyrażających zgodę na przetwarzanie danych osobowych jest jednak utrudnione. Administrator danych opiera się bowiem wyłącznie na informacjach udzielonych przez dziecko. Nie ma on dostępu do innych baz, umożliwiających weryfikację uzyskanych informacji. Mając to na uwadze, wymaga się od niego wyłącznie podjęcia „rozsądnych starań", z uwzględnieniem dostępnej technologii. Kluczową rolę odgrywają w tym zakresie odpowiednie procedury, w tym m.in. żądanie potwierdzenia wyrażenia zgody lub aprobaty z innego adresu mailowego. Opierają się one jednak na uczciwości dziecka, która może być największą barierą utrudniającą ochronę jego praw.

---

241 z 17.09.2015 r., s. 1), stanowiącej, że jest nią każda usługa normalnie świadczona za wynagrodzeniem na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. Przy czym (i) „na odległość" oznacza, że usługa świadczona jest bez równoczesnej obecności stron; (ii) „drogą elektroniczną" oznacza, iż usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych; (iii) „na indywidualne żądanie odbiorcy usług" oznacza, że usługa świadczona jest poprzez przesyłanie danych na indywidualne żądanie. Zdaniem I. Wróbel pojęcie „usługi społeczeństwa informacyjnego" należy obecnie do *acquis communautaire* (I. Wróbel, *Pojęcie usługi społeczeństwa informacyjnego w prawie wspólnotowym*, „E-Biuletyn: elektroniczny biuletyn naukowy CBKE" 2007, Nr 4, s. 2).

[620] Państwa członkowskie mogą określić w prawie wewnętrznym niższą granicę wiekową, jednak nie niższą niż 13 lat.

[621] Grupa Robocza art. 29 ds. ochrony danych, *Opinia 2/2009 w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół) przyjęta dnia 11 lutego 2009*, sygn. 398/09/PL WP 160, wersja el., s. 4, https://giodo.gov.pl/pl/1520022/2991 [dostęp 09.07.2018].

[622] Artykuł 8 RODO.

2.4. Wycofanie zgody

Artykuł 7 ust. 3 RODO stanowi, że osoba, której dane dotyczą, ma prawo w dowolnym czasie wycofać zgodę. O treści przysługującego jej prawa należy poinformować jeszcze przed jej wyrażeniem. Zgoda jest udzielana bezterminowo, o ile co innego nie wynika z jej treści. Okres przetwarzania danych powinien być wyznaczany w relacji do celów przetwarzania.

Cofnięcie zgody powinno być równie łatwe jak jej wyrażenie[623]. W praktyce można zaobserwować utrudnienia związane z wycofaniem zgody. Przykładowo, wyrażenie zgody wymaga zaznaczenia okienka wyboru podczas przeglądania strony internetowej, a jej cofnięcie wymaga już wysłania maila do administratora danych osobowych. Nie jest to działanie prawidłowe.

Wycofanie zgody jest skuteczne *ex nunc*. Oznacza to, że wszelkie czynności dokonane przed skutecznym cofnięciem zgody i mieszczące się w jej zakresie są legalne[624]. Wycofanie zgody wiąże administratora. Nie ma on prawa do oceny celowości wycofania zgody na przetwarzanie i jest związany żądaniem osoby, której dane dotyczą.

3. Prawo dostępu do danych osobowych

Prawo dostępu do danych przysługujące osobie, której dane dotyczą, było uregulowane w przepisie art. 12 lit. a dyrektywy 95/46/WE. Jest ono również uregulowane w RODO[625] stanowiącym, że osobie, której dane dotyczą, przysługuje prawo uzyskania informacji (potwierdzenia), czy jej dane osobowe są przetwarzane przez administratora[626]. Przepisy nie określają przesłanek warunkujących realizację tego prawa. Należy więc przyjąć, że pytanie w tym przedmiocie może być skierowane do administratora

[623] Artykuł 7 ust. 3 RODO.

[624] *Ibidem*.

[625] Zgodnie z przepisami dyrektywy 95/46/WE jego wykonywanie nie wymagało realizacji tak rozbudowanego obowiązku informacyjnego.

[626] Artykuł 15 ust. 1 RODO.

w dowolnej formie, zarówno ustnej, jak i pisemnej, w tym elektronicznej. Administrator powinien mieć możliwość zweryfikowania, czy jest ono składane przez osobę, której dane dotyczą[627]. W tym celu powinien wykorzystać wszelkie możliwe środki. Weryfikacja nie powinna wiązać się z dodatkowymi formalnościami obciążającymi nadmiernie osobę wnioskującą. Administrator nie powinien żądać udzielenia informacji, których dotychczas nie zgromadził[628].

Jeśli administrator przetwarza dane dotyczące osoby, może ona skutecznie żądać dostępu do tych danych oraz dostępu do innych określonych przepisami prawa informacji[629]. Dane powinny zostać udostępnione w formie, w której zażądano dostępu, jeśli osoba, której dane dotyczą, nie wyraziła odmiennej woli. Odnosi się to przede wszystkim do formy elektronicznej[630]. Przepisy prawa mogą wprowadzać ograniczenia dotyczące formy lub formatu udostępnianych danych[631]. Ich zastosowanie nie powinno utrudniać zapoznania się z treścią zgromadzonych danych. Właściwa realizacja prawa dostępu wpływa bowiem na wykonywanie innych praw określonych w przepisach art. 16–22 RODO[632].

Dane powinny być udostępnione w zakresie, o który wnioskuje osoba, której dane dotyczą. Jeśli nie precyzuje ona zakresu żądania, należy

[627] Motyw 64 preambuły RODO.

[628] Wyjątek określono w przepisie art. 11 ust. 2 RODO.

[629] Katalog tych informacji zawiera art. 18 ust. 1–2 RODO. Są nimi w szczególności informacje dotyczące: celów przetwarzania, kategorii przetwarzanych danych osobowych, ich odbiorców lub kategorii odbiorców, planowanego okresu przechowywania danych, praw przysługujących osobie w związku z przetwarzaniem oraz źródła lub źródeł, z których pochodzą dane (gdy nie pochodzą od osoby, której dotyczą) oraz informacje o zautomatyzowanym podejmowaniu decyzji.

[630] Artykuł 15 ust. 3 RODO.

[631] Zob. np. rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r., poz. 2247), określające szczegółowe wymogi techniczne odnoszące się do wymiany informacji.

[632] F. Voigt, A. von Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer, Cham 2017, s. 150.

przyjąć, że odnosi się ono do wszystkich zgromadzonych danych jej dotyczących. Wyjątkiem jest sytuacja, w której administrator przetwarza duże ilości informacji o tej osobie. Ma on wówczas prawo – przed ich udostępnieniem – zwrócić się do osoby, której dane dotyczą, o sprecyzowanie zakresu żądania przez wskazanie informacji lub czynności przetwarzania, których dotyczy żądanie[633].

Opisana regulacja ma na celu ochronę administratorów danych osobowych przed nadużywaniem prawa przez osoby, których dane dotyczą. Charakter ochronny ma również przepis umożliwiający pobieranie opłat za kolejne kopie danych osobowych podlegających udostępnianiu[634], przepis przyjmujący, że prawo dostępu do danych powinno być wykonywane w „rozsądnych odstępach czasu"[635] oraz przepis odnoszący się do działań „ewidentnie nieuzasadnionych lub nadmiernych, ze względu na swój ustawiczny charakter"[636]. Wprowadzenie tych regulacji należy ocenić pozytywnie. Wzmacniają one pozycję administratora danych osobowych bez szkody dla osób, których dane dotyczą. Dążą do zagwarantowania realizacji „idei" dostępu do danych osobowych, chroniąc przed jej wypaczeniem. Prawa nie należy bowiem wykorzystywać w celu spowolnienia lub paraliżu pracy podmiotu zapewniającego jego realizację, co można zaobserwować w praktyce wykonywania innych praw[637].

[633] Motyw 63 preambuły RODO.

[634] Artykuł 15 ust. 3 RODO.

[635] Motyw 63 preambuły RODO. Wyrażenie „rozsądnych odstępach czasu" jest niedookreślone. Powinno być interpretowane *a casu ad casum*. Dokonując interpretacji, należy wziąć pod uwagę przede wszystkim cele przetwarzania danych osobowych i zakres zgromadzonych danych.

[636] Artykuł 12 ust. 5 RODO.

[637] Dotyczy to w szczególności składania skarg powszechnych i wniosków o udostępnienie informacji publicznej. W przypadku skarg ustawodawca wprowadził mechanizmy chroniące organ administracji publicznej przed tzw. skargami pieniackimi (zob. art. 239 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, t.j. Dz. U. z 2017 r., poz. 1257 ze zm.). Nie wprowadził jednak analogicznego uregulowania w odniesieniu do wniosków o udostępnienie informacji publicznej, co powoduje problemy w praktyce stosowania prawa (zob. ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, t.j. Dz. U. z 2016 r., poz. 1764 ze

Osoba, której dane dotyczą, ma prawo uzyskania kopii danych osobowych podlegających przetwarzaniu. Realizacja prawa wymaga wniosku tej osoby, w którym powinien być wskazany sposób udostępnienia, np. udostępnienie w wersji papierowej lub na nośniku danych. Pierwsza kopia jest wydawana bezpłatnie, a za kolejne może zostać pobrana opłata w rozsądnej wysokości, wynikającej z kosztów administracyjnych[638]. Nie powinna ona być barierą w dostępie do danych, lecz powinna pozostawać w ścisłej relacji do kosztów ponoszonych przez administratora danych, w związku z ich przygotowaniem.

Jeśli jest to możliwe, administrator powinien umożliwić osobie, której dane dotyczą uzyskanie zdalnego dostępu do danych za pośrednictwem bezpiecznego systemu[639], który powinien posiadać funkcje umożliwiające oddzielenie danych osobowych osoby, która uzyskała dostęp od innych informacji, w sposób uniemożliwiający naruszenie praw i wolności innych osób, w szczególności tajemnic handlowych, własności intelektualnej i praw autorskich chroniących oprogramowanie[640].

Żądanie osoby, której dane dotyczą, w przedmiocie udzielenia informacji odnośnie do przetwarzania jej danych osobowych oraz żądanie dostępu do nich powinny być zrealizowane bez zbędnej zwłoki. Powinno to nastąpić najpóźniej w terminie miesiąca od otrzymania żądania przez administratora. Ze względu na liczbę żądań lub skomplikowany charakter sprawy termin ten można przedłużyć o kolejne dwa miesiące pod warunkiem, że – w terminie miesiąca od otrzymania żądania – poinformuje się wnioskodawcę o przedłużeniu terminu[641].

Jeśli administrator nie podejmuje działań w związku z żądaniem, to najpóźniej w terminie miesiąca od jego otrzymania powinien poinfor-

zm.; M. Maciejewski (red.), *Prawo do informacji publicznej. Efektywność regulacji i perspektywy jej rozwoju*, Biuro Rzecznika Praw Obywatelskich, Warszawa 2014).

638 Artykuł 15 ust. 3 RODO.

639 Motyw 63 preambuły RODO.

640 *Ibidem*; art. 15 ust. 4 RODO.

641 Artykuł 12 ust. 3 RODO.

mować o tym wnioskodawcę oraz wskazać przyczyny opóźnienia, a także pouczyć wnioskodawcę o przysługującym mu prawie wniesienia skargi do organu nadzorczego oraz prawie skorzystania ze środków ochrony prawnej przed sądem[642]. Administrator powinien ponadto zrealizować obowiązki informacyjne określone w art. 19 RODO. Jeśli nie wywiąże się z nich w terminie, to osoba, której dane dotyczą, może dochodzić swoich praw przed właściwym organem nadzorczym i sądem.

4. Prawo do sprostowania danych osobowych

Artykuł 5 ust. 1 lit. d RODO stanowi, że dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy więc podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Aby zrealizować ten wymóg, osobie, której dane dotyczą, przyznano m.in. prawo żądania sprostowania danych. Zgodnie z nim osoba, której dane dotyczą, może żądać od administratora skorygowania błędów w przetwarzanych danych przez usunięcie rozbieżności między zgromadzonymi przez niego danymi a stanem faktycznym. Może również żądać uzupełnienia niekompletnych danych.

Artykuł 16 RODO przyznaje osobie, której dane dotyczą, wyłącznie prawo „żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych", a nie prawo ich „sprostowania". Oznacza to, że osoba ta nie jest uprawniona do samodzielnego dokonywania zmian w zgromadzonych przez administratora danych, lecz wyłącznie do wnioskowania o ich dokonanie.

Warto zauważyć, że RODO uprawnia do żądania „niezwłocznego" sprostowania, podczas gdy przepis art. 12 lit. b dyrektywy 95/46/WE uprawniał wyłącznie do żądania sprostowania. Zamiarem prawodaw-

[642] Artykuł 12 ust. 4 RODO.

cy było więc jak najszybsze usunięcie niezgodności zgromadzonych danych ze stanem faktycznym. Termin „niezwłoczne" jest jednak nieostry, a RODO nie zawiera w tym zakresie wskazówek interpretacyjnych. Oznacza to, że do realizacji prawa do sprostowania danych znajdą zastosowanie terminy określone w art. 12 RODO.

RODO przyjmuje szerokie rozumienie „sprostowania", obejmujące dwa prawa. Pierwsze to prawo żądania usunięcia nieprawidłowych danych osobowych i zastąpienia ich danymi prawidłowymi. Chodzi o zastępowanie danych niezgodnych ze stanem faktycznym, w szczególności nieaktualnych (sprostowanie *sensu stricto*). Przykładem działania mieszczącego się w tym zakresie jest żądanie uaktualnienia nazwiska lub miejsca zamieszkania osoby, gdy nastąpiła jego zmiana.

Drugie to prawo żądania uzupełnienia danych osobowych (uzupełnienie). Odnosi się ono wyłącznie do „niekompletnych" danych, a więc tych, których przetwarzanie przez administratora jest niezbędne dla osiągnięcia celu przetwarzania. To administrator ustala zakres „niezbędnych" danych, które gromadzi, oraz jest on odpowiedzialny za dokonanie prawidłowych ustaleń w tym zakresie.

Warto odnotować, że w niektórych przypadkach żądanie sprostowania danych ma podwójny charakter, jest jednocześnie prawem i obowiązkiem osoby, której dane dotyczą. Źródłem obowiązku są wówczas przepisy szczególne. Przykładem jest skierowane przez studenta do dziekana żądanie sprostowania jego danych osobowych. Obowiązek działania wynika w tym przypadku z przepisów regulaminu studiów, nakazujących bieżące weryfikowanie danych osobowych, a w razie konieczności występowanie z wnioskiem o ich sprostowanie lub uzupełnienie[643]. Prawo wynika natomiast m.in. z przepisów art. 51 ust. 1 Konstytucji RP, art. 16 RODO i art. 8 ust. 2 KPP.

[643] Zob. § 5 pkt 7a uchwały Nr 26/2015 Senatu Uniwersytetu Wrocławskiego z dnia 25 marca 2015 r. w sprawie Regulaminu studiów w Uniwersytecie Wrocławskim, https://uni.wroc.pl/wp-content/uploads/2015/09/Regulamin-studiów-na-Uniwersytecie-Wrocławskim.pdf [dostęp 11.07.2018].

RODO nie zawiera szczegółowych wytycznych dotyczących formy żądania sprostowania danych. Nie wprowadza też zamkniętego katalogu dowodów, na podstawie których można dokonać sprostowania. Wskazuje tylko, że żądanie może być poparte dodatkowym oświadczeniem. Nie zakazuje zatem żądania przez administratora przedłożenia określonych dokumentów. Kwestia ta może mieć istotne znaczenie w praktyce stosowania prawa. Przykładowo, gdy osoba występuje o sprostowanie nazwiska, administrator może np. żądać okazania nowego dowodu osobistego lub – gdy ten nie został jeszcze wydany – odpisu aktu małżeństwa. Gdy żąda ona sprostowania naliczonego okresu pracy, od którego zależą uprawnienia pracownicze, administrator może zażądać przedłożenia świadectwa pracy. Nie dysponuje on jednak żadnymi władczymi środkami prawnymi umożliwiającymi egzekwowanie podjęcia działań przez osobę, której dane dotyczą. Jedyną konsekwencją, którą może wyciągnąć, jest nieuwzględnienie żądania osoby w przedmiocie sprostowania. Nie może on ponadto domagać się przedłożenia dokumentów wykraczających poza cele przetwarzania.

Wykonywanie prawa żądania sprostowania danych nie jest ograniczone temporalnie. Oznacza to, że osoba, której dane dotyczą, może je wykonywać w każdym czasie. Za niecelowe należy jednak uznać np. żądanie sprostowania danych, gdy przetwarzanie jest już zbędne dla celów, dla których dane zostały zebrane, lub gdy dane są przetwarzane niezgodnie z prawem. W tych przypadkach osobie, której dane dotyczą, przysługują bowiem inne środki prawne. Przykładowo, jeśli w procesie rekrutacji kandydat przesłał do działu rekrutacji swoje dane osobowe, w tym informacje dotyczące doświadczenia zawodowego, to gdy zakończy się ten proces, dane są już zbędne dla realizacji celu, tj. dla tej rekrutacji. W tym przypadku korzystanie z prawa do sprostowania danych można uznać za niecelowe, dane są bowiem zbędne dla realizacji celu. Jeśli jednak kandydat wyraził zgodę na wykorzystanie jego danych osobowych w innych postępowaniach rekrutacyjnych, a więc wyraził zgodę na przetwarzanie jego danych w innych celach, żądanie przez niego sprostowa-

nia jego danych jest pożądane, bowiem doświadczenie zawodowe i umiejętności podlegają stałym zmianom.

Obowiązkiem administratora danych osobowych jest udzielenie osobie, której dane dotyczą, informacji o działaniach podjętych w związku z jej żądaniem. Następuje to na tych samych zasadach, co w przypadku realizacji prawa dostępu do danych[644]. Różnią się one jednak tym, że administrator nie ma obowiązku uwzględnienia żądania sprostowania. Uwzględnia je, gdy uzna to za zasadne na podstawie obiektywnych przesłanek. Informuje wówczas o sprostowaniu każdego odbiorcę, któremu ujawniono dane, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Jeśli osoba, której dane dotyczą, tego zażąda, informuje ją ponadto o odbiorcach tych danych[645]. Gdy administrator nie dokona sprostowania danych, ma natomiast obowiązek poinformowania osoby, której dane dotyczą, o podjętych działaniach związanych z wykonywaniem jej prawa[646].

RODO nie określa sposobu realizacji obowiązku informacyjnego. Może on być zatem zrealizowany w dowolnej formie, umożliwiającej osobie żądającej sprostowania zapoznanie się z jego treścią. W przypadku odmowy sprostowania danych należy jednak postulować udzielanie informacji w formie pisemnej. Służy to przede wszystkim celom dowodowym, aby osoba, której dane dotyczą, mogła dochodzić swoich praw w drodze właściwego postępowania.

5. Prawo do usunięcia danych osobowych

Określone w art. 17 RODO prawo łączy się z zasadą ograniczenia przechowywania danych osobowych. Prawo to – w zdecydowanie węższym zakresie – było uregulowane przede wszystkim[647] w dyrektywie 95/46/WE

[644] Zob. art. 12 RODO.

[645] Artykuł 19 RODO.

[646] Artykuł 12 RODO.

[647] Istotną rolę w kształtowaniu tego prawa odegrał również francuski *Kodeks dobrych praktyk prawa do bycia zapomnianym w sieciach społecznościowych i wyszukiwarkach interneto-*

i było wyrażane w orzecznictwie[648]. Podkreślano, że wobec dynamicznego rozwoju nowych technologii i związanych z nim zagrożeń w zakresie ochrony danych osobowych[649] nie jest ono dostosowane do obecnych realiów[650], a przede wszystkim do współczesnej konstrukcji Internetu[651]. Konieczne było więc wprowadzenie nowego uregulowania, uwzględniającego w jak najszerszym zakresie prawa osób, których dane dotyczą.

Artykuł 17 RODO jest zatytułowany „prawo do usunięcia danych («prawo do bycia zapomnianym»)"[652]. Wyniki wykładni literalnej prowadzą do wniosku, że prawodawca unijny utożsamia prawo do usunięcia

wych z 2010 r. i Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu regionów *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej* z dnia 4 listopada 2010 r. (zob. szerzej: B. Fischer, *Prawo do usunięcia danych*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017, s. 205–209.

[648] Zob. wyrok Trybunału Sprawiedliwości z dnia 13 maja 2014 r., sygn. C-131/12, LEX nr 1455816, wydany na podstawie przepisów dyrektywy 95/46/WE. Rozstrzygana sprawa dotyczyła hiszpańskiego obywatela, względem którego ponad dziesięć lat wcześniej była prowadzona egzekucja z nieruchomości. Informacja na ten temat pojawiała się jednak nadal w wyszukiwarce internetowej (link do stron dziennika, w którym podano jego imię i nazwisko i ogłoszenie w przedmiocie licytacji). Zażądał on usunięcia lub zmiany stron w sposób uniemożliwiający pojawienie się na nich jego danych osobowych lub wykorzystanie narzędzi ochrony jego danych osobowych. Wniósł ponadto o nakazanie usunięcia lub ukrycia jego danych osobowych tak, aby nie były one ujawniane w wynikach wyszukiwania i powiązane z linkami do publikacji, w których były one zawarte. Sąd orzekł, że żądanie osoby, której dane dotyczą, jest w pełni uzasadnione. Niezależnie od tego czy wyrządza jej to szkodę, może ona domagać się, aby informacje te nie były z nią łączone w wyszukiwarce. Sąd uznał prymat interesu jednostki nad interesem gospodarczym operatora wyszukiwarki internetowej. Podkreślił jednocześnie, że analizowane prawo może doznawać ograniczeń, w szczególności względem osób pełniących funkcję w życiu publicznym.

[649] Zob. szerzej na ich temat: G. Szpor, *op. cit.*, s. 137–155.

[650] M. Krzysztofek, *„Prawo do bycia zapomnianym" i inne aspekty prywatności w epoce Internetu w prawie UE*, „Europejski Przegląd Sądowy" 2012, Nr 8, s. 29–34; K. Łuczejko, *Dane osobowe w internecie – wybrane zagadnienia administracyjnoprawne*, „Acta Iuris Stetiensis – Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2014, Nr 812, s. 255.

[651] Ł. Goździaszek, *Prawo do bycia zapomnianym w wyszukiwarce internetowej – glosa do wyroku Trybunału Sprawiedliwości z 13.05.2014 r. w sprawie C-131/12 Google Spain SL i Google Inc. Przeciwko Agencia de Protección de Datos (AEPD) i Mario Costeja González*, „Europejski Przegląd Sądowy" 2015, Nr 2, s. 44.

[652] Niem. *Recht auf Löschung (Recht auf Vergessenwerden)*, franc. *Droit à l'effacement (droit à l'oubli)*.

danych z prawem do bycia zapomnianym. Stanowisko to jest zajmowane przez niektórych przedstawicieli nauki prawa6[653]. Większość z nich odróżnia jednak prawo do usunięcia danych od prawa do bycia zapomnianym lub przyjmuje słusznie, że prawo do bycia zapomnianym mieści w sobie prawo do usunięcia danych, będąc jego rozwinięciem[654]. Z perspektywy osoby, której dane dotyczą, większe znaczenie od przyjętej nomenklatury mają konkretne prawa jej przysługujące.

Pierwsze to żądanie od administratora niezwłocznego usunięcia dotyczących jej danych osobowych. Może ono przyjąć dowolną formę, przepisy prawa nie wprowadzają dodatkowych wymogów w tym zakresie. Żądanie powinno zatem dotrzeć do administratora w sposób umożliwiający zapoznanie się z jego treścią i zakresem. W określonych prawem przypadkach żądanie to jest skorelowane z obowiązkiem administratora usunięcia danych. Dotyczy to sytuacji, w których została zrealizowana co najmniej jedna z przesłanek określonych w zamkniętym katalogu przepisu art. 17 ust. 1 RODO[655]. Oznacza to, że żądanie osoby jest sku-

[653] Zob. np.: A. Krasuski, *Ochrona danych osobowych…*, s. 254.; B. Baran, K. Południak-Gierz, *Perspektywa regulacji prawa do bycia „zapomnianym" w Internecie. Zarys problematyki*, „Zeszyty Naukowe Towarzystwa Doktorantów UJ. Nauki Społeczne" 2017, Nr 17, s. 149–150.

[654] Zob. np.: M. Czerniawski, *Komentarz do art. 17*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 524–525; J. Żak, *Koncepcja „prawa do bycia zapomnianym"*, [w:] M. Jabłoński, S. Jarosz-Żukowska (red.), *Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi*, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2014, s. 148–149.

[655] Artykuł 17 ust. 1 RODO stanowi, że są nimi sytuacje, w których: a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane; b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a, i nie ma innej podstawy prawnej przetwarzania; c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania; d) dane osobowe były przetwarzane niezgodnie z prawem; e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega administrator; f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

teczne, gdy zrealizowano jedną z tych przesłanek. Są one pojemne treściowo, w szczególności przesłanka odnosząca się do przetwarzania danych niezgodnie z prawem.

Sposób usunięcia danych jest związany ze sposobem i celem przetwarzania danych przez administratora. Inaczej usuwa się dane przechowywane w formie kartotecznej, a inaczej zapisane w chmurze lub na kilku powiązanych ze sobą serwerach. RODO nie określa procedury usunięcia danych osobowych. Osoba, której dane dotyczą, jest zależna od administratora danych i nie ma możliwości pełnej weryfikacji prawidłowości podjętego przez administratora działania. Jeśli jej dane są ogólnie dostępne, np. na stronie internetowej lub w Biuletynie Informacji Publicznej administratora, ma ona wówczas częściowy wgląd w podejmowane działania. W przypadku przetwarzania ich w formie, do której osoba ta nie ma łatwego dostępu, nie posiada ona dodatkowych uprawnień o charakterze kontrolnym, umożliwiających jej weryfikację podjętych działań w siedzibie administratora. Mieszczą się one natomiast w zakresie działania organu nadzorczego.

Usunięcie danych jest nie tylko skutkiem wykonywania praw osób, których dane dotyczą. Może ono także nastąpić w wyniku samodzielnych działań administratora, zmierzających do ograniczenia okresu przechowywania danych do ścisłego minimum. W tym celu powinien on ustalić termin usuwania zgromadzonych informacji lub dokonywania ich okresowego przeglądu[656].

Drugie prawo przysługujące osobie, której dane dotyczą, jest ściśle związane z prawem do usunięcia danych osobowych. Jest jego wzmocnieniem i rozszerzeniem[657]. Jest wykonywane, gdy administrator upublicznił dane osobowe i ma obowiązek je usunąć, ponieważ osoba, której dane dotyczą, tego zażądała. W celu realizacji tego prawa administrator podejmuje rozsądne działania, w tym wykorzystuje środki techniczne, aby poin-

[656] Motyw 39 preambuły RODO.
[657] Motyw 66 preambuły RODO.

formować innych administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda usunięcia przez nich wszelkich łączy do tych danych, ich kopii lub replikacji. Podejmując te działania administrator bierze pod uwagę dostępną technologię i koszt realizacji działań[658].

Twierdzi się, że danych udostępnionych w Internecie nie da się skutecznie i kompleksowo usunąć. Zawsze pozostawią one jakiś ślad, zostaną zapisane w innym miejscu lub przez kogoś udostępnione, nawet bez świadomości i kontroli podmiotu wprowadzającego dane do sieci. Niejednokrotnie dane pozostają w obiegu cyfrowym dłużej niż funkcjonuje podmiot lub żyje osoba je wprowadzająca. Unijny prawodawca ma tego świadomość. Dlatego formułując analizowany przepis, nie wprowadził wymogu skutecznego usunięcia wszystkich danych („absolutnego zapomnienia")[659], byłoby to bowiem niemożliwe lub niezwykle skomplikowane, pracochłonne i kosztowne. Administrator odpowiedzialny za właściwą realizację tego prawa – pod groźbą wysokiej kary pieniężnej – byłby zmuszony do podejmowania nadmiernych i nieproporcjonalnych wysiłków zmierzających do realizacji praw osób, których dane dotyczą. Mogłoby to powodować szkodę w jego działalności podstawowej.

Ustawodawca unijny wymaga więc podjęcia przez niego „rozsądnych działań" z uwzględnieniem środków technicznych, racjonalnej technologii i kosztów realizacji. Wyrażenie „rozsądne działania" jest nieostre. Dokonując jego interpretacji należy wziąć pod uwagę przede wszystkim rodzaj danych oraz zakres i cele ich przetwarzania przez administratora, skalę na jaką następuje przetwarzanie (potencjalna liczba administratorów je przetwarzających) oraz status osoby, której dane dotyczą. Przykładowo, jeśli zostały upublicznione dane osobowe osoby publicznej znanej w wielu państwach, występuje większe prawdopodobieństwo, że zostaną one wielokrotnie po-

[658] Artykuł 17 ust. 2 RODO.

[659] Zob. szerzej: T. Grzegory, *Pamięć absolutna czy kontrolowana amnezja – wybrane problemy prawne regulacji „prawa do bycia zapomnianym" w ogólnym rozporządzeniu o ochronie danych*, [w:] G. Sibiga (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, C.H. Beck, Warszawa 2016, s. 58–68.

wielone niż w przypadku upublicznienia danych osobowych innych osób. „Rozsądne działania" będą zatem w każdym z tych przypadków przyjmować inny zakres. Dotyczy to także upublicznienia danych osobowych dzieci. RODO podkreśla bowiem szczególne znaczenie prawa do usunięcia danych, gdy zgoda na przetwarzanie została wyrażona przez dziecko, które nie było w pełni świadome ryzyka związanego z przetwarzaniem, a następnie wyraziło wolę usunięcia tych danych, w szczególności z Internetu[660].

Warto zaznaczyć, że działania administratora mają ograniczone zastosowanie. Może on bowiem wyłącznie „żądać" od pozostałych administratorów podjęcia określonego działania, nie może natomiast ingerować w ich działania w inny sposób. Właściwe wywiązywanie się przez nich z tego obowiązku może być przedmiotem weryfikacji w ramach odrębnych postępowań, w tym kontrolnych prowadzonych przez właściwe organy.

Nawiązując do sposobu realizacji omawianego prawa warto zauważyć, że imperatywne brzmienie przepisu[661] sugeruje, że jego wykonanie nie wymaga dodatkowego działania osoby, której dane dotyczą. Następuje ono zawsze, gdy administrator jest obowiązany do usunięcia danych osoby w trybie art. 17 ust. 1 RODO. Innego zdania jest M. Czerniawski, który słusznie zauważa, że na żądanie osoby, której dane dotyczą, należy od tego odstąpić. Ma to służyć przede wszystkim ochronie osoby przed nagłośnieniem sprawy usuwania informacji jej dotyczących i niezamierzonego ich rozpowszechnienia[662].

Odnosząc się do obydwu omawianych praw należy podkreślić, że można je zasadniczo wykonywać w każdym czasie, RODO nie wprowadza bowiem ograniczeń temporalnych. Prawa te nie będą jednak wykonywane w ten sam sposób względem wszystkich osób. W niektórych sytuacjach ich realizacja nie jest dopuszczalna nawet, gdy wystąpią pozytywne przesłanki określone w przepisie art. 17 ust. 1 i 2 RODO. Przy-

[660] Motyw 65 preambuły RODO.

[661] „Jeżeli administrator upublicznił dane osobowe […], to […] podejmuje rozsądne działania".

[662] M. Czerniawski, *Komentarz do art. 17...*, s. 524–525.

padki te zostały ujęte w enumeratywnym katalogu zawartym w art. 17 ust. 3 RODO. Dotyczą one konfliktu interesu indywidualnego z interesem publicznym lub z innymi prawami albo obowiązkami, uznanymi w tym przypadku za nadrzędne[663]. Zapewniając wykonywanie prawa administrator jest związany terminami określonymi w art. 12 RODO i obowiązkami informacyjnymi określonymi w art. 19 RODO.

6. Prawo do ograniczenia przetwarzania danych osobowych

Prawo do ograniczenia przetwarzania danych osobowych w kształcie nadanym przepisami RODO „jest nowością w konglomeracie uprawnień osób, których dane dotyczą"[664]. Jest rozszerzeniem i wzmocnieniem prawa zablokowania danych, uregulowanego dotychczas w dyrektywie 95/46/WE. Realizuje jeden z głównych celów RODO, którym jest zwiększenie zakresu kontroli sprawowanej przez osoby, których dane dotyczą[665].

RODO definiuje wyrażenie „ograniczenie przetwarzania". Jest to „oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania"[666]. Definicja ta jest obarczona błędem *idem per idem*. W celu ustalenia jej znaczenia należy sięgnąć do języka potocznego.

[663] Są nimi: a) korzystanie z prawa do wolności wypowiedzi i informacji; b) wywiązanie się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega administrator, lub wykonanie zadania realizowanego w interesie publicznym czy w ramach sprawowania władzy publicznej powierzonej administratorowi; c) względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h oraz i, a także art. 9 ust. 3; d) cele archiwalne w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub e) ustalenie, dochodzenie lub obrona roszczeń.

[664] A. Nerka, *Prawo do ograniczenia przetwarzania danych osobowych*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017, s. 225.

[665] M. Czerniawski, *Komentarz do art. 18*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018s. 531.

[666] Artykuł 4 pkt 3 RODO.

Termin „ograniczony" oznacza m.in. „zamkniętego w szczupłych granicach, mającego niewielki zakres"[667]. Uwzględniając to znaczenie i brzmienie przepisu art. 18 RODO można przyjąć, że ograniczenie przetwarzania polega na oznaczeniu przez administratora danych osobowych osoby, której dane dotyczą, i zawężeniu sposobów ich przetwarzania wyłącznie do jednego z nich, którym jest przechowywanie.

Legalne przetwarzanie danych przez administratora w inny sposób (np. poprzez modyfikowanie lub wykorzystywanie) jest możliwe wyłącznie po uzyskaniu uprzedniej zgody osoby, której dane dotyczą, lub zrealizowaniu przesłanek określonych w art. 18 ust. 2 RODO[668]. Uchylenie ograniczenia przetwarzania danych wymaga uprzedniego poinformowania o nim osoby, której dane dotyczą. Obowiązek ten spoczywa na administratorze danych[669].

Wykonywanie prawa do ograniczenia przetwarzania danych osobowych nie powoduje tak dalece idących skutków jak wykonywanie prawa do usunięcia danych. W przypadku ograniczenia przetwarzania dane osobowe są nadal przechowywane, a ich oznaczenie, przechowywanie i chronienie przed przetwarzaniem w inny sposób niż przechowywanie[670] jest obowiązkiem administratora. Oznaczenie danych powinno nastąpić w sposób umożliwiający ich jednoznaczne odróżnienie od innych danych.

Osoba, której dane dotyczą, może zażądać ograniczenia przetwarzania jej danych w dowolnej formie. RODO nie wprowadza w tym zakresie szczególnych wymogów. Żądanie może zatem przyjąć formę ustną lub pisemną, w tym elektroniczną. Może być skierowane do administra-

[667] S. Skorupka, H. Auderska, Z. Łempicka (red.), *Mały słownik języka…,* s. 501.

[668] Są nimi: ustalenie dochodzenia lub obrony roszczeń, ochrona praw innej osoby fizycznej lub prawnej albo istnienie ważnych względów interesu publicznego Unii Europejskiej lub państwa członkowskiego.

[669] Artykuł 19 ust. 3 RODO.

[670] Mowa przede wszystkim o: utrwalaniu, organizowaniu, porządkowaniu, adaptowaniu lub modyfikowaniu, pobieraniu, przeglądaniu, wykorzystywaniu, ujawnianiu poprzez przesłanie, rozpowszechnianiu lub innego rodzaju udostępnianiu, dopasowywaniu lub łączeniu, ograniczaniu, usuwaniu lub niszczeniu (art. 4 pkt 2 RODO).

tora w każdym czasie. Powinno umożliwiać identyfikację osoby, od której pochodzi. RODO nie wymaga, aby określało ono precyzyjnie zakres danych, których przetwarzanie ma zostać ograniczone. Jeśli coś innego nie wynika z treści żądania osoby, której dane dotyczą, należy przyjąć, że odnosi się ono do wszystkich jej danych osobowych przetwarzanych przez tego administratora.

Należy opowiedzieć się za tym, że żądanie powinno wskazywać powód ograniczenia przetwarzania. Zgodnie z art. 18 ust. 1 RODO osoba, której dane dotyczą, ma bowiem prawo żądania ograniczenia przetwarzania, gdy:

1) kwestionuje prawidłowość danych osobowych (w tym przypadku ograniczenie może nastąpić na okres pozwalający administratorowi sprawdzić prawidłowość danych);
2) przetwarzanie jest niezgodne z prawem, a osoba ta sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
4) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania (w tym przypadku ograniczenie następuje do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą).

Przepisy prawa powszechnie obowiązującego nie określają procedury rozpatrzenia żądania. Można więc przyjąć, że administrator powinien przede wszystkim ustalić tożsamość osoby formułującej żądanie oraz to, czy wystąpiła przesłanka określona w żądaniu. Administrator nie jest zobowiązany do dokonania kompleksowej analizy realizacji wszystkich przesłanek, w tym wykraczających poza żądanie osoby, której dane do-

tyczą. Przemawia za tym cel regulacji, którym jest zwiększenie kontroli sprawowanej przez osoby, których dane dotyczą.

Weryfikując zrealizowanie określonych w żądaniach przesłanek, administrator powinien wziąć pod uwagę różne kwestie. W przypadku pierwszej przesłanki powinien uwzględnić przede wszystkim zasadę prawidłowości danych, określoną w przepisie art. 5 ust. 1 lit. d RODO oraz przeanalizować prawidłowość i aktualność zgromadzonych danych oraz ich niezbędność dla realizacji celów przetwarzania. W przypadku drugiej przesłanki administrator powinien przede wszystkim ustalić czy dokonywane przez niego przetwarzanie spełnia wymogi określone w art. 6–l4 RODO, a więc czy ma on prawo przetwarzać określone dane osobowe, czy ma niezbędną zgodę na przetwarzanie (gdy jest ona wymagana), czy we właściwy sposób zrealizował obowiązki informacyjne względem osoby, której dane dotyczą, oraz czy we właściwy sposób zabezpiecza jej dane. W przypadku trzeciej przesłanki powinien wziąć pod uwagę zasadę minimalizacji danych osobowych i zasadę ograniczenia czasowego. Powinien również ustalić, czy dane są „potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń". RODO nie wymaga udowodnienia, że dane są niezbędne dla celów konkretnych postępowań. Wydaje się więc, że wystarczające dla realizacji tej przesłanki będzie oświadczenie osoby, której dane dotyczą. Ostatnia przesłanka jest stosowana niejako „automatycznie", wniesienie sprzeciwu przez osobę, której dane dotyczą, skutkuje bowiem czasowym ograniczeniem przetwarzania tych danych[671].

Jeśli wystąpiły wymagane przesłanki, administrator ogranicza przetwarzanie danych osobowych w wymaganym zakresie. Dobór metody ograniczenia przetwarzania zależy od sposobu przetwarzania danych. Może to nastąpić m.in. poprzez czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do tych danych lub czasowe ich usunięcie ze strony inter-

[671] A. Nerka, *op. cit.*, s. 241–243.

netowej. W przypadku zautomatyzowanych zbiorów danych przetwarzanie należy zasadniczo ograniczyć środkami technicznymi, tak aby dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmienione. Informację dotyczącą wprowadzonego ograniczenia przetwarzania zaznacza się wyraźnie w systemie[672].

W związku z zapewnieniem realizacji omawianego prawa administrator jest związany terminami określonymi w art. 12 RODO i obowiązkami informacyjnymi określonymi w art. 19 RODO.

Na marginesie warto zauważyć, że ograniczenie przetwarzania danych osobowych może nastąpić nie tylko w konsekwencji realizacji praw osób, których dane dotyczą, lecz także wskutek działania organu nadzorczego. Dysponuje on bowiem uprawnieniami naprawczymi, w których zakresie mieści się wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania[673].

7. Prawo do przenoszenia danych osobowych

Przenoszenie danych osobowych jest nowym prawem przyznanym osobie, której dane dotyczą. Jest ono uznawane za istotne narzędzie służące wsparciu swobodnego przepływu danych osobowych wewnątrz Unii Europejskiej i rozwijaniu konkurencji między poszczególnymi administratorami, w szczególności świadczącymi usługi. Służy ono przede wszystkim ochronie praw osób, których dane dotyczą[674], i jest odpowiedzią na istniejące dotychczas problemy i trudności w zakresie przenoszenia danych osobowych między podmiotami świadczącymi usługi[675].

[672] Motyw 67 preambuły RODO.

[673] Motyw 129 preambuły i art. 38 ust. 2 lit. f RODO.

[674] Grupa Robocza art. 29, *Wytyczne dotyczące prawa do przenoszenia danych*, wersja el., s. 3–4, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 [dostęp 19.07.2018].

[675] P. Lambert, *Understanding the New European Data Protection Rules*, Taylor & Francis Group, Boca Raton 2018.

Twierdzi się, że prawo to jest „szansą na «przywrócenie równowagi» w stosunkach między osobami, których dane dotyczą, i administratorami danych”[676]. Trudno jednak zgodzić się z tym poglądem, bowiem administratorzy danych – w szczególności będący jednocześnie usługodawcami – mają silniejszą pozycję (faktyczną i prawną) od osób, których dane dotyczą. Niejednokrotnie dysponują wykwalifikowaną kadrą pracowniczą, w tym profesjonalnymi pełnomocnikami oraz mają wieloletnie doświadczenie i dominującą pozycję na rynku w świadczeniu określonych usług. Przykładowo, przyznanie prawa przenoszenia danych osobie zamieszkującej w miejscowości nieobjętej zasięgiem co najmniej dwóch sieci komórkowych – mimo że teoretycznie wzmacnia jej pozycję prawną – nie wpływa na nią w sposób istotny w praktyce. Wobec braku odpowiedniej infrastruktury i podmiotów konkurujących między sobą wykonywanie tego prawa nie przynosi bowiem zamierzonych efektów.

Warunkiem wykonywania prawa do przenoszenia danych jest łączna realizacja dwóch przesłanek. Pierwsza to przetwarzanie przez administratora danych osobowych w sposób zautomatyzowany[677]. Prawo to nie odnosi się więc do większości dokumentów wytwarzanych w formie papierowej. Druga to przetwarzanie tych danych na podstawie zgody (w tym wyraźnej) udzielonej w konkretnym celu lub celach przetwarzania przez osobę, której dane dotyczą[678], albo przetwarzanie ich na podstawie umowy – której stroną jest osoba, której dane dotyczą – gdy jest ono niezbędne do wykonania tej umowy[679]. Prawo to nie może być wykonywane w innych przypadkach, np. gdy przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Wpisuje

[676] Grupa Robocza art. 29, *op. cit*., s. 4.

[677] Motyw 68 preambuły i art. 20 ust. 1 lit. b RODO.

[678] Artykuł 20 ust. 1 lit. a RODO w zw. z art. 6 ust. 1 lit. a oraz art. 9 ust. 2 lit. a RODO.

[679] Artykuł 20 ust. 1 lit. a RODO w zw. z art. 6 ust. 1 lit. b RODO.

się to zatem w cel tej regulacji, którym jest wpływanie na rozwój konkurencji między administratorami.

Zgodnie z art. 20 ust. 1–2 RODO prawo do przenoszenia danych umożliwia osobie, której dane dotyczą:

1) otrzymanie danych osobowych jej dotyczących[680] w ustrukturyzowanym, powszechnie używanym formacie[681] nadającym się do odczytu maszynowego, a więc umożliwiającym ich swobodny odczyt przez komputer[682]. Jeżeli jest to możliwe, dane powinny być przekazane w sposób i w formacie wskazanym przez osobę wykonującą prawo (np. mailowo lub na nośniku danych). Osoba, której dane dotyczą, może poprzestać na realizacji tylko tego uprawnienia. Będzie ono wówczas uzupełnieniem prawa dostępu do danych i będzie służyć „celom własnym" tej osoby[683];
2) samodzielne przesłanie tych danych innemu administratorowi, bez przeszkód ze strony administratora, który umożliwił wykonywanie prawa dostępu. Przed przesłaniem danych osoba, której dane dotyczą, ma prawo dokonania selekcji przenoszonych danych, uwzględniając cele przetwarzania;
3) żądanie od administratora przesłania tych danych bezpośrednio innemu administratorowi, jeżeli jest to możliwe technicznie. Administrator, który przesyła dane, nie jest odpowiedzialny za przetwarzanie danych przez administratora, który je otrzymuje. Ten

[680] Grupa Robocza art. 29 postuluje, aby wyrażenie „dane osobowe jej dotyczące" nie było interpretowane zbyt restrykcyjnie. Przykładowo, jeśli bank przetwarza dane dotyczące transakcji na koncie, to realizując prawo do przeniesienia nie musi on usuwać lub anonimizować danych osobowych powiązanych z wszystkimi wpływami zewnętrznymi (Grupa Robocza art. 29, *op. cit*., s. 13).

[681] Dyrektywa 95/46/WE nie stwarzała osobom, których dane dotyczą, możliwości wpływu na format danych, w którym zostaną one udostępnione.

[682] W punkcie 68 preambuły RODO mowa jest dodatkowo o interoperacyjnym formacie danych.

[683] Osoba, której dane dotyczą, może np. żądać przesłania jej historii transakcji dokonywanych jej kartą płatniczą, ponieważ zamierza ustalić, które wydatki można ograniczyć.

ostatni dokonuje wstępnej selekcji danych, z uwzględnieniem celów przetwarzania[684]. Jako nowy administrator jest on bowiem obowiązany do przestrzegania przepisów dotyczących przetwarzania, w szczególności zasad wyrażonych w art. 5 RODO.

Prawo do przenoszenia danych polega zatem na ich przekazaniu osobie, której dane dotyczą, lub wskazanemu przez nią administratorowi. Jest ono odrębnym prawem przysługującym osobie, której dane dotyczą. Nie skutkuje usunięciem danych lub ograniczeniem dostępu do nich. Administrator, który dokonuje przeniesienia danych, nie traci z tego powodu dotychczasowego statusu administratora. Przeniesienie nie wpływa także na realizację innych praw przysługujących osobie, której dane dotyczą, ani nie może wpływać niekorzystnie na prawa i wolności innych osób[685].

Prawo do przenoszenia danych znajduje zastosowanie wyłącznie do danych osobowych, które osoba dostarczyła administratorowi bezpośrednio lub pośrednio. Bezpośrednie dostarczenie polega na aktywnym i świadomym działaniu osoby, której dane dotyczą. Ma ona świadomość udzielania określonych informacji administratorowi danych i godzi się na to, np. podając swoje imię i nazwisko oraz wiek i adres zamieszkania. Pośrednie dostarczenie polega natomiast na gromadzeniu przez administratora danych dotyczących osoby poprzez obserwowanie jej aktywności podczas korzystania z określonej usługi lub urządzenia[686]. Przykładowo, osoba mająca konto i korzystająca z krokomierza dostarcza pośrednio administratorowi informacji na temat swojej lokalizacji i częstotliwości podejmowanej aktywności fizycznej.

W nauce prawa wyrażany jest pogląd, że dane zaobserwowane nie powinny być uznane za „dostarczone przez osobę", nie znajduje to bowiem oparcia w przepisach prawa i spowoduje wiele problemów praktycznych

[684] Grupa Robocza art. 29, *WP242 ZAŁĄCZNIK – Często zadawane pytania*, wersja el., s. 1, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 [dostęp 19.07.2018].

[685] Artykuł 20 ust. 4 RODO.

[686] Grupa Robocza art. 29, *Wytyczne dotyczące prawa…*, s. 12.

w zakresie realizacji tego prawa[687]. Przyjęcie tego stanowiska oznaczałoby poszerzenie zakresu danych gromadzonych przez administratorów, które pozostają niejako „poza kontrolą" osoby, której one dotyczą. Jeśli osoba ta korzysta z pewnych funkcji urządzenia (np. funkcji lokalizacji), to ma ona świadomość gromadzenia przez administratora konkretnych danych. W tym przypadku przez swoje działanie dostarcza administratorowi danych dotyczących jej położenia w sposób pośredni. Uniemożliwienie wykonywania prawa do przenoszenia danych względem tej kategorii danych oznaczałoby osłabienie pozycji prawnej osoby, której dane dotyczą, i stałoby w sprzeczności z celem RODO, którym jest zwiększenie kontroli osób nad ich danymi.

Poza zakresem prawa do przenoszenia danych[688] pozostają dane wywnioskowane i wywiedzione przez administratora na podstawie danych dostarczonych przez osobę, której dane dotyczą. Chodzi o dane, które uzyskuje on na podstawie analizy aktywności tej osoby i dostarczonych przez nią danych, np. przydzielenia punktów w ocenie kredytowej. Mimo że administrator przetwarza je i są one częścią profilu tej osoby, nie są one objęte prawem do przeniesienia[689].

Prawo do przenoszenia danych może być wykonywane w każdym czasie pod warunkiem, że administrator przetwarza dane dotyczące określonej osoby. Żądanie przeniesienia danych może być skierowane do administratora danych w dowolnej formie. Mając na uwadze specyfikę prawa, najczęściej będzie to forma elektroniczna. Administrator może także umożliwić realizację prawa np. przez samodzielne pobranie przez osobę danych z jej konta internetowego. Nie będzie wówczas potrzebne jego pośrednictwo.

---

[687] M. Czerniawski, *Komentarz do art. 20*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 545–546.

[688] Zdaniem A. Krasuskiego poza zakresem tego prawa znajdują się także dane będące w chmurze obliczeniowej, które dostawca usług przetwarza w sposób zagregowany i nie jest możliwa identyfikacja określonej osoby fizycznej oraz dane, które nie dotyczą tej osoby (A. Krasuski, *Ochrona danych osobowych…*, s. 261).

[689] *Ibidem*.

Jeśli administrator otrzyma wniosek o przeniesienie danych, weryfikuje tożsamość osoby, od której on pochodzi, aby jak najpełniej chronić przetwarzane dane. Następnie ustala zakres żądania i sposób jego realizacji. Jeżeli nic innego nie wynika z treści żądania, odnosi się ono do wszystkich przetwarzanych przez administratora danych dotyczących tej osoby. Jeśli dane te mają dużą pojemność i nie jest możliwe ich przeniesienie w żądanej formie (np. mailowej), może on zwrócić się do wnioskodawcy z prośbą o wyrażenie zgody na inny sposób przeniesienia. Działanie to powinno mieć wyjątkowy charakter, RODO wskazuje bowiem na konieczność opracowywania interoperacyjnych formatów umożliwiających przenoszenie danych[690]. W zakresie realizacji omawianego prawa administrator jest związany terminami określonymi w art. 12 RODO.

8. Prawo do sprzeciwu wobec przetwarzania danych osobowych

Prawo do sprzeciwu wobec przetwarzania danych osobowych przysługiwało osobie, której dane dotyczą, na podstawie przepisów dyrektywy 95/46/WE[691]. Mogła ona je realizować – w określonych w dyrektywie przypadkach – z ważnych i uzasadnionych przyczyn wynikających z jej konkretnej sytuacji. W szczegółowych wywodach podkreślano jednak, że sposób sfomułowania prawa w dyrektywie nie gwarantuje jego skutecznej realizacji. Dotyczyło to przede wszystkim obszaru „nowych technologii przetwarzania danych oraz nowych środowisk i usług, takich jak internet i portale społecznościowe”[692]. Z uwagi na to, przepisy RODO modyfikują to prawo.

[690] Motyw 68 preambuły RODO.

[691] Chodzi przede wszystkim o art. 14 oraz motyw 25 i 45 preambuły tej dyrektywy.

[692] M. Krzysztofek, *Prawo do sprzeciwu wobec przetwarzania danych osobowych w rodo*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017, s. 291.

W aktualnym stanie prawnym osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych osobowych, nawet gdy jest ono zgodne z prawem[693]. Sprzeciw wobec przetwarzania – zależnie od sytuacji i terminu wniesienia – może powodować ograniczenie przetwarzania danych osobowych[694] lub ich usunięcie[695].

„Główną różnicą między prawem do sprzeciwu a prawem do usunięcia danych jest to, że pierwsze z nich skupia się na określonej operacji przetwarzania, podczas gdy drugie odnosi się w ogólności do danych osobowych. To rozróżnienie ma szczególne znaczenie w kontekście usług społeczeństwa informacyjnego, w ramach których te same dane są często przetwarzane do znacznej liczby celów. Prawo do sprzeciwu zapobiega tylko dalszemu przetwarzaniu dla jednego lub większej liczby określonych celów, podczas gdy prawo do usunięcia danych zapobiega jakiemukolwiek przetwarzaniu i dane nie mogą być już dłużej przechowywane przez administratora”[696].

Prawo do sprzeciwu jest ściśle związane z celami przetwarzania. Jego wykonywanie jest możliwe, gdy przetwarzanie danych następuje dla celów określonych w RODO. W niektórych przypadkach konieczne jest również zrealizowanie dodatkowych przesłanek.

Biorąc pod uwagę cele przetwarzania danych osobowych i skutki wniesienia sprzeciwu, prawo do sprzeciwu można podzielić na trzy grupy.

1. Pierwsza grupa obejmuje sprzeciw wobec przetwarzania danych osobowych do celów marketingu bezpośredniego i sprzeciw wobec profilowania na potrzeby związane z tym marketingiem[697].

[693] Motyw 69 preambuły RODO.

[694] Zob. art. 18 ust. 1 lit. d RODO.

[695] Zob. art. 17 ust. 1 lit. c w zw. z art. 21 ust. 1–2 RODO.

[696] J. Ausloos, *The Interaction between the Rights to Object and to Erasure in the GDPR*, wersja el., https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and -the-right-to-erasure/ [dostęp 20.07.2018].

[697] Polega on na kierowaniu specjalnie dobranych komunikatów i informacji bezpośrednio do konsumenta. Nie używa się dodatkowych kanałów dystrybucji. Obejmuje on zróżnicowane działania, w szczególności reklamę z kanałem zwrotnej odpowiedzi (z podaniem adresu lub lin-

Ich wniesienie skutkuje niedopuszczalnością dalszego przetwarzania danych dla tych celów[698]. Chodzi np. o sytuacje, w których w wyniku przeglądania określonej strony internetowej przez osobę są zapisywane pliki *cookies* z informacją o odwiedzanej stronie. Są one następnie wykorzystywane do wyświetlania produktów z tej strony w postaci spersonalizowanych reklam na innych stronach internetowych odwiedzanych przez tę osobę. Jeśli osoba ta sprzeciwia się wyświetlaniu tych reklam, które jest wynikiem profilowania, ma prawo wnieść sprzeciw wobec przetwarzania. Administrator danych jest nim związany i nie jest uprawniony do dokonywania oceny jego zasadności. Jeśli osoba tego zażąda, powinien on również niezwłocznie usunąć jej dane osobowe[699]. Sprzeciw może być złożony w dowolnej formie[700] i nie musi zawierać uzasadnienia.

2. Druga grupa obejmuje sprzeciw wobec przetwarzania danych osobowych – w tym profilowania – które jest niezbędne dla:
   a) wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub
   b) osiągnięcia celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wyma-

ku, pod którym można dokonać zakupu), reklamę pocztową i sprzedaż katalogową (B. Lundén, U. Svensson, *Marketing dla małych i średnich przedsiębiorstw*, BL Info Polska, Gdańsk 2014, wyd. 5, s. 144).

[698] Motyw 70 preambuły i art. 21 ust. 2–3 RODO.

[699] Zob. art. 17 ust. 1 lit. c RODO.

[700] RODO dopuszcza wprost wykonywanie tego prawa „za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne", a więc także w formie elektronicznej (art. 21 ust. 5 RODO).

gające ochrony tych danych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem[701].

Wniesienie sprzeciwu wobec przetwarzania danych w tych przypadkach nie zobowiązuje administratora danych do jego uwzględnienia. Następuje to dopiero, gdy ustali on, że zrealizowano jedną z wymienionych przesłanek i sprzeciw wynika „z przyczyny związanej ze szczególną sytuacją" osoby, której dane dotyczą[702].

Ciężar udowodnienia istnienia przesłanek spoczywa na osobie wnoszącej sprzeciw (osobie, której dane dotyczą). Sprzeciw powinien więc zawierać uzasadnienie. RODO nie wprowadza wymogów dotyczących terminu jego wniesienia, może on więc zostać wniesiony w dowolnym czasie. Nie ma również wytycznych co do formy. Zasadne wydaje się jednak zastosowanie formy pisemnej (w tym elektronicznej). Zabezpiecza ona bowiem pełniej prawa osoby wnoszącej sprzeciw, ułatwiając przeprowadzenie kontroli prawidłowości działania administratora w przypadku nieuwzględnienia żądania osoby, której dane dotyczą.

Jeśli sprzeciw zostanie uwzględniony, administrator nie może już przetwarzać danych objętych sprzeciwem. Gdy nie ma nadrzędnych prawnie uzasadnionych podstaw przetwarzania, to osoba, której dane dotyczą, może żądać usunięcia jej danych[703].

W niektórych przypadkach – mimo kumulatywnego zrealizowania wymienionych przesłanek i wykazania ich w sprzeciwie – administrator może nadal przetwarzać dane. Następuje to, gdy wykaże on, że istnieją ważne, prawnie uzasadnione podstawy do przetwarzania, nadrzędne względem interesów, praw i wolności osoby, której dane dotyczą, lub że istnieją podstawy do

[701] Artykuł 21 ust. 1w zw. z art. 6 ust. 1 lit. e i f RODO.
[702] Artykuł 21 ust. 1 RODO.
[703] Zob. art. 17 ust. 1 lit. c RODO.

ustalenia, dochodzenia lub obrony roszczeń[704]. Aby nadal przetwarzać dane, administrator powinien wykazać istnienie przesłanki, na którą się powołuje. Do czasu jej wykazania przetwarzanie jest ograniczone[705].

Warto zwrócić uwagę na zagrożenia wynikające z pełnienia podwójnej roli przez administratora. Dokonuje on bowiem oceny i wartościowania przesłanek, na które się powołuje, oraz przesłanek, których istnienie wykazuje osoba, której dane dotyczą. W każdym z tych przypadków przepisy prawa formułują przesłanki w sposób ogólny i posługują się pojęciami niedookreślonymi. Administrator mający silniejszą pozycję prawną od osoby, której dane dotyczą, może ją wykorzystywać dla realizacji własnych celów. Istotne jest więc zapewnienie dostępności i sprawnego funkcjonowania organów zapewniających ochronę praw osób, których dane dotyczą.

3. Trzecia grupa obejmuje sprzeciw wobec przetwarzania danych osobowych, które następuje do celów badań naukowych, historycznych lub statystycznych na mocy przepisu art. 89 ust. 1 RODO[706]. Sprzeciw ten może zostać wniesiony w dowolnym czasie i formie. Powinien on zawierać uzasadnienie, ponieważ osoba, której dane dotyczą, powinna wykazać w nim istnienie „przyczyn związanych z jej szczególną sytuacją". Chodzi o wykazanie konkretnych przyczyn, których doniosłość uzasadnia zaprzestanie przetwarzania danych osobowych w tym przypadku.

Otrzymując sprzeciw, administrator dokonuje weryfikacji tożsamości osoby go wnoszącej i wykazywanych w nim przesła-

[704] *Ibidem*.

[705] Artykuł 18 ust. 1 lit. d RODO.

[706] Artykuł 21 ust. 6 RODO. Warto podkreślić, że przepis art. 89 ust. 1 RODO – w kontekście przetwarzania danych do tych celów – nakazuje zastosowanie odpowiednich zabezpieczeń dla praw i wolności osoby, której dane dotyczą. Chodzi przede wszystkim o wdrożenie odpowiednich środków i stosowanie określonych zasad przetwarzania danych.

nek. W tym zakresie wiążą go terminy określone w art. 12 RODO. Warto zauważyć, że w analizowanym przepisie – podobnie jak w przypadku określonym w art. 21 ust. 1 RODO – prawodawca przewiduje istnienie konfliktu interesów. W tym przypadku uznaje on jednak apriorycznie prymat interesu publicznego nad interesem jednostki. Jeśli administrator stwierdzi, że przetwarzanie określonych danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym, to osobie, której dane dotyczą, prawo sprzeciwu nie przysługuje[707]. Pozycja prawna osoby, której dane dotyczą ulega zatem osłabieniu.

Rozważenia wymaga kwestia, w jakiej formie powinno nastąpić udzielenie odpowiedzi na sprzeciw, gdy administrator stwierdzi, że przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym. Prezentowany jest pogląd, że „w takiej sytuacji administrator dysponuje dodatkową podstawą umożliwiającą odrzucenie sprzeciwu"[708]. Nie jest on jednak zasadny, bowiem RODO nie określa procedury postępowania w tym przypadku i nie wprowadza środka, którym jest „odrzucenie sprzeciwu". Nie przewiduje go również k.p.a., które *nota bene* nie znajduje zastosowania w niniejszej sprawie. „Odrzucenie" określają przepisy prawa regulujące postępowania sądowe[709]. Jest ono skutkiem podjęcia czynności procesowej w formie prawnej postanowienia. Nie znajdzie ono więc zastosowania w niniejszej sprawie. Należy zatem przyjąć, że administrator da-

[707] „Osoba, której dane dotyczą, ma prawo wnieść sprzeciw […] chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym". W ten sam sposób konstrukcję tego prawa ujęto w wersji angielsko-, niemiecko- i francuskojęzycznej.

[708] M. Czerniawski, *Komentarz do art. 21*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 559.

[709] Zob. np. ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2018 r., poz. 1302), ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2018 r., poz. 1360).

nych osobowych powinien skierować do osoby wnoszącej sprzeciw pismo informacyjne, w którym wskazuje, że dokonywane przez niego przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym. Powinien on powołać się na konkretne realizowane przez niego zadanie. Zadanie to powinno być ujawnione przez administratora już podczas realizacji obowiązku informacyjnego. Informacja o tym może także widnieć na jego stronie internetowej, jeśli ją posiada. Zadaniem administratora jest ponadto wprowadzenie konkretnych procedur ułatwiających osobom, których dane dotyczą, realizację ich praw[710]. Przyczyni się to do zwiększenia przejrzystości i zapewnienia jednolitości stosowanych procedur.

9. Prawo do wniesienia skargi do organu nadzorczego

Przyznanie praw osobom, których dane dotyczą – bez jednoczesnego zagwarantowania środków ochrony prawnej zabezpieczających ich skuteczną realizację – byłoby wyłącznie niezobowiązującą deklaracją prawodawcy. Osoby te byłyby bowiem pozbawione możliwości wykonywania tych praw, w przypadku ich naruszenia.

Istotną rolę dla ochrony praw osób, których dane dotyczą, odgrywają środki ochrony prawnej określone w rozdziale VIII RODO. Są nimi prawo do wniesienia skargi do organu nadzorczego w związku z naruszeniem przepisów rozporządzenia, prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu i prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu. Środki te są względem siebie komplemen-

[710] Motyw 59 preambuły RODO.

tarne. Oznacza to, że mogą być wykonywane bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej[711].

Prawo do wniesienia skargi do organu nadzorczego przysługiwało osobie, której dane dotyczą, na podstawie przepisów dyrektywy 95/46/WE[712], która regulowała je w sposób szczątkowy. Sygnalizowała raczej jego istnienie niż określała konkretne elementy tego prawa. Szczegółowe kwestie związane z wniesieniem skargi, w szczególności dotyczące właściwych organów i procedur, określały samodzielnie państwa członkowskie[713].

RODO formułuje prawo do wniesienia skargi do organu nadzorczego bardziej szczegółowo niż dyrektywa 95/46/WE. Wyznacza jego ramy, pozostawiając dookreślenie szczegółów związanych z jego wykonywaniem państwom członkowskim. Prawo do wniesienia skargi do organu nadzorczego zostanie omówione z uwzględnieniem regulacji polskiego prawa wewnętrznego, w szczególności przepisów rozdziału 7 u.o.d.o.

Wykonywanie prawa do wniesienia skargi jest warunkowane subiektywnym odczuciem osoby, której dane dotyczą[714]. Chodzi o sytuacje, gdy osoba, której dane dotyczą, twierdzi, że nastąpiło konkretne naruszenie. W tym przypadku może ona wnieść skargę do jednego organu nadzorczego[715]. RODO posługuje się stwierdzeniem „jeden organ nadzorczy", ponieważ dopuszcza się równoległe funkcjonowanie kilku organów nadzorczych w jednym państwie[716].

Osoba, której dane dotyczą, może w zasadzie dowolnie decydować o tym, do którego właściwego miejscowo organu nadzorczego wniesie skar-

[711] Artykuł 77 ust. 1 RODO.

[712] Zob. motyw 63 preambuły i art. 28 ust. 4 dyrektywy.

[713] M. Jagielski, *op. cit.*, s. 154.

[714] Zob. art. 77 ust. 1 RODO („każda osoba, której dane dotyczą ma prawo wnieść skargę […], *jeżeli sądzi* [podkr. – J. B.], że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie") i art. 79 RODO („osoba, której dane dotyczą ma prawo do skutecznego środka ochrony prawnej przed sądem, *jeżeli uzna* [podkr. J. B.] ona, że prawa przysługujące jej […] zostały naruszone".

[715] Motyw 141 preambuły RODO.

[716] Zob. art. 51 ust. 1 RODO.

gę. Może ona wnieść ją w państwie członkowskim jej zwykłego pobytu, jej miejsca pracy lub miejsca, w którym popełniono domniemane naruszenie[717]. Zawarte w przepisie wyliczenie ma charakter otwarty. Nie ma zatem formalnych przeszkód, aby wnieść skargę do organu nadzorczego mającego siedzibę w innym państwie członkowskim. Ustalając właściwy organ, należy wziąć pod uwagę wskazania zawarte w przepisie art. 56 RODO.

Należy podzielić pogląd, w myśl którego powinien istnieć związek między państwem, w którym jest rozpatrywana skarga, a osobą, której dane dotyczą lub miejscem popełnienia naruszenia[718]. Warto jednak zwrócić uwagę na inny powód uzasadniający istnienie tego związku. Jest nim ryzyko wystąpienia „turystyki skargowej", a więc wybierania przez podmioty danych określonego organu nadzorczego z powodu szybszego rozpatrywania przez niego spraw lub wydawania rozstrzygnięć bardziej korzystnych w ocenie osób wnoszących skargi. Mimo że postuluje się wzajemną wymianę informacji między organami i dąży się do jednolitości rozstrzygnięć i spójnego stosowania przepisów RODO, występowania tego problemu nie można wykluczyć w praktyce[719].

Organem właściwym w sprawie ochrony danych osobowych, w tym w zakresie rozpatrywania skarg w przedmiocie naruszenia przepisów RODO jest w Rzeczypospolitej Polskiej Prezes Urzędu Ochrony Danych Osobowych[720]. Jest to organ centralny, którego obszar działania obejmuje terytorium całego państwa[721]. Stoi on na czele Urzędu Ochrony Danych Osobowych[722].

[717] Artykuł 77 ust. 1 RODO.

[718] A. Mednis, *Prawo do wniesienia skargi do organu nadzorczego*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017, s. 349.

[719] Zob. np. motyw 36, 116, 123, 135, 138 i art. 50–51, 57, 60–63 RODO.

[720] Artykuł 34 ust. 1 i art. 60 u.o.d.o., art. 51 RODO.

[721] Sposób wyłonienia jego piastuna i jego kompetencje określa ustawa. Określa ona również działający przy nim organ pomocniczy, którym jest Rada do Spraw Ochrony Danych Osobowych.

[722] Zastąpił on funkcjonującego dotychczas Generalnego Inspektora Ochrony Danych Osobowych.

Skargi do tego organu można wnosić w formie pisemnej, w tym elektronicznej – także wypełniając dostępny na stronie internetowej formularz skargi – lub ustnie do protokołu[723]. Powinny one spełniać wymogi przewidziane dla podania[724], a ponadto wskazywać jednoznacznie podmiot, który – w ocenie wnoszącego skargę – dokonał naruszenia, szczegółowy opis naruszenia i konkretne żądanie, tj. sformułowanie działań, których podjęcia domaga się wnoszący skargę (np. żądanie sprostowania danych lub ich usunięcia). Udzielenie tych informacji jest istotne, ponieważ postępowanie wyjaśniające na podstawie skargi jest prowadzone „w zakresie odpowiadającym konkretnej sprawie"[725].

Postępowanie w sprawie naruszenia przepisów o ochronie danych jest wszczynane z inicjatywy osoby, której dane dotyczą[726]. Może ona działać samodzielnie lub przez pełnomocnika (w tym profesjonalnego)[727] albo umocować do reprezentowania podmiot, organizację lub zrzeszenie[728] spełniające wymogi określone w RODO[729]. Postępowanie jest sfor-

[723] Zob. *Składanie skargi w formie tradycyjnej, w tym do protokołu w siedzibie Prezesa Urzędu*, wersja el., https://uodo.gov.pl/pl/83/154 [dostęp 24.07.2018]. Formy te realizują postulaty formułowane w RODO, związane z ułatwieniem wnoszenia skarg (motyw 141 preambuły RODO).

[724] Zob. art. 63 § 2 k.p.a.

[725] Motyw 141 RODO.

[726] Motyw 141 i art. 77 RODO.

[727] Jest to możliwe, ponieważ art. 7 ust. 1 u.o.d.o. przyjmuje, że w sprawach nieuregulowanych w ustawie do postępowań administracyjnych przed Prezesem Urzędu Ochrony Danych Osobowych, o których mowa w rozdziałach 4–7 i 11, stosuje się k.p.a. Akt ten dopuszcza działanie przez pełnomocnika (art. 32–34 k.p.a.). Jest to zgodne z interpretacją dokonywaną przez Prezesa Urzędu Ochrony Danych Osobowych (zob. *Jeśli chcesz złożyć skargę…*, wersja el., https://uodo.gov.pl/pl/83/155 [dostęp 23.07.2018]). Nieuprawnione wydaje się więc stwierdzenie, że „z zakresu podmiotów, które mogą reprezentować podmioty danych, należy wykluczyć osoby fizyczne" (A. Mednis, *op. cit*., s. 348). Przyjęcie tej interpretacji oznaczałoby bowiem osłabienie pozycji prawnej osób, których dane dotyczą.

[728] W przepisie art. 61 u.o.d.o. mowa jest o „występowaniu w postępowaniu" organizacji społecznej.

[729] Są nimi: 1) należyte ustanowienie zgodnie z prawem państwa członkowskiego; 2) niezarobkowy charakter; 3) działanie w dziedzinie ochrony praw i wolności osób, których dane dotyczą; 4) określenie ich celów statutowych w sposób mieszczący się w zakresie interesów publicznych (art. 80 ust. 1 RODO).

malizowane i jednoinstancyjne[730]. Jego tryb określają przepisy rozdziału 7 u.o.d.o., a w zakresie nieuregulowanym przepisy k.p.a.

Przepisy u.o.d.o. wprowadzają dodatkową ochronę skarżącego w ramach postępowania w sprawie naruszenia przepisów o ochronie danych osobowych. Przyznają Prezesowi UODO kompetencję do przeprowadzenia w toku postępowania – w określonych prawem przypadkach – postępowania kontrolnego[731]. Służy ona realizacji zasady prawdy obiektywnej wyrażonej w przepisie art. 7 k.p.a. i stwarza możliwość uzyskania dowodów niezbędnych do ustalenia istnienia i zakresu zarzucanego naruszenia. Umożliwiają one ponadto zobowiązanie podmiotu, któremu zarzuca się naruszenie do ograniczenia przez niego przetwarzania określonych danych osobowych[732].

Przepisy RODO wymagają informowania skarżącego o postępach i efektach rozpatrywania skargi oraz dopuszczalności skorzystania z sądowego środka ochrony prawnej przeciwko organowi nadzorczemu[733]. Źródłem tego obowiązku są również przepisy k.p.a., przede wszystkim zasady ogólne postępowania[734].

Postępowanie w sprawie naruszenia przepisów o ochronie danych kończy wydanie decyzji administracyjnej przez Prezesa UODO. Ze względu na charakter sprawy należy wykluczyć zawarcie między stronami ugody. Przepisy prawa nie przewidują w tym przypadku również milczącego

[730] Artykuł 7 u.o.d.o.

[731] Postępowanie kontrolne można przeprowadzić, gdy istnieje konieczność uzupełnienia dowodów. Prowadzi się je zgodnie z przepisami rozdziału 9 u.o.d.o. (art. 68 u.o.d.o.).

[732] Może to nastąpić w określonych prawem przypadkach, z równoczesnym ustaleniem dopuszczalnego zakresu przetwarzania. Chodzi o sytuacje, w których w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki. Zobowiązanie podmiotu do ograniczenia przetwarzania danych następuje w formie postanowienia, na które przysługuje skarga do WSA (art. 70 u.o.d.o.).

[733] Artykuł 77 ust. 2 RODO.

[734] Szerzej na ich temat: B. Adamiak, *Komentarz do art. 6–16*, [w:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, C.H. Beck, wyd. 15, Warszawa 2017, s. 46–124.

załatwienia sprawy. Decyzja powinna spełniać wymogi określone w przepisie art. 107 k.p.a. i w motywie 129 RODO.

Decyzja może nakładać na sprawcę naruszenia administracyjną karę pieniężną, stosownie do przepisów art. 83 RODO i rozdziału 11 u.o.d.o. Kara jest niepodatkową należnością budżetową[735]. Jej nałożenie jest fakultatywne. RODO wymaga, aby była ona skuteczna, proporcjonalna i odstraszająca. Wymiar kary powinien być dostosowany do konkretnego przypadku. Decydując o jej wymierzeniu, organ bierze pod uwagę zobiektywizowane przesłanki, w tym zakres naruszenia, jego charakter i czas przez jaki ono występowało[736]. Kara nie powinna służyć realizacji partykularnych interesów skarżącego. Nie powinien on sugerować konieczności jej nałożenia ani jej wysokości. Decyzja w tym przedmiocie należy wyłącznie do organu. Skarżący nie może również skutecznie żądać przyznania jemu odszkodowania, jest ono bowiem przyznawane w ramach odrębnego postępowania.

Decyzja kończąca postępowanie jest ostateczna, nie przysługuje od niej odwołanie ani wniosek o ponowne rozpatrzenie sprawy[737]. Podlega ona zaskarżeniu do Wojewódzkiego Sądu Administracyjnego w Warszawie[738]. Wniesienie przez stronę skargi wstrzymuje wykonanie decyzji w zakresie administracyjnej kary pieniężnej[739].

10. Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu

Dyrektywa 95/46/WE zawierała szczątkowe regulacje dotyczące zaskarżania rozstrzygnięć organu nadzorczego. Stanowiła, że od decyzji organu

[735] Zgodnie z art. 104 u.o.d.o. jest ona dochodem budżetu państwa.

[736] Artykuł 83 ust. 1 RODO.

[737] Artykuł 16 § 1 k.p.a.

[738] Artykuł 13 § 2 p.p.s.a. Zob. J. Drachal, J. Jagielski, M. Cherka, *Komentarz do art. 13*, [w:] R. Hauser, M. Wierzbowski (red.), *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, C.H. Beck, Warszawa 2018, s. 180–181.

[739] Artykuł 74 u.o.d.o.

nadzorczego, względem którego były zgłaszane zastrzeżenia, przysługiwało odwołanie do właściwego sądu[740]. Określony w dyrektywie zakres praw przysługujących w przypadku działań i bezczynności organu nadzorczego był jednak ograniczony.

Przepisy RODO wprowadzają *expressis verbis* prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu. Biorąc pod uwagę osoby, którym przysługuje to prawo, można je ująć w dwie grupy.

Pierwsza grupa obejmuje osoby fizyczne i prawne, których dotyczy prawnie wiążąca decyzja organu nadzorczego[741]. Słusznie zauważa się, że w polskim porządku prawnym zakres ten obejmuje również jednostki organizacyjne nieposiadające osobowości prawnej[742]. Grupa ta dotyczy zatem szerokiego zakresu podmiotów. Są nimi w szczególności osoby, których dane dotyczą, administratorzy danych i podmioty przetwarzające.

Osobom tym przysługuje prawo do skutecznego środka ochrony prawnej przeciwko prawnie wiążącej decyzji organu nadzorczego ich dotyczącej, a więc decyzji oddziałującej na ich prawa lub obowiązki. RODO nie określa zakresu ani stopnia wymaganego oddziaływania. Szerokiej ochronie tych osób służyłoby przyjęcie interpretacji, zgodnie z którą oddziaływanie to może być nawet niewielkie. Szybkości postępowań sądowych i ograniczeniu nadużywania tego prawa służyłoby z kolei przyjęcie wąskiej interpretacji, w myśl której oddziaływanie powinno wpływać w istotny sposób na ich prawa lub obowiązki. Przepisy RODO nie wprowadzają jednak takiego wymagania. Precyzują natomiast wymogi dotyczące decyzji wskazując, że powinna ona być prawnie wiążąca. Może ona więc

[740] Artykuł 28 ust. 3 dyrektywy.

[741] Artykuł 78 ust. 1 RODO.

[742] Zob. J. Łuczak, *Komentarz do art. 78*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 1034; M. Górski, *Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017, s. 374.

dotyczyć m.in. prowadzonego przez organ postępowania wyjaśniającego, wykonywania przez niego uprawnień naprawczych, wydania lub odmowy wydania zezwolenia. Poza zakresem prawa pozostają więc w szczególności decyzje nieostateczne, zalecenia, opinie i instrukcje[743].

Druga grupa obejmuje wyłącznie osoby, których dane dotyczą. Przysługuje im dodatkowo prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli właściwy organ nadzorczy nie rozpatrzył ich skargi lub nie poinformował ich w terminie trzech miesięcy o postępach lub efektach rozpatrywania ich skargi, wniesionej na podstawie przepisu art. 77 RODO[744]. Osoby te są więc podwójnie chronione. Przepis art. 78 ust. 1 RODO zapewnia im ochronę przed działaniem organu nadzorczego, a przepis art. 78 ust. 2 RODO gwarantuje im ochronę przed bezczynnością organu nadzorczego.

Z uwagi na przyznaną państwom członkowskim autonomię proceduralną[745] i instytucjonalną RODO nie określa konkretnych sądów ani szczegółowych procedur, w tym terminów umożliwiających wykonywanie analizowanego prawa[746]. Oznacza to, że kwestie te mogą być ukształtowane różnie w każdym z państw, w których obwiązuje RODO. Od decyzji organu nadzorczego może więc przysługiwać – zależnie od państwa i wdrożonych procedur – skarga, odwołanie lub inny środek odwoławczy. Może je rozpatrywać sąd powszechny w ramach tzw. procedury hybrydowej, sąd administracyjny lub inny sąd, utworzony specjalnie w celu rozpatrywania tych środków. Jednolicie ukształtowano kwestię właściwości

[743] Motyw 143 preambuły RODO.

[744] Artykuł 78 ust. 2 RODO.

[745] Autonomia proceduralna jest uznawana za „kompetencję państwa członkowskiego do uregulowania właściwości sądów i procedur (sądowych) służących rozpoznawaniu roszczeń opartych na prawie wspólnotowym (ochronie praw wynikających z bezpośrednio skutecznych przepisów prawa wspólnotowego)". (A. Wróbel, *Autonomia proceduralna państw członkowskich. Zasada efektywności i zasada efektywnej ochrony sądowej w prawie Unii Europejskiej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2005, z. 1, s. 35).

[746] RODO rozstrzyga natomiast kolizję powodowaną wszczęciem postępowania przed sądami w więcej niż jednym państwie członkowskim (zob. art. 81 i motyw 144 preambuły RODO).

miejscowej postępowania przeciwko organowi nadzorczemu przyjmując, że wszczyna się je przed sądem państwa członkowskiego, w którym organ ten ma siedzibę[747].

RODO wymaga, aby środki ochrony prawnej przed sądem były „skuteczne". Zapewnienie skutecznych środków odgrywa istotną rolę, sprawia bowiem, że przyznana osobom ochrona prawna jest realna, a nie pozorna.

W języku potocznym „skuteczny" oznacza „dający pozytywne, pożądane wyniki, oczekiwany skutek"[748]. Pojęcie to należy interpretować z uwzględnieniem treści przepisu art. 47 Karty praw podstawowych Unii Europejskiej, określającego prawo do skutecznego środka prawnego przed sądem. Zdaniem M. Górskiego obejmuje ono wiązkę uprawnień wymienionych w tym przepisie, a więc uprawnienie do rozpatrzenia sprawy w rozsądnym terminie, w sposób sprawiedliwy i jawny przez niezawisły i bezstronny sąd ustanowiony na mocy ustawy, a także prawo do uzyskania porady prawnej[749], skorzystania z pomocy obrońcy i przedstawiciela[750].

Przyjęcie tego założenia oznacza, że aby stwierdzić czy środek prawny jest skuteczny, należy zbadać czy są przestrzegane wszelkie reguły i standardy związane z funkcjonowaniem sądownictwa w danym państwie[751], w szczególności określone w prawie międzynarodowym. Można zatem stwierdzić, że skuteczność, o której mowa w przepisie, jest wa-

[747] Artykuł 78 ust. 3 RODO.

[748] S. Skorupka, H. Auderska, Z. Łempicka (red.), *op. cit*., s. 753.

[749] Zdaniem O. Hałub komentowany przepis pozostaje w ścisłym związku z Konwencją o Ochronie Praw Człowieka i Podstawowych Wolności, a wyrażone w nim prawo dostępu do porady prawnej może być wykonywane również na etapie przedsądowym (O. Hałub, *Sformalizowany model dostępu do nieodpłatnej pomocy prawnej na etapie przedsądowym w Polsce*, Wrocław 2018, rozprawa doktorska [niepubl.], s. 50).

[750] Innego zdania jest A. Wróbel, który dostrzega trzy uprawnienia: prawo do skutecznego środka prawnego, prawo dostępu do sądu i prawo do pomocy prawnej (A. Wróbel, *Komentarz do art. 47*, [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, C.H. Beck, Warszawa 2013, s. 1193).

[751] Zob. szerzej nt. reguł i standardów: A. Sulikowski, *Współczesny paradygmat sądownictwa konstytucyjnego wobec kryzysu nowoczesności*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2008, s. 65 i n.

runkowana spełnieniem wymogów ogólnych i szczególnych. Wymogi ogólne odnoszą się do funkcjonowania wymiaru sprawiedliwości w danym państwie członkowskim[752], a wymogi szczególne dotyczą przyjęcia i właściwego stosowania w tym państwie konkretnego środka prawnego, mającego na celu ochronę praw tych osób.

W polskim porządku prawnym jest zagwarantowane powszechne prawo do sądu i co najmniej dwuinstancyjne postępowanie sądowe[753]. Wynika to z przepisów prawa wewnętrznego[754] i międzynarodowego[755].

Skargi na decyzje administracyjne wydane przez Prezesa UODO, skargi na bezczynność lub przewlekłe prowadzenie postępowania przez ten organ i skargi na wydane przez niego określone przepisami prawa postanowienia – w tym, w przedmiocie czasowego ograniczenia przetwarzania danych osobowych – rozpatrują sądy administracyjne[756]. „Skarga do sądu administracyjnego jest rodzajem środka prawnego (środka zaskarżenia) nadzwyczajnego, o charakterze zewnętrznym. Uruchamia bowiem postępowanie kontrolne prowadzone przez organ usytuowany poza systemem organów administracji publicznej – niezawisły sąd administracyjny”[757].

Sądem właściwym miejscowo do rozpatrzenia skargi w pierwszej instancji jest Wojewódzki Sąd Administracyjny w Warszawie, a w drugiej Naczelny Sąd Administracyjny[758]. Rozstrzygają one sprawę wyrokiem. Prowadzone przez nie postępowanie odbywa się na zasadach i w trybie

[752] Szerzej na ich temat zob. np.: wyrok Trybunału Sprawiedliwości z dnia 25 lipca 2018 r., sygn. C-216/18 PPU (http://curia.europa.eu/juris/document/document.jsf?text=&docid=204384&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=958627, [dostęp: 10.08.2018]); wyrok Trybunału Sprawiedliwości z dnia 9 października 2014 r., sygn. C-222/13 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=158428&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=960651, [dostęp 10.08.2018]).

[753] Artykuł 176 ust. 1 i art. 45 Konstytucji RP.

[754] W szczególności Konstytucji RP i ustaw określających ustrój sądów.

[755] Określa je m.in. art. 8 i 10 PDPCz i art. 13 MPPOiP.

[756] Artykuł 3 § 2 p.p.s.a. i art. 7 ust. 4 i art. 70 u.o.d.o.

[757] T. Woś, *Komentarz do art.* 3, [w:] T. Woś (red. nauk.), *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Wolters Kluwer Polska, Warszawa 2016, wyd. VI, s. 57.

[758] Artykuł 13 § 2 i art. 15 § 1 p.p.s.a.

określonym przepisami Prawa o postępowaniu przed sądami administracyjnymi. Dotyczy to w szczególności terminu i warunków wniesienia skargi i skargi kasacyjnej[759], określenia zdolności sądowej i procesowej oraz stron postępowania, ustanawiania pełnomocników[760], zasad prowadzenia postępowania, dowodów w postępowaniu i przysługujących środków odwoławczych. Sądy uwzględniają również kwestie określone w motywie 143 preambuły RODO.

Sądy administracyjne funkcjonują zasadniczo na podstawie modelu kasacyjnego[761]. Oznacza to, że badają czy konkretne działanie organu lub jego brak było zgodne z prawem. Sądy administracyjne są sądami prawa, a nie faktu. Formułują ocenę co do legalności działania (bezczynności) organu, nie zastępując jednak organu administracji publicznej w jego działaniach. Nie orzekają również o wysokości odszkodowania należnego stronie. Rozstrzygnięcie tej kwestii mieści się w zakresie kognicji sądów powszechnych.

Korzystanie ze środków prawnych opisanych w tej części następuje bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej. Nie wyklucza ono także dochodzenia przez osobę, której dane dotyczą – we właściwym trybie – odszkodowania za poniesioną szkodę w związku z naruszeniem jej praw w zakresie ochrony danych[762] ani dochodzenia praw na podstawie odrębnych przepisów prawa[763], a także stosowania – w określonych prawem przypadkach – środków karnych.

[759] Zob. szerzej: B. Adamiak, *Skarga i skarga kasacyjna w postępowaniu sądowoadministracyjnym. Komentarz*, Wolters Kluwer Polska, Warszawa 2017.

[760] Do reprezentacji odnosi się także przepis art. 80 RODO.

[761] Zob. szerzej: B. Banaszak, K. Wygoda, *Funkcjonowanie sądownictwa administracyjnego w Polsce w zderzeniu z problemami współczesności – wybrane zagadnienia*, „Studia Iuridica Lublinensia" 2014, Nr 22, s. 169–170.

[762] Artykuł 78 i 82 RODO.

[763] Motyw 164 preambuły RODO i art. 263 TFUE.

11. Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu

Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu nie było wyrażone wprost w dyrektywie 95/46/WE[764]. Zdaniem W. Kuberskiej określone w RODO prawo nie może być jednak uznane za *novum*. Nie wprowadza ono zasadniczo większych zmian merytorycznych względem dotychczasowego katalogu uprawnień przyznanych osobie, której dane dotyczą, bowiem osoba ta mogła wcześniej dochodzić swoich praw przed sądem powszechnym[765].

Warto zauważyć, że opierała ona swe roszczenie najczęściej na przepisach Konstytucji RP i przepisach prawa cywilnego regulujących ochronę dóbr osobistych, w tym prawa do prywatności. Dowodziła naruszenia dóbr w związku z bezprawnym[766] przetwarzaniem jej danych osobowych. Opisany reżim prawny różni się od reżimu ochrony danych osobowych, który jest oparty na przepisach Konstytucji RP i ustawy o ochronie danych osobowych[767]. Różnice występują przede wszystkim w zakresie wykonywania prawa, stosowanej procedury i organów właściwych do ustalenia naruszenia[768]. Reżimy te są mylone w praktyce ze względu na to, że

[764] Artykuł 23 ust. 1 dyrektywy.

[765] W. Kuberska, *Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowy przetwarzającemu*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017, s. 388

[766] „Pojęcie bezprawności oznacza ujemną ocenę zachowania się opartą na sprzeczności tego zachowania z szeroko pojętym porządkiem prawnym, a więc na sprzeczności z obowiązującymi przepisami ustawy bądź regułami wynikającymi z zasad współżycia społecznego. Bezprawność stanowi kwalifikację przedmiotową czynu, ujmuje zachowanie jako obiektywnie nieprawidłowe, abstrahując przy tym od elementu zawinienia. Przy ustaleniu bezprawności rozważeniu podlega stosunek, w jakim pozostaje dane zachowanie względem obowiązujących reguł postępowania" (wyrok SA w Warszawie z dnia 7 czerwca 2013 r., sygn. I ACa 1584/12, LEX nr 1327625).

[767] Zob. np. wyrok SA w Warszawie z dnia 25 listopada 2016 r., sygn. I ACa 1565/15, LEX nr 22373847.

[768] Zob. np. art. 51 Konstytucji RP i art. 18 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 stara i nieobowiązująca) oraz art. 47 Konstytu-

nieprawidłowe przetwarzanie danych osobowych narusza niejednokrotnie dobra osobiste[769].

Przechodząc do rozważań dotyczących RODO należy zauważyć, że prawo do skutecznego środka ochrony prawnej przed sądem przysługuje każdej osobie, której dane dotyczą, gdy uzna ona, że administrator lub podmiot przetwarzający[770] naruszył przysługujące jej na mocy RODO prawa w wyniku przetwarzania jej danych z naruszeniem RODO[771]. Wykonywanie tego prawa nie jest więc zależne od istnienia obiektywnie weryfikowalnych przesłanek, lecz od subiektywnej oceny osoby, której dane dotyczą. Wystarczające jest bowiem przeświadczenie o naruszeniu prawa.

RODO przyjmuje szeroką interpretację wyrażenia „przetwarzanie naruszające RODO". Jest nim naruszenie przepisów tego aktu, wydanych na jego podstawie przepisów aktów delegowanych i wykonawczych oraz przepisów prawa wewnętrznego państw członkowskich doprecyzowujących RODO[772]. Przyjęte znaczenie jest zgodne z celami RODO. Zwiększa zakres kontroli osób, których dane dotyczą, nad przetwarzaniem ich danych osobowych i ich ochronę prawną.

Ze względu na zasadę autonomii proceduralnej państw członkowskich RODO nie określa konkretnych sądów ani procedur umożliwiających wykonywanie omawianego prawa. Zawiera wyłącznie wytyczne umożliwiające ustalenie właściwego miejscowo sądu rozpatrującego tego rodzaju sprawy. Aby nie tworzyć barier utrudniających lub uniemożliwiających realizację tego prawa przyjmuje ono, że o tym, który sąd jest właściwy miejscowo, decyduje osoba, której dane dotyczą. Następuje to przez wniesienie przysługującego jej środka prawnego do określonego sądu[773].

---

cji RP i art. 23–24 k.c.

[769] Postanowienie SN z dnia 15 lutego 2013 r., sygn. I CSK 684/12.

[770] Podmiotem przetwarzającym jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt 8 RODO).

[771] Artykuł 79 RODO.

[772] Motyw 146 preambuły RODO.

[773] *Ibidem*.

Prawo wyboru przyznane osobie, której dane dotyczą, jest ograniczone. Może ona wybrać sąd w państwie członkowskim, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną lub sąd w państwie członkowskim, w którym osoba ta ma miejsce zwykłego pobytu. Dokonanie wyboru nie jest jednak możliwe, gdy administrator lub podmiot przetwarzający dane są organami publicznymi państwa członkowskiego[774] wykonującymi swe uprawnienia publiczne. Ma to związek z zasadą nieingerencji w sprawy wewnętrzne państw.

Należy zauważyć, że prawodawca wykazuje się niekonsekwencją terminologiczną. W art. 79 ust. 2 RODO stosuje bowiem łącznik „miejsca zwykłego pobytu" osoby, podczas gdy w motywie 145 preambuły RODO posługuje się łącznikiem jej „miejsca zamieszkania"[775]. W prawie prywatnym międzynarodowym łączniki te różnią się od siebie.

Miejsce zamieszkania nie jest rozumiane jednolicie. Odnosi się je najczęściej do miejsca zamieszkania osoby w określonym państwie. Ustalając je, bierze się pod uwagę dwa czynniki, obiektywny i subiektywny. Pierwszy to przebywanie w określonym miejscu, a drugi, to zamiar pobytu. Aby ustalić miejsce zamieszkania określonej osoby, czynniki te muszą wystąpić jednocześnie. Na ustalenie miejsca zamieszkania nie wpływa faktyczna przerwa w przebywaniu osoby w określonej miejscowości[776].

Mniej intensywne powiązanie osoby z miejscem występuje w przypadku ustalenia zwykłego pobytu osoby. Jest nim miejsce, w którym osoba ta zazwyczaj przebywa i ma główny ośrodek swoich interesów życiowych. M. Pazdan dostrzega, że w stosunkach międzynarodowych zastępuje się

[774] Ma to związek z zasadą nieingerencji w sprawy wewnętrzne państw.

[775] W ten sam sposób zostało to ujęte w wersji angielskojęzycznej (art. 79 – *where the data subject has his or her habitual residence*; motyw 145 – *where the data subject resides*) i niemieckojęzycznej (art. 79 – *in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat*; motyw 145 – *in dem die betroffene Person wohnt*).

[776] M. Świerczyński, *Łączniki w normach kolizyjnych*, [w:] M. Pazdan (red.), *System prawa prywatnego. Prawo prywatne międzynarodowe*, C.H. Beck, Instytut Nauk Prawnych PAN, Warszawa 2014, t. 20A, s. 226–232.

stopniowo łącznik miejsca zamieszkania łącznikiem miejsca zwykłego pobytu. Odnosi się to w szczególności do osób, których charakter zatrudnienia utrudnia ustalenie miejsca zamieszkania[777]. Mając to na uwadze można stwierdzić, że bardziej korzystne dla osoby, której dane dotyczą, byłoby umożliwienie jej dokonania wyboru między sądem w państwie, w którym ma ona miejsce zwykłego pobytu, a sądem w państwie, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną[778]. Założenie to jest zgodne z treścią przepisu art. 79 RODO.

Państwa członkowskie określają samodzielnie sądy krajowe właściwe do rozpatrywania tego rodzaju spraw na ich terenie. W Rzeczypospolitej Polskiej są nimi właściwe sądy okręgowe[779]. Rozpatrują one również sprawy odszkodowawcze, o których mowa w art. 82 RODO. Do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych stosują one przepisy ustawy o ochronie danych osobowych i RODO, a w zakresie nieuregulowanym także przepisy Kodeksu cywilnego.

Postępowanie przed sądem okręgowym zostaje wszczęte z inicjatywy osoby, której dane dotyczą. Pierwszym pismem procesowym w sprawie jest – wnoszony przez tę osobę – pozew, spełniający określone prawem wymogi[780]. Postępowanie toczy się z uwzględnieniem zasad postępowania cywilnego[781]. Jest ono prowadzone na podstawie przepisów Kodeksu postępowania cywilnego, z zastrzeżeniem odmienności przewidzianych w ustawie o ochronie danych osobowych[782]. Kodeks określa w szczegól-

[777] *Ibidem*, s. 232–236.

[778] RODO rozstrzyga ewentualne kolizje powodowane wszczęciem postępowania przed sądami w więcej niż jednym państwie członkowskim (zob. art. 81 i motyw 144 preambuły RODO).

[779] Artykuł 93 u.o.d.o. Ustalenie właściwości następuje na podstawie przepisów art. 15–46 k.p.c.

[780] Są to wymogi odnoszące się do pozwu (art. 187 k.p.c.) i ogólne warunki pism procesowych (art. 126 k.p.c.).

[781] Zob. szerzej nt. zasad postępowania cywilnego: A. Zieliński, *Postępowanie cywilne. Kompendium*, C.H. Beck, Warszawa 2017, s. 20–32.

[782] Są nimi: wymiana informacji między sądem i Prezesem UODO oraz uprawnienia Prezesa UODO w zakresie wytaczania powództw, wstępowania do toczących się postępowań i wyrażania istotnych dla sprawy poglądów, sposób rozstrzygania kolizji w przypadku rozpatrywania

ności: terminy na dokonanie czynności procesowych, sposoby określenia zdolności sądowej i procesowej, strony postępowania, ustanawianie pełnomocników[783], dowody w postępowaniu i środki odwoławcze przysługujące od zapadłych w sprawie rozstrzygnięć. Rozstrzygając sprawę, sąd wydaje wyrok, od którego przysługuje apelacja do sądu drugiej instancji (sądu apelacyjnego)[784].

RODO stanowi, że opisane w nim środki prawne nie są konkurencyjne. Od woli osoby, której dane dotyczą, jest uzależnione zastosowanie określonego trybu dochodzenia roszczeń związanych z naruszeniem jej praw (administracyjny lub sądowy). Może ona zatem dokonać świadomego wyboru zastosowania konkretnej procedury, biorąc pod uwagę całokształt okoliczności sprawy, swoje zasoby i możliwości oraz wady i zalety konkretnego postępowania. Jest to niewątpliwą zaletą wprowadzenia omawianego rozwiązania. Niesie ono jednak za sobą ryzyko wystąpienia niejednolitości rozstrzygnięć.

Zaletą postępowania przed Prezesem UODO jest jego szybkość. Jest to postępowanie jednoinstancyjne, w którym terminy na dokonanie poszczególnych czynności określają przepisy prawa. W postępowaniu tym organ przestrzega zasady informowania stron. W sposób należyty i wyczerpujący informuje osobę, której dane dotyczą, o okolicznościach faktycznych i prawnych, które mogą mieć wpływ na ustalenie jej praw i obowiązków będących przedmiotem toczącego się postępowania. Prezes UODO czuwa nad tym, aby osoba, której dane dotyczą, nie poniosła szkody z powodu nieznajomości prawa i w tym celu udziela jej niezbędnych wyjaśnień i wskazówek[785]. Stoi on na straży praworządności i podejmuje wszelkie czynności niezbędne do wyjaśnienia stanu faktycznego sprawy i jej załatwienia. Reali-

tej samej sprawy przez więcej niż jeden organ (sąd) oraz zakres związania sądu decyzją Prezesa UODO (rozdział 10 u.o.d.o.).

[783] Do reprezentacji odnosi się także przepis art. 80 RODO.

[784] Artykuł 267 § 1 i 2 k.p.c.

[785] Artykuł 9 k.p.a.

zuje zatem zasadę prawdy obiektywnej[786]. Istotną kompetencją – z perspektywy osoby, której dane dotyczą – jest fakultatywne prowadzenie postępowania kontrolnego, umożliwiającego pozyskanie dodatkowych dowodów w sprawie[787]. Zaletą postępowania jest także nieodpłatność[788] i możliwość nałożenia administracyjnej kary pieniężnej na administratora lub podmiot przetwarzający dane. Wadą postępowania jest konieczność wszczęcia odrębnego postępowania przed sądem powszechnym, w przypadku ubiegania się o przyznanie odszkodowania za naruszenie. Wadą dla niektórych osób może być również znaczna odległość siedziby organu od ich miejsca zamieszkania. Wydaje się jednak, że ze względu na dopuszczalne zróżnicowane formy kontaktu z organem (także w formie pisemnej, w tym elektronicznej), nie powinno to powodować znacznych trudności.

Zaletą postępowania przed sądem powszechnym jest jego dostępność. Siedziba sądu znajduje się najczęściej bliżej miejsca zamieszkania osoby, której dane dotyczą, niż siedziba Prezesa UODO. Sądy są niezależne, a sędziowie rozpatrujący sprawę są niezawiśli[789]. Cech tych nie posiada organ administracji publicznej. Zaletą postępowania przed sądem powszechnym jest również dopuszczalność dochodzenia w ramach tego postępowania odszkodowania za poniesione szkody. Za wadę należy uznać koszty postępowania[790] i występującą niekiedy przewlekłość postępowania[791]. Może nią także być znaczne sformalizowanie postępowania i przyjęta w nim zasada kontradyktoryjności, polegająca na tym, że strony powinny „przygotować,

[786] Artykuł 7 k.p.a..

[787] Artykuł 68 u.o.d.o.

[788] Wyjątkiem jest uiszczenie opłaty skarbowej.

[789] Artykuł 45 ust. 1 i art. 178 ust. 1 Konstytucji RP.

[790] Zob. art. 16 ust. 1 pkt 3 ustawy z dnia 28 lipca 2005 r. o kosztach postępowania w sprawach cywilnych (t.j. Dz. U. z 2018 r., poz. 300 ze zm.). Należy jednak zauważyć, że w określonych prawem przypadkach można ubiegać się o zwolnienie z nich.

[791] Zob. np. wyrok ETPCz w Strasburgu z dnia 5 lipca 2015 r. w sprawie *Rutkowski i inni przeciwko Polsce (skargi nr 72287/10, 13927/11 i 46187/11)* oraz 591 innych skarg (http://trybunal.gov.pl/uploads/media/ Sprawa_Rutkowski_i_inni_przeciwko_Polsce__skargi_nr_72287_10__13927_11_i_46187_11_oraz_591_innych_skarg___wyrok_z_7_lipca_2015_r._.pdf, [dostęp 17.07.2018]).

gromadzić i dostarczyć materiał procesowy […], a sąd jedynie ocenić ten materiał i wydać rozstrzygnięcie”[792]. Będzie to szczególnie dotkliwe w przypadku osób nieporadnych, które nie potrafią prawidłowo sformułować pisma procesowego. W tym przypadku sąd może jednak zarządzić stawiennictwo tej osoby w sądzie, aby wyjaśniła sprawę[793]. Może jej także przyznać pomoc z urzędu[794], jeśli spełnia ona określone prawem wymogi.

Jeśli strona zainicjuje równolegle wszczęcie postępowania sądowego i administracyjnego, to pierwszeństwo przysługuje postępowaniu administracyjnemu[795]. Jeśli sprawa została już prawomocnie rozstrzygnięta przez sąd lub organ – ze względu na powagę rzeczy osądzonej (*res iudicata*) – nie będzie ona już ponownie rozpatrywana przez sąd ani przez organ.

12. Prawo do odszkodowania

Prawo do odszkodowania określał przepis art. 23 dyrektywy 95/46/WE. Zobowiązywał on państwa członkowskie do zapewnienia każdej osobie, która poniosła szkodę wskutek niezgodnej z prawem operacji przetwarzania danych lub innej czynności niezgodnej z przepisami krajowymi przyjętymi na podstawie dyrektywy, prawo do odszkodowania od administratora danych za tę szkodę. Polski ustawodawca nie dokonał implementacji przepisów dyrektywy poprzez wprowadzenie do polskiego porządku prawnego przepisów szczególnych, regulujących wprost kwestię odpowiedzialności odszkodowawczej administratora za niezgodne z prawem przetwarzanie. Za wystarczające uznał natomiast ogólne reguły odpowiedzialności określone w Kodeksie cywilnym[796].

[792] J. Studzińska, *Zasady i przesłanki postępowania cywilnego*, [w:] J. Studzińska, P. Cioch, *Postępowanie cywilne*, C.H. Beck, Warszawa 2017, wyd. 5, s. 69.

[793] Artykuł 216 k.p.c.

[794] Artykuł 117 i n. k.p.c.

[795] Zob. art. 94–94 u.o.d.o.

[796] A. Błaszczyńska, *Prawo do odszkodowania i odpowiedzialność*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017, s. 404.

Przepis art. 82 RODO reguluje prawo do odszkodowania odmiennie od dyrektywy 95/46/WE. Zawarta w nim norma prawna jest sformułowana w sposób jasny, precyzyjny i zupełny. Ze względu na bezpośrednie obowiązywanie RODO jest ona samodzielną podstawą roszczeń odszkodowawczych. Osoba, której dane dotyczą, może zatem oprzeć dochodzone przed sądem roszczenie bezpośrednio na tym przepisie i nie musi odwoływać się do przepisów wykonawczych prawa krajowego. Warto zauważyć, że omawiana regulacja nie wyklucza dochodzenia przed sądem roszczeń na podstawie innych przepisów. Nie należy ich jednak łączyć z art. 82 RODO, różne są bowiem przesłanki ich realizacji[797].

Określone w RODO prawo do odszkodowania przysługuje każdej osobie, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów RODO i wydanych na jego podstawie przepisów aktów delegowanych i wykonawczych oraz przepisów prawa wewnętrznego państw członkowskich doprecyzowujących RODO[798].

Zastosowane w RODO pojęcie „szkody" należy interpretować szeroko. Powinno ono w pełni odzwierciedlać cele RODO[799] i uwzględniać orzecznictwo Trybunału Sprawiedliwości[800]. Jego interpretacja może więc ulegać zmianom wskutek działalności orzeczniczej Trybunału przez przyjęcie odmiennej interpretacji stosowanych pojęć i uwzględnienie dodatkowych czynników lub rezygnację z dotychczas aprobowanych.

Z obszernego orzecznictwa odnoszącego się do szkody można wyodrębnić istotne kwestie z nią związane. Po pierwsze, zdarzenie powodujące szkodę powinno być bezprawne, a naruszona przez nie norma prawna

[797] *Ibidem*, s. 406.

[798] Artykuł 82 ust. 1 i motyw 146 preambuły RODO.

[799] Motyw 146 preambuły RODO. Ustalenie celów regulacji powinno nastąpić przede wszystkim w nawiązaniu do treści motywów 1–15 preambuły RODO i odpowiednich motywów nieobowiązującej już dyrektywy 95/46/WE (zob. motyw 9 preambuły RODO).

[800] Zob. szerzej nt. szkody w świetle orzecznictwa: M. Taborowski, *Konsekwencje naruszenia prawa Unii Europejskiej przez sądy krajowe*, Wolters Kluwer Polska, Warszawa 2012, s. 153–156.

powinna być źródłem uprawnień dla jednostek. Po drugie, między zdarzeniem powodującym szkodę a szkodą powinien istnieć związek przyczynowy. Po trzecie, szkoda powinna być rzeczywista i pewna, a nie hipotetyczna i potencjalna. Za poniesioną szkodę powinno zostać przyznane odszkodowanie, które jest do niej współmierne. Może ono również objąć utracone korzyści i należne odsetki[801]. „Przekładając powyższe na grunt polskich przepisów, będzie chodziło zarówno o postępowania o odszkodowania za wyrządzoną szkodę majątkową – na mieniu, w postaci rzeczywistej straty (*damnum emergens*) lub utraconych korzyści (*lucrum cessans*), jak i o zadośćuczynienie za krzywdę (szkodę niemajątkową) – związaną z naruszeniem dóbr niemajątkowych”[802].

Za szkody spowodowane przetwarzaniem naruszającym przepisy RODO jest odpowiedzialny każdy administrator uczestniczący w przetwarzaniu. Odpowiedzialność podmiotu przetwarzającego jest ograniczona i aktualizuje się wyłącznie w trzech przypadkach. Pierwszym jest niedopełnienie przez niego określonych w RODO obowiązków nałożo-

[801] Zob. np.: wyrok Trybunału z dnia 27 stycznia 1982 r., sygn. 51/81 (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:61981CJ0051, [dostęp 01.01.2018]); wyrok Sądu z dnia 2 sierpnia 1993 r., sygn. C-271/91 (http://curia.europa.eu/juris/showPdf.jsf?text= &docid=98212&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=518551, [dostęp 01.01.2018]); wyrok Trybunału w sprawach połączonych z dnia 5 marca 1996 r., sygn. C-46/93 i C-48/93 (https://curia.europa.eu/arrets/TRA-DOC-PL-ARRET-C-0046-1993-200406772-05_00.html); wyrok Trybunału w sprawach połączonych z dnia 8 marca 2001 r., sygn. C-397/98 i C-410/98 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=45879&pageIndex=0 &doclang=pl&mode=lst&dir=&occ=first&part=1&cid=508843, [dostęp 01.01.2018]); wyrok Trybunału z dnia 9 listopada 2006 r., sygn. C-243/05 P (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:62005CJ0243, [dostęp 01.01.2018]); wyrok Trybunału w sprawach połączonych z dnia 13 lipca 2006, sygn. C-295/04 do C-298/04 (http://curia.europa.eu/juris/document/document.jsf?text=&docid=56474&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=508913, [dostęp 01.01.2018]); wyrok Sądu z dnia 20 lipca 2016 r., sygn. T-483/13 (http://curia.europa.eu/juris/document/document.jsf?text=szkoda+ochrona+danych+osobowych&docid=181874 &pageIndex=0&doclang=pl&mode=req&dir=&occ=first&part=1&cid=266927#ctx1, [dostęp 01.01.2018]).

[802] P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 82*, [w:] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, C.H. Beck, Warszawa 2018, s. 822–823.

nych bezpośrednio na podmioty przetwarzające[803]. Drugim jest podejmowanie działań wykraczających poza zgodne z prawem instrukcje administratora. Są to działania podejmowane „dodatkowo", które nie zostały określone w umowie łączącej administratora z podmiotem przetwarzającym, udzielonych podmiotowi przetwarzającemu wytycznych, wydanych poleceniach ani w żaden inny sposób. Trzecim jest podejmowanie działań wbrew instrukcjom administratora[804].

Administrator i podmiot przetwarzający mogą uwolnić się od odpowiedzialności za szkody spowodowane przetwarzaniem, gdy „udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody"[805]. RODO wprowadza ciekawe rozwiązanie, różniące się od przyjętego w wielu aktach prawnych prawa międzynarodowego i wewnętrznego. Przyjmuje bowiem domniemanie winy administratora i podmiotu przetwarzającego[806], formułując je w bardzo rygorystyczny sposób. Obalenie domniemania następuje dopiero, gdy zostanie wykazane, że podmioty te „w żaden sposób nie ponoszą winy". Oznacza to, że będą one odpowiedzialne, gdy nie uda im się obalić domniemania nawet w niewielkiej części.

Analizując odpowiedzialność należy również uwzględnić spoczywający na administratorze i podmiocie przetwarzającym obowiązek ustanowienia i wdrożenia odpowiednich procedur oraz środków technicznych i organizacyjnych związanych z przetwarzaniem danych[807]. Biorąc go pod uwagę można stwierdzić, że podmioty te będą obowiązane do udowodnienia dwóch kwestii. Pierwszą jest podejmowanie działań zgodnie z przyjęty-

[803] Zob. wykaz obowiązków podmiotów przetwarzających: Information Commisioner's Office, *ICO GDPR guidance: Contracts and liabilities between controllers and processors*, wersja el., s. 27, https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf [dostęp 02.08.2018].

[804] Artykuł 82 ust. 2 RODO.

[805] Artykuł 82 ust. 3 RODO.

[806] Warto zauważyć, że dyrektywa 95/46/WE nie przewidywała odpowiedzialności podmiotu przetwarzającego za szkody wyrządzone niezgodnym z prawem przetwarzaniem danych.

[807] Artykuł 25 RODO.

mi procedurami. Drugą jest ustanowienie i wdrożenie procedur oraz środków adekwatnych do zagrożeń występujących w związku z przetwarzaniem i w sposób zapewniający ochronę praw osób, których dane dotyczą.

Jeśli udowodniono winę administratora i/lub podmiotu przetwarzającego, to osoba, która poniosła szkodę, ma prawo uzyskać odszkodowanie od podmiotu, który dokonał naruszeń[808]. Jeżeli dane przetwarzał więcej niż jeden podmiot[809] i stwierdzono ich odpowiedzialność, to odpowiadają oni za całą szkodę solidarnie. Oznacza to, że osoba, która poniosła szkodę, może żądać zapłaty odszkodowania od każdego z nich, od kilku z nich lub od wszystkich wspólnie. Zapłacenie całości odszkodowania przez któregokolwiek z nich zwalnia z obowiązku zapłaty pozostałych. Kwestią wewnętrzną – między podmiotami, których odpowiedzialność udowodniono – jest rozliczenie. Podmiot, który zapłacił całość odszkodowania, może żądać od pozostałych obowiązanych zwrotu kwoty odpowiadającej części odszkodowania, do uiszczenia której byli zobowiązani. Dotyczy to również podmiotu, który zapłacił większą część kwoty niż tę, do której uiszczenia był zobowiązany.

Ustanowienie odpowiedzialności solidarnej służy rzeczywistemu uzyskaniu odszkodowania. Chroni wierzyciela w przypadku niewypłacalności jednego lub kilku dłużników. Umożliwia ponadto uzyskanie całości (pełnego i skutecznego) odszkodowania od jednego z nich, bez konieczności podejmowania działań względem pozostałych[810].

Osoba, która poniosła szkodę, może dochodzić ustalenia odszkodowania przed sądem właściwym w państwie członkowskim, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną lub przed sądem państwa, w którym osoba ta ma miejsce zwykłego pobytu. Jeśli szkoda została wyrządzona przez organ publiczny państwa

[808] W odrębnym postępowaniu może na nich zostać ponadto nałożona administracyjna kara pieniężna za niezgodne z prawem przetwarzanie.

[809] Administrator i podmiot przetwarzający w dowolnej ilości i kombinacji.

[810] Motyw 146 preambuły i art. 82 ust. 1 i 4–5 RODO.

członkowskiego, który wykonuje swoje uprawnienia publiczne, odszkodowanie może być dochodzone przed właściwym sądem tego państwa członkowskiego[811]. W Rzeczypospolitej Polskiej sprawy związane z przyznaniem odszkodowania rozpatrują właściwe sądy okręgowe[812]. Prowadzą one postępowanie na podstawie przepisów i z uwzględnieniem zasad opisanych w części poświęconej analizie prawa do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu.

Określona w przepisie art. 82 RODO odpowiedzialność odszkodowawcza wykazuje podobieństwo do regulacji odpowiedzialności z tytułu czynów niedozwolonych, określonej w przepisie art. 415 k.c.[813] Dotyczy to w szczególności przesłanek odpowiedzialności. Podkreśla się jednak słusznie, że mimo podobieństw regulacja ta tworzy „swoisty reżim bezumownej odpowiedzialności odszkodowawczej"[814].

[811] Artykuł 82 ust. 6 w zw. z art. 79 ust. 2 RODO.

[812] Artykuł 93 u.o.d.o.

[813] Zob. szerzej nt. tej odpowiedzialności: W. Dubis, *Komentarz do art. 415*, [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks Cywilny. Komentarz*, C.H. Beck, Warszawa 2014, s. 769–777; J. Gudowski, *Komentarz do art. 415*, [w:] J. Gudowski (red. nauk.), *Kodeks Cywilny. Komentarz. Tom III. Zobowiązania. Część ogólna*, Wolters Kluwer, Warszawa 2018, wyd. 2, s. 588–627.

[814] N. Zawadzka, *Komentarz do art. 82*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 1049.

Zakończenie

We współczesnym świecie obserwujemy intensywny rozwój wysokich technologii. Powszechnie stosuje się nowe narzędzia informacyjne i komunikacyjne, umożliwiające porozumiewanie się na odległość. Wzrosło znaczenie wiedzy i informacji. Wiedza jest wykorzystywana do wprowadzania innowacji w różnych sektorach, a informacje są traktowane jak towar. Przetwarza się je na ogromną skalę. Następuje to także w sposób zautomatyzowany, co umożliwia zwiększenie szybkości przetwarzania danych i szybkie wyprowadzenie miarodajnych wniosków.

Informacje wykazują znaczne zróżnicowanie, podlegają licznym podziałom. Jeśli dotyczą zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych, określa się je jako „dane osobowe". Przetwarzają je podmioty publiczne i prywatne, a przetwarzanie to niejednokrotnie nie ogranicza się do terytorium jednego państwa. Powoduje ono ryzyko, może bowiem skutkować naruszeniem praw osobistych osób fizycznych oraz może powodować występowanie zjawisk szkodliwych społecznie. Zapewnienie skutecznej ochrony tych danych leży zarówno w interesie publicznym, jak i prywatnym.

Prawo do ochrony danych osobowych jest jednym z praw człowieka. Jego źródeł – podobnie jak wszystkich innych praw – należy upatrywać przede wszystkim w godności osoby ludzkiej, która jest przyrodzona i niezbywalna. Prawo do ochrony danych osobowych jest uznawane za prawo autonomiczne lub jest uznawane za element (wymiar) prawa do prywatności.

Jest ono zagwarantowane w wielu aktach normatywnych prawa krajowego i międzynarodowego, należących do różnych systemów ochrony praw człowieka. Są to regulacje odnoszące się wyłącznie lub w znacz-

nej części do ochrony danych osobowych (akty o charakterze szczegółowym) lub nawiązujące do niej wyłącznie w określonej części (akty o charakterze ogólnym).

Jednym z aktów dotyczących ochrony danych osobowych jest RODO. Akt ten został uchwalony w ramach europejskiej reformy ochrony danych osobowych. Obowiązuje we wszystkich państwach członkowskich Unii Europejskiej i jest bezpośrednio skuteczny, nie wymaga więc implementacji do krajowych porządków prawnych. Ujednolica zasady przetwarzania danych osobowych i określa wymogi związane z tym przetwarzaniem. Określa ponadto konkretne prawa przysługujące osobom, których dane w związku z przetwarzaniem danych ich dotyczących.

RODO nie ogranicza swobody przepływu danych w Unii Europejskiej, którą prawodawca unijny uznaje za szczególną wartość. W preambule RODO stwierdza on bowiem, że przetwarzanie danych powinno służyć ludzkości i przyczyniać się do zapewnienia ludziom pomyślności. Aby zapewnić realizację założonych celów, RODO dąży do umiejętnego wyważania interesów podmiotów procesu przetwarzania, czyli administratora i osoby, której dane dotyczą. W interesie administratora jest jak najszersze przetwarzanie danych osobowych. W interesie osoby, której dane dotyczą, jest natomiast sprawowanie jak największego zakresu kontroli nad jej danymi osobowymi.

Przepisy RODO stanowią w znacznej mierze powtórzenie przepisów dyrektywy 95/46/WE, regulującej przed wejściem w życie RODO ochronę praw osób, których dane dotyczą, w związku z przetwarzaniem ich danych. Rozporządzenie zwiększa jednak kontrolę tych osób nad ich danymi osobowymi. Poszerza zakres niektórych praw oraz przyznaje podmiotom danych nowe prawa. Obserwacja dotychczasowej praktyki umożliwiła wyciągnięcie wniosków i doprecyzowanie niektórych postanowień.

W celu uporządkowania rozważań czynionych w pracy, dotyczących praw osób, których dane dotyczą, posłużono się pojęciem „środków prawnych ochrony danych". Uznano, że są nimi działania prawnie uwa-

runkowane skierowane na zapewnienie przestrzegania przepisów prawa w toku procesu przetwarzania danych osobowych. Przyjęcie proponowanego znaczenia umożliwiło odniesienie tego pojęcia zarówno do osób, których dane dotyczą, jak i do innych podmiotów procesu przetwarzania danych osobowych.

Tak pojmowane środki prawne ochrony danych podzielono na środki prawne *sensu stricto* i środki prawne *sensu largo.* Pierwsze obejmują działania zmierzające do ochrony prywatności konkretnej osoby oraz indywidualnie określonych danych jej dotyczących. Drugie obejmują środki *sensu stricto* oraz środki zmierzające pośrednio do ochrony tej osoby, chroniące dane osobowe w sposób generalny i abstrakcyjny.

Podział na bezpośrednie i pośrednie środki ochrony danych może być także przeprowadzony z uwzględnieniem kryterium podmiotowego. Środki bezpośrednie są podejmowane jedynie przez osobę, której dane dotyczą. Środki pośrednie są natomiast podejmowane przez inne podmioty procesu przetwarzania.

Proponowany podział na bezpośrednie i pośrednie środki ochrony danych osobowych ma charakter porządkujący, umożliwia usystematyzowanie prowadzonych wywodów. Prowadzi do wyróżnienia następujących środków prawnych:

1) pośrednich – a więc działań podejmowanych przez administratora danych lub podmiot przetwarzający, do których podjęcia zobowiązuje ich prawo lub których zastosowanie umożliwia im prawo. Są nimi: środki techniczne i organizacyjne, środki informacyjne, dokonywanie oceny skutków przetwarzania danych osobowych i konsultowanie ich z organem nadzorczym, rejestrowanie czynności przetwarzania, certyfikacja, wprowadzanie i stosowanie wiążących reguł korporacyjnych oraz przyjmowanie i stosowanie kodeksów postępowania. Korzystanie z tych środków nie wymaga aktywnej postawy osoby, której dane dotyczą;

2) bezpośrednich – a więc działań podejmowanych przez osobę, której dane dotyczą. Są nimi: prawo do wyrażenia i wycofania zgody na przetwarzanie danych osobowych, prawo dostępu do danych osobowych, prawo do sprostowania danych osobowych, prawo do usunięcia danych osobowych, prawo do ograniczenia przetwarzania danych osobowych, prawo do przenoszenia danych osobowych, prawo do sprzeciwu wobec przetwarzania danych osobowych, prawo do wniesienia skargi do organu nadzorczego, prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu, prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu i prawo do odszkodowania. Korzystanie z tych środków jest warunkowane aktywną postawą (działaniem) osoby, której dane dotyczą.

Zastosowanie proponowanego podziału umożliwiło przeanalizowanie ochrony danych osobowych w procesie przetwarzania danych z dwóch perspektyw. W środkach bezpośrednich była to perspektywa osoby, której dane dotyczą, która to podejmuje działania dla ochrony własnego interesu. W środkach pośrednich była to perspektywa innych podmiotów procesu przetwarzania (administratora i podmiotu przetwarzającego), podejmujących działania w celu realizacji nałożonych przepisami prawa obowiązków.

Dokonany w pracy przegląd i analiza szczegółowych regulacji prawnych dotyczących bezpośrednich i pośrednich środków prawnych ochrony danych osobowych umożliwił dostrzeżenie niespójności regulacji prawnych z tego obszaru oraz wskazanie zagrożeń, które mogą wystąpić w praktyce stosowania prawa. W pracy zaproponowano ponadto konkretne sposoby rozstrzygnięcia spornych kwestii.

Bibliografia

Wykaz cytowanej literatury

Adamiak B., *Komentarz do art. 6–16*, [w:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, C. H. Beck, wyd. 15, Warszawa 2017

Adamiak B., *Skarga i skarga kasacyjna w postępowaniu sądowoadministracyjnym. Komentarz*, Wolters Kluwer Polska, Warszawa 2017

Ausloos J., *The Interaction between the Rights to Object and to Erasure in the GDPR*, wersja el., https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure/ [dostęp 20.07.2018].

Bałaban A., Dubel L., Leszczyński L., *Zasady tworzenia prawa*, UMCS, Lublin 1986

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* C.H. Beck, Warszawa 2012

Banaszak B., *Prawo konstytucyjne*, C.H. Beck, Warszawa 2008, wyd. 4 zm.

Banaszak B., Wygoda K., *Funkcjonowanie sądownictwa administracyjnego w Polsce w zderzeniu z problemami współczesności – wybrane zagadnienia*, „Studia Iuridica Lublinensia" 2014, Nr 22

Banyś T.A.J., *Funkcje prawa ochrony danych osobowych*, [w:] T.A.J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *Prawo ochrony danych osobowych*, Difin, Warszawa 2016

Baran B., Południak-Gierz K., *Perspektywa regulacji prawa do bycia „zapomnianym" w Internecie. Zarys problematyki*, „Zeszyty Naukowe Towarzystwa Doktorantów UJ. Nauki Społeczne" 2017, Nr 17

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych*, Wolters Kluwer SA, Warszawa 2015, wyd. 6

Barta J., Markiewicz R., *Komentarz do art. 7*, [w:] J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Zakamycze, Kraków 2001

Beskosty M., *Zarządzanie bezpieczeństwem informacji*, Studia nad Bezpieczeństwem 2017, Nr 2

Bielak-Jomaa E., *Źródła prawa ochrony danych osobowych*, [w:] T.A.J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *Prawo ochrony danych osobowych*, Difin, Warszawa 2016

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

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

Błaszczyńska A., *Prawo do odszkodowania i odpowiedzialność*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017.

Błażewski M., *Płaszczyzny administracji elektronicznej*, Acta Universitatis Wratislaviensis, Prawo 2017, Nr 323

Błażewski M., *Wartości w e-administracji i ich wyważenie*, [w:] J. Zimmermann (red.), *Aksjologia prawa administracyjnego. Tom I*, Wolters Kluwer, Warszawa 2017

Błażewski M., *Zasada zapewnienia bezpieczeństwa w e-administracji*, Folia Iuridica Universitatis Wratislaviensis 2017, vol. 6 (1)

Braxton Craven Jr. J., *Personhood: the right to be let alone*, „Duke Law Journal" 1976

Broniatowski K., *Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni – regulacje w prawie polskim i unijnym*, Kancelaria Senatu. Biuro Spraw Senatorskich, Warszawa 2017

Cannataci J.A., *The end of the purpose-specification principle in data protection?*, „International Review of Law, Computers & Technology" 2010, Vol. 24, Nr 1

Castells M., *Społeczeństwo sieci,* Wydawnictwo Naukowe PWN, Warszawa 2008

Chmura J., *Wartość informacji i jej bezpieczeństwo w gospodarce opartej na wiedzy*, „Journal of Modern Science", 2016, Nr 3

Czarnowski A.P., Gawroński M., *Bezpieczeństwo danych w świetle RODO – analiza ryzyka i adekwatności środków*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018

Czarny-Drożdżejko E., *Ochrona danych osobowych w Internecie w świetle orzecznictwa Trybunału Sprawiedliwości*, „Przegląd Sądowy" 2015, Nr 11–12

Czelny M., *Ochrona danych osobowych w działalności Kościoła Katolickiego w Polsce*, „Studia z Prawa Wyznaniowego" 2011, T. 14

Czerwińska B., *Ochrona danych osobowych a prawo dostępu do dziennika elektronicznego – aspekt formalnoprawny*, „Ogrody Nauk i Sztuk" 2017, Nr 7

Dąbek D., *Prawo miejscowe*, Wolters Kluwer SA, Warszawa 2015, wyd. 2

Detrick S., *A Commentary on the United Nations Convention on the Rights of the Child*, Martinus Nijhoff Publishers, Hague Boston London 1999

Dominiak M., Gawroński M., *Zasady przetwarzania danych osobowych*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018

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

Drachal J., Jagielski J., Cherka M., *Komentarz do art. 13*, [w:] R. Hauser, M. Wierzbowski (red.), *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, C.H. Beck, Warszawa 2018

Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy,* LexisNexis, Warszawa 2007, wyd. 3

Duniewska Z., *Pojęcie prawa, określenie i charakterystyka systemu*, [w:] M. Stahl (red. nauk.), *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie*, Warszawa 2016

Duniewska Z., *Pojęcie prawa, określenie i charakterystyka systemu oraz źródeł prawa administracyjnego*, [w:] M. Stahl (red. nauk.), *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie*, Wolters Kluwer Polska SA, Warszawa 2013, wyd. 5

Duniewska Z., *Zakres, przedmiot, rola, cele funkcje, czynniki wyznaczające i cechy prawa administracyjnego*, [w:] R. Hauser, Z. Niewiadomski, A. Wróbel (red. nacz.), *System prawa administracyjnego. Instytucje prawa administracyjnego*, C.H. Beck, Instytut Nauk Prawnych PAN, Warszawa 2010, t. 1

Ehlers D., Fehling M., Pünder H. (red.), *Besonderes Verwaltungsrecht*, C. F. Müller, Heidelberg München Landsberg 2013, wyd. 3, t. 3

Fajgielski P., *Zgoda na przetwarzanie danych osobowych*, [w:] G. Sibiga, X. Konarski (red.), *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Wolters Kluwer Polska, Warszawa 2007

Firlus J. G., *Fakultatywny charakter wniosku o ponowne rozpatrzenie sprawy w świetle zmodyfikowanego kształtu zasady dwuinstancyjności postępowania administracyjnego*, Zeszyty Naukowe Towarzystwa Doktorantów UJ Nauki Społeczne 2017, Nr 17

Fischer B., *Prawo do usunięcia danych*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017

Garlicki L. (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* Wydawnictwo Sejmowe, Warszawa 2001, t. 2, wyd. 1

Garlicki L., *Konstytucyjne źródła prawa administracyjnego*, [w:] R. Hauser, Z. Niewiadomski, A. Wróbel (red.), *System prawa administracyjnego. Konstytucyjne podstawy funkcjonowania administracji publicznej*, C.H. Beck, Instytut Nauk Prawnych PAN, Warszawa 2012, t. 2

Gawroński M. (red.), *RODO. Przewodnik ze wzorami*, Wolters Kluwer Polska, Warszawa 2018

Gawroński M., Kloc K., Wojtas M., *Administrator i podmiot przetwarzający*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018

Gniewek E., Machnikowski P. (red.), *Kodeks Cywilny. Komentarz*, C.H. Beck, Warszawa 2014

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999

Golka M., *Czym jest społeczeństwo informacyjne*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2005, z. 4

Gołaczyński J., *Umowy elektroniczne w prawie prywatnym międzynarodowym*, Wolters Kluwer Polska, Warszawa 2007

Goździaszek Ł., *Prawo do bycia zapomnianym w wyszukiwarce internetowej – glosa do wyroku Trybunału Sprawiedliwości z 13.05.2014 r. w sprawie C-131/12 Google Spain SL i Google Inc. Przeciwko Agencia de Protección de Datos (AEPD) i Mario Costeja González*, „Europejski Przegląd Sądowy" 2015, Nr 2

Górski M., *Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu*, [w:] *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017

Górski M., *Prawo do skutecznego środka prawnego w art. 47 Karty Prawo Podstawowych UE – znaczenie i deficyty*, „Europejski Przegląd Sądowy" 2016, Nr 8

Grzegory T., *Pamięć absolutna czy kontrolowana amnezja – wybrane problemy prawne regulacji „prawa do bycia zapomnianym" w ogólnym rozporządzeniu o ochronie danych*, [w:] G. Sibiga (red.), *Ogólne rozporządzenie o ochronie*

danych. Aktualne problemy prawnej ochrony danych osobowych 2016, C.H. Beck, Warszawa 2016

Gudowski J. (red. nauk.), *Kodeks Cywilny. Komentarz. Tom III. Zobowiązania. Część ogólna*, Wolters Kluwer, Warszawa 2018, wyd. 2

Guziński M., *Środki prawne w ustawie – Prawo zamówień publicznych (wybrane zagadnienia)*, [w:] L. Kieres (red.), *Środki prawne publicznego prawa gospodarczego*, Kolonia Limited, Wrocław 2007

Haberko J., *Komentarz do art. 19*, [w:] J. Haberko, I. Uhrynowska-Tyszkiewicz, *Ustawa o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów. Komentarz*, wersja el., https://sip.lex.pl/#/commentary/587370341/167781 [dostęp 30.07.2018.

Haczkowska M. (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Wolters Kluwer, Warszawa 2014, wyd. 1

Hałub O., *Sformalizowany model dostępu do nieodpłatnej pomocy prawnej na etapie przedsądowym w Polsce*, Wrocław 2018, rozprawa doktorska (niepubl.)

Horubski K., *Charakter prawny zezwolenia na prowadzenie działalności gospodarczej na terenie specjalnej strefy ekonomicznej uprawniającego do korzystania z pomocy publicznej*, [w:] L. Kieres (red.), *Środki prawne publicznego prawa gospodarczego*, Kolonia Limited, Wrocław 2007

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

Kaczmarek-Templin B., *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – wybrane zagadnienia*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *Polska i europejska reforma danych osobowych*, Wolters Kluwer, Warszawa 2016

Kamińska I., *Ochrona danych osobowych. Komentarz*, wersja el., https://sip.lex.pl/#/commentary/587555936/353376 [dostęp 31.07.2018]

Kamińska-Pietnoczko A., *Dane osobowe w zatrudnieniu*, „Monitor Prawa Pracy" 2015, Nr 1

Kawecki M., *Prawo ochrony danych osobowych jako nowa dziedzina prawa*, „Europejski Przegląd Sądowy" 2017, Nr 5

Kawka W., *Policja w ujęciu historycznym i współczesnym*, Zakład Administracji i Prawa Administracyjnego U.S.B., Wilno 1939

Kaźmierczak K., Litwiński P., *Zagadnienia wstępne z zakresu ochrony danych osobowych pracowników*, [w:] D. Dorre-Kolasa (red.), *Ochrona danych osobowych pracow-*

ników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, C.H. Beck, Warszawa 2017

Kennedy S., *The Sources of International Law*, American University International Law Review 1987, Vol. 2, Nr 1

Kibil M., Gawroński M., *Inspektor ochrony danych (IOD)*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018

Kloc K., *Rejestrowanie czynności przetwarzania danych*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018

Kłoda M. T., *Naruszenie dóbr osobistych kredytobiorcy jako skutek uchybienia przez bank zasadom przetwarzania danych osobowych*, „Bezpieczny Bank" 2016, Nr 2

Konieczna-Drzewiecka B., Zubrycka A., *Tajemnica upoważnionego do przetwarzania danych osobowych*, „Monitor Prawniczy" 2015, Nr 21

Kozłowski A., *Istota zasad ogólnych prawa i orzeczeń sądów międzynarodowych jako źródło prawa międzynarodowego*, [w:] J. Kolasa (red.), *Istota źródła w porządku prawa międzynarodowego*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2016

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

Krasuski A., *Podstawy prawne przetwarzania danych objętych tajemnicą telekomunikacyjną*, „Przegląd Ustawodawstwa Gospodarczego" 2016, Nr 8

Krzysztofek M., *„Prawo do bycia zapomnianym" i inne aspekty prywatności w epoce Internetu w prawie UE*, „Europejski Przegląd Sądowy" 2012, Nr 8

Krzysztofek M., *Prawo do sprzeciwu wobec przetwarzania danych osobowych w rodo*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017

Kuberska W., *Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017

Lambert P., *Understanding the New European Data Protection Rules*, Taylor & Francis Group, Boca Raton 2018

Langrod J. S., *Instytucje prawa administracyjnego. Zarys części ogólnej*, Kantor Wydawniczy Zakamycze, Zakamycze 2003, reprint

Leszczyński L., *Wykładnia systemowo-aksjologiczna*, [w:] R. Hauser, Z. Niewiadomski, A. Wróbel (red.), *System prawa administracyjnego. Wykładnia w prawie administracyjnym. Tom 4*, C.H. Beck, Warszawa 2012

Lewandowski S., Machińska A., *Definicje*, [w:] S. Lewandowski, H. Machińska, A. Malinowski, J. Petzel, *Logika dla prawników,* Wydawnictwo Prawnicze LexisNexis, Warszawa 2002

Lipowicz I., *Konstytucyjne podstawy ochrony danych osobowych*, [w:] P. Fajgielski (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Wydawnictwo KUL, Lublin 2008

Lipowicz I., *Prawne formy działania administracji publicznej – między stabilizacją a potrzebą przełomu*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2016, z. 4

Litwiński P. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, C.H. Beck, Warszawa 2018

Litwiński P. (red.), *Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, C.H. Beck, Warszawa 2018

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

Lubasz D., Kwiatkowska-Cylke M., *Zasady przetwarzania danych osobowych*, [w:] D. Lubasz (red.), *RODO w e-commerce*, Warszawa 2018

Lundén B., Svensson U., *Marketing dla małych i średnich przedsiębiorstw*, BL Info Polska, Gdańsk 2014, wyd. 5

Łuczak J., *Ochrona danych osobowych jako element zarządzania bezpieczeństwem informacji*, „Studia Oeconomica Posnaniensia" 2016, Vol. 4, No. 12

Łuczejko K., *Dane osobowe w internecie – wybrane zagadnienia administracyjnoprawne*, „Acta Iuris Stetiensis – Zeszyty Naukowe Uniwersytetu Szczecińskiego" 2014, Nr 812

Maciejewski M. (red.), *Prawo do informacji publicznej. Efektywność regulacji i perspektywy jej rozwoju*, Biuro Rzecznika Praw Obywatelskich, Warszawa 2014

Masuda Y., *The Information Society as Post-Industrial Society*, World Future Society, Washington D. C. 1980

Maurer H., *Allgemeines Verwaltungsrecht*, Verlag C. H. Beck, München 2006

Maurer H., *Ogólne prawa administracyjne*, (tłum. i red.) K. Nowacki, Kolonia Limited, Wrocław 2003

Mazewski M., *Prawo do wyrażenia i wycofania zgody na przetwarzanie danych*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017

Mazurkiewicz J., *Non omnis moriar. Ochrona dóbr osobistych zmarłego w prawie polskim*, Prawnicza i Ekonomiczna Biblioteka Cyfrowa, Wrocław 2010

Mecenaite M., *Consent for processing children's personal data in the EU: following in US footsteps?*, „Information & Communications Technology Law" 2017, Vol. 26, Nr 2

Mednis A., *Prawo do wniesienia skargi do organu nadzorczego*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017

Miemiec M., *Wstęp*, [w:] M. Miemiec (red. nauk.), *Materialne prawo administracyjne*, Wolters Kluwer Polska SA, Warszawa 2013

Młynarska-Sobaczewska A., *Trzy wymiary prywatności. Sfera prywatna i publiczna we współczesnym prawie i teorii społecznej*, „Przegląd Prawa Konstytucyjnego" 2013, nr 1(13)

Naklicka P., Gawron A., *Rodosłowniczek, czyli omówienie podstawowych pojęć RODO wraz z przykładami*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018

Nerka A., *Prawo do ograniczenia przetwarzania danych osobowych*, [w:] B. Fischer, M. Sakowska-Baryła (red. nauk.), *Realizacja praw osób, których dane dotyczą*, PRESSCOM, Wrocław 2017

Nowacki J., Tobor Z., *Wstęp do prawoznawstwa*, Wolters Kluwer Polska, Warszawa 2007, wyd. 3

Ochendowski E., *Prawo administracyjne. Część ogólna*, Wydawnictwo „Dom Organizatora", Toruń 2004

Ossowska D., *Wolności i prawa osobiste*, [w:] M. Chmaj (red.), *Wolności i prawa człowieka w Konstytucji Rzeczypospolitej Polskiej*, Wolters Kluwer Polska, Warszawa 2008, wyd. 2

Pichlak M., *Zamknięty system źródeł prawa. Studium instytucjonalizacji dyskursu prawniczego*, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2013

Piechowiak M., *Filozofia praw człowieka. Prawa człowieka w świetle ich międzynarodowej ochrony*, Towarzystwo Naukowe Katolickiego Uniwersytetu Lubelskiego, Lublin 1999

Pieprzny S., *Policja. Organizacja i funkcjonowanie*, Wolters Kluwer business, Warszawa 2011

Pierzchała E., *Standardy funkcjonowania administracyjnych środków prawnych w postępowaniu przed organami pomocy społecznej*, [w:] J. Blicharz, L. Klat-Wertelecka, E. Rutkowska-Tomaszewska (red.), *Ubóstwo w Polsce*, E-Wydawnictwo, Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2017

Pizzetti F., *Article 39 TEU*, [w:] H.J. Blake, S. Mangiameli (red.), *The Treaty on European Union (TEU). A commentar*, Springer, Heidelberg-New York-Dordrecht-London 2013

Punda P., Czarnowski A.P., Gawroński M., *Kodeksy postępowania i certyfikacja*, [w:] M. Gawroński (red.), *RODO. Przewodnik ze wzorami*, Warszawa 2018

Rehof L.A., *Article 12*, [w:] G. Alfreddson, A. Eide (red.), *The Universal Declaration of Human Rights. A Common Standard of Achievement*, Martinus Nijhoff Publishers, Hague, Boston, London 1999

Riedel E., Derpa U., *Kompetenzen des Bundes und der Länder im Gesundheitswesen – dargestellt anhand ausgewählter Regelungen im Sozialgesetzbuch*, Springer-Verlag, Berlin Heidelberg 2002, cz. 5

Ruszkowski J., *Ponadnarodowość w systemie politycznym Unii Europejskiej*, Wolter Kluwer Polska, Warszawa 2010

Safjan M., *Ochrona danych osobowych – granice autonomii informacyjnej. Paradoks towarzyszący rozwojowi współczesnych technik informatycznych*, [w:] M. Wyrzykowski, *Ochrona danych osobowych*, Instytut Spraw Publicznych. Centrum Konstytucjonalizmu i Kultury Prawnej, Warszawa 1999

Sakowska-Baryła M., *Kontrolowanie przez GIODO przetwarzania danych osobowych*, „Kontrola Państwowa" 2016, Nr 2

Skorupka S., Auderska H., Łempicka Z. (red.), *Mały słownik języka polskiego*, Państwowe Wydawnictwo Naukowe, Warszawa 1968

Sobczak J., *Komentarz do art. 8*, [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, C.H. Beck, Warszawa 2013

Sobczyk P., *Ochrona danych osobowych jako element prawa do prywatności*, „Zeszyty Prawnicze" 2009, Nr 9/1

Srogosz T., *Źródła prawa międzynarodowego*, [w:] J. Barcik T. Srogosz, *Prawo międzynarodowe publiczne,* C.H. Beck, Warszawa 2017

Stępień A., Biały P., *Bezpieczeństwo danych osobowych zgodnie z RODO*, Wydawnictwo Wiedza i Praktyka, Warszawa 2017

Strzyczkowski K., *Prawo gospodarcze publiczne*, Wolters Kluwer Polska, Warszawa 2005

Studzińska J., *Zasady i przesłanki postępowania cywilnego*, [w:] J. Studzińska, P. Cioch, *Postępowanie cywilne*, C.H. Beck, Warszawa 2017, wyd. 5

Sulikowski A., *Współczesny paradygmat sądownictwa konstytucyjnego wobec kryzysu nowoczesności*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2008

Susałko M., *Ochrona danych w fazie projektowania i domyślna ochrona danych*, [w:] D. Lubasz (red.), *RODO w e-commerce*, Warszawa 2018

Szewc T., *Zgoda na przetwarzanie danych osobowych*, „Państwo i Prawo" 2008, Nr 2

Szpor G., *Strategia ochrony danych osobowych w polityce społecznej*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2012, Nr 87

Świerczyński M., *Łączniki w normach kolizyjnych*, [w:] M. Pazdan (red.), *System prawa prywatnego. Prawo prywatne międzynarodowe*, C.H. Beck, Instytut Nauk Prawnych PAN, Warszawa 2014, t. 20A

Tabakow M., Korczak J., Franczyk B., *Big Data – definicje, wyzwania i technologie informatyczne*, „Informatyka Ekonomiczna" 2014, Nr 1(31)

Taborowski M., *Konsekwencje naruszenia prawa Unii Europejskiej przez sądy krajowe*, Wolters Kluwer Polska, Warszawa 2012

Taras W., *Środki prawne – pojęcia i podziały*, [w:] K. Chorąży, W. Taras, A. Wróbel (red.), *Postępowanie administracyjne, egzekucyjne i sądowoadministracyjne*, Wolters Kluwer business, Warszawa 2009

Tarnawa-Zajączkowska M., *Rewolucje w ochronie danych osobowych – gdzie ich szukać?*, „Casus" 2017, Nr 4

Tarnawa-Zajączkowska M., *Zmiana ustawy o ochronie danych osobowych. Administrator danych osobowych jako podmiot zbiorowy*, „Casus" 2016, Nr 2

Trubalski A., *Prawne aspekty implementacji prawa UE do systemu prawnego RP*, C.H. Beck, Warszawa 2016

Ura E., *Prawo administracyjne*, LexisNexis, Warszawa 2010

Voigt F., von Bussche A., *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer, Cham 2017

Walasek R., *Systemy bezpieczeństwa informacji w przedsiębiorstwach logistycznych – wyniki badania*, „Nauki o zarządzaniu. Management Sciences" 2016, Nr 1

Webster F., *Theories of the Information Society*, Routledge Taylor & Francis Group, London – New York 2006, wyd. 3

Wentkowska A., *Prawo UE wobec prawa międzynarodowego i prawa krajowego*, [w:] J. Barcik, A. Wentkowska, *Prawo Unii Europejskiej*, C.H. Beck, Warszawa 2014

Wojciechowski Ł., *Bezpieczeństwo informacji i ochrona danych osobowych jako polityka publiczna – analiza wprowadzenia mechanizmów i uregulowań prawnych*, „Polityka i Społeczeństwo" 2016, Nr 4

Woś T., *Komentarz do art.* 3, [w:] T. Woś (red. nauk.), *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Wolters Kluwer Polska, Warszawa 2016, wyd. VI

Wronkowska S., *System prawny a porządek prawny i ład społeczny*, [w:] S. Wronkowska, Z. Ziembiński (red.), *Zarys teorii prawa*, Wydawnictwo Ars boni et aequi, Poznań 1997

Wronkowska S., Zieliński M., Ziembiński Z., *Zasady prawa. Zagadnienia podstawowe*, Wydawnictwo Prawnicze, Warszawa 1974

Wróbel A. (red.), *Stosowanie prawa Unii Europejskiej przez sądy*, Wolters Kluwer Polska, Warszawa 2010, wyd. 2, t. I

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

Wróbel A., *Komentarz do art. 47*, [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, C.H. Beck, Warszawa 2013

Wróbel I., *Pojęcie usługi społeczeństwa informacyjnego w prawie wspólnotowym*, „E Biuletyn: elektroniczny biuletyn naukowy CBKE" 2007, Nr 4

Wygoda K., *Administrator bezpieczeństwa informacji a inspektor ochrony danych na tle regulacji krajowych i unijnych – wybrane zagadnienia*, „Przegląd Prawa i Administracji" 2016, Nr 105

Zieliński A., *Postępowanie cywilne. Kompendium*, C.H. Beck, Warszawa 2017

Zieliński M., *Wykładnia prawa. Zasady, reguły, wskazówki*, LexisNexis, Warszawa 2010

Zieliński T., *Stosunek prawa pracy do prawa administracyjnego*, Państwowe Wydawnictwo Naukowe, Warszawa 1977

Zimmermann J., *Motywy decyzji administracyjnej i jej uzasadnienie*, Wydawnictwo Prawnicze, Warszawa 1981

Zimmermann J., *Prawo administracyjne*, Wolters Kluwer, Warszawa 2014

Zubik M., Sokolewicz W., *Komentarz do art. 7*, [w:] L. Garlicki, M. Zubik (red.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Wydawnictwo Sejmowe, Warszawa 2016, wyd. II uzup., t. I

Żak J., *Koncepcja „prawa do bycia zapomnianym"*, [w:] M. Jabłoński, S. Jarosz-Żukowska (red.), *Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi*, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2014

Wykaz cytowanej literatury w formie elektronicznej i wykaz innych źródeł

Banki błędnie formułują klauzule zgody na przetwarzanie danych osobowych w celach marketingowych, wersja el., https://giodo.gov.pl/pl/259/10003/ [dostęp 06.07.2018]

Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, wersja el., http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 [dostęp 03.07.2018]

Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim wydany przez Konferencję Episkopatu Polski, w dniu 13 marca 2018 r., podczas 378. Zebrania Plenarnego w Warszawie, na podstawie kan. 455 Kodeksu Prawa Kanonicznego, w związku z art. 18 Statutu Konferencji Episkopatu Polski, po uzyskaniu specjalnego zezwolenia Stolicy Apostolskiej z dnia 3 czerwca 2017 r., wersja el., https://episkopat.pl/wp-content/uploads/2018/04/13.3.2018.PL_.Dekret-ogolny-o-ochronie-danych-osobowych.pdf [dostęp: 19.07.2018]

Grupa Robocza art. 29 ds. ochrony danych, *Opinia 2/2009 w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół) przyjęta dnia 11 lutego 2009*, sygn. 398/09/PL WP 160, wersja el., https://giodo.gov.pl/pl/1520022/2991 [dostęp 09.07.2018]

Grupa Robocza art. 29, *WP242 ZAŁĄCZNIK – Często zadawane pytania*, wersja el., s. 1, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 [dostęp 19.07.2018]

Grupa Robocza art. 29, *Wytyczne dotyczące prawa do przenoszenia danych*, wersja el., http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233 [dostęp 19.07.2018].

ICO GDPR guidance: Contracts and liabilities between controllers and processors, https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf [dostęp 02.08.2018]

Jeśli chcesz złożyć skargę…, https://uodo.gov.pl/pl/83/155 [dostęp 23.07.2018]

Pismo Rzecznika Praw Obywatelskich z dnia 26 kwietnia 2018 r. do Ministra Spraw Wewnętrznych i Administracji, sygn. VII.501.315.2014.AG, wersja el., https://www.rpo.gov.pl/sites/default/files/Stanowisko RPO w sprawie projektu ustawy wdrażającej dyrektywę policyjną .pdf [dostęp 30.07.2018]

Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/prace-legislacyjne-rm-i/ prace-legislacyjne-rady/wykaz-prac-legislacyjny/r70792937308 32,Projekt-ustawy-Przepisy-wprowadzajace-ustawe-o-ochronie-danych-osobowych.html [dostęp 30.07.2018]

RPO do Ministra Sprawiedliwości: „rejestr pedofilów" uderza w niewinnych członków rodzin sprawców. Są już pierwsze takie przypadki, wersja el., https://www.rpo.gov.pl/pl/content/Bodnar-do-Ziobry-rejestr-pedofilow-uderza-w-niewinnych [dostęp 30.07.2018]

Rządowy projekt ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości wraz z uzasadnieniem, wersja el., https://bip.kprm.gov.pl/kpr/form/r8706884065,Projekt-ustawy-o-ochronie-danych-osobowych-przetwarzanych-w-zwiazku-z-zapobiegan.html [dostęp 30.07.2018]

Składanie skargi w formie tradycyjnej, w tym do protokołu w siedzibie Prezesa Urzędu, wersja el., https://uodo.gov.pl/pl/83/154 [dostęp 24.07.2018]

Polskie akty normatywne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.)

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2017 r., poz. 1257 ze zm.)

Ustawa z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy (t.j. Dz. U. z 2017 r., poz. 682 ze zm.).

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2018 r., poz. 1025 ze zm.)

Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2018 r., poz. 1360)

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2018 r., poz. 917 ze zm.)

Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (t.j. Dz. U. z 2016 r., poz. 487 ze zm.)

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2017 r., poz. 2067 ze zm.)

Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (t.j. Dz. U. z 2018 r., poz. 997 ze zm.)

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883)

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922 ze zm.)

Ustawa z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (t.j. Dz. U. z 2017 r., poz. 1523)

Ustawa z dnia 6 lipca 2001 r. o usługach detektywistycznych (t.j. Dz. U. z 2017 r., poz. 556 ze zm.)

Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (t.j. Dz. U. z 2018 r., poz. 430 ze zm.)

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t j. Dz. U. z 2016 r., poz. 1764 ze zm.)

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2017 r., poz. 1219 ze zm.)

Ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2018 r., poz. 1302)

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2017 r., poz. 1907 ze zm.)

Ustawa z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (t.j. Dz. U. z 2017 r., poz. 1000)

Ustawa z dnia 28 lipca 2005 r. o kosztach postępowania w sprawach cywilnych (t.j. Dz. U. z 2018 r., poz. 300 ze zm.)

Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. Dz. U. z 2018 r., poz. 1030)

Ustawa z dnia 24 września 2010 r. o ewidencji ludności (t.j. Dz. U. z 2018 r., poz. 1382)

Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz. U. Nr 229, poz. 1497)

Ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego (t.j. Dz. U. z 2016 r., poz. 2064 ze zm.).

Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (t.j. Dz. U. z 2018 r., poz. 999 ze zm.)

Ustawa z dnia 13 kwietnia 2016 r. o bezpieczeństwie obrotu prekursorami materiałów wybuchowych (t.j. Dz. U. z 2018 r., poz. 410 ze zm.)

Ustawa z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2017 r., poz. 1398 ze zm.)

Ustawa z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań z zakresu informatyzacji działalności organów Krajowej Administracji Skarbowej (t.j. Dz. U. z 2017 r., poz. 2192)

Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r., poz. 138 ze zm.)

Ustawa z dnia 9 maja 2018 r. o przetwarzaniu danych dotyczących przelotu pasażera (Dz. U. poz. 894)

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000)

Ustawa z dnia 15 czerwca 2018 r. o zbiorowym zarządzaniu prawami autorskimi i prawami pokrewnymi (Dz. U. poz. 1293)

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r., poz. 2247)

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 lipca 2016 r. w sprawie przetwarzania informacji przez Policję (Dz. U. poz. 1091 ze zm.)

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 maja 2018 r. w sprawie przetwarzania informacji przez Służbę Ochrony Państwa (Dz. U. poz. 1069)

Akty prawa Unii Europejskiej

Traktat o funkcjonowaniu Unii Europejskiej (Dz. U. z 2004 r. Nr 90, poz. 864/2 ze zm.)

Traktat o Unii Europejskiej podpisany dnia 7 lutego 1992 r. w Maastricht (Dz. U. z 2004 r. Nr 90, poz. 864/30 ze zm.)

Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 303 z 12.12.2007 r., s. 1 ze zm.).

Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz. Urz. UE L z dnia 12.01.2001 r., s. 1 ze zm.)

Rozporządzenie Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej (Dz. Urz. UE L z dnia 26.06.2013 r., Nr 173, s. 2)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L 119 z dnia 04.05.2016 r., poz. 1

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. L 281 z dnia 23 listopada 1995 r., Nr 31 ze zm.)

Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. L 241 z 17.9.2015 r., s. 1)

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.05.2016 r., s. 89 ze zm.)

Zalecenie Komisji z dnia 10 października 2014 r. w sprawie szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych (Dz. Urz. UE L 300 z 18.10.2014 r., s. 63)

Międzynarodowe akty normatywne

Europejska Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.)

Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25 ze zm.) wraz z protokołem dodatkowym do Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych

Konwencja o prawach dziecka przyjęta przez Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych dnia 20 listopada 1989 r. (Dz. U. z 1991 r. Nr 120, poz. 526 ze zm.)

Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167)

Powszechna Deklaracja Praw Człowieka uchwalona przez ZO ONZ dnia 10 grudnia 1948 r. rezolucją 217/III A

Rekomendacja R (85)20 Komitetu Ministrów dla Państw Członkowskich w sprawie ochrony danych osobowych używanych dla celów marketingu bezpośredniego, Rady Europy „Ochrona Danych Osobowych Wykorzystywanych dla potrzeb marketingu bezpośredniego" z 25 października 1985 r.

Rekomendacja z dnia 23 listopada 2010 r. w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili; rekomendacja R(91) 10 z dnia 9 września 1991 r. dotycząca ochrony danych osobowych przekazywanych osobom trzecim przez instytucje publiczne

Rekomendacja CM/REC (2015) 5 Komitetu Ministrów dla Państw Członkowskich na temat ochrony danych osobowych wykorzystywanych dla celów zatrudnienia

Rezolucja (73) 22 z dnia 26 września 1973 r. o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze prywatnym

Rezolucja 45/95 ZO ONZ z dnia 14 grudnia 1990 r.

Wykaz wykorzystanych orzeczeń Trybunału Sprawiedliwości Unii Europejskiej

Wyrok Trybunału z dnia 27 stycznia 1982 r., sygn. 51/81

Wyrok Sądu z dnia 2 sierpnia 1993 r., sygn. C-271/91

Wyrok Trybunału w sprawach połączonych z dnia 5 marca 1996 r., sygn. C-46/93 i C-48/93

Wyrok Trybunału w sprawach połączonych z dnia 8 marca 2001 r., sygn. C 397/98 i C-410/98

Wyrok Trybunału w sprawach połączonych z dnia 13 lipca 2006, sygn. od C-295/04 do C-298/04

Wyrok Trybunału z dnia 9 listopada 2006 r., sygn. C-243/05 P

Wyrok Trybunału Sprawiedliwości z dnia 13 maja 2014 r., sygn. C-131/12, LEX nr 1455816

Wyrok Trybunału Sprawiedliwości z dnia 9 października 2014 r., sygn. C-222/13

Wyrok Sądu z dnia 20 lipca 2016 r., sygn. T-483/13

Wyrok Trybunału Sprawiedliwości z dnia 25 lipca 2018 r., sygn. C-216/18

Wykaz wykorzystanych orzeczeń polskich sądów i trybunałów

Orzeczenie TK z dnia 24 czerwca 1997 r., sygn. K 21/96, LEX nr 29146

Wyrok TK z dnia 20 listopada 2002 r., sygn. 41/02, LEX nr 57092

Wyrok TK z dnia 17 czerwca 2008 r., sygn. K 8/04, LEX nr 387751

Postanowienie SN z dnia 15 lutego 2013 r., sygn. I CSK 684/12

Wyrok SA w Warszawie z dnia 7 czerwca 2013 r., sygn. I ACa 1584/12, LEX nr 1327625

Wyrok SA w Warszawie z dnia 25 listopada 2016 r., sygn. I ACa 1565/15, LEX nr 22373847

Wyrok NSA z dnia 11 kwietnia 2003 r., sygn. II SA 3942/02, LEX nr 1148407

Wyrok NSA z dnia 10 stycznia 2013 r., sygn. I OSK 2029/11, LEX nr 1341461

Wyrok NSA z dnia 25 lipca 2017 r., sygn. I OSK 2859/16, LEX nr 2333310

Wyrok WSA w Warszawie z dnia 21 października 2009 r., sygn. II SA/Wa 857/09, LEX nr 573915

Wyrok WSA w Warszawie z dnia 18 czerwca 2010 r., sygn. II SA/Wa 151/10, LEX nr 643811

Wyrok WSA w Warszawie z dnia 18 października 2012 r., sygn. II SA/Wa 697/12, LEX nr 1241598

Wyrok WSA w Krakowie z dnia 22 lipca 2015 r., sygn. I SA/Kr 415/15, LEX nr 1770518

Wyrok WSA w Gliwicach z dnia 26 października 2015 r., sygn. IV SA/Gl 748/15, LEX nr 1816386

Wyrok WSA w Warszawie z dnia 12 lipca 2017 r., sygn. II SA/Wa 221/16, LEX nr 2113510

Pracownia Badań nad Elektroniczną Administracją

Pracownia Badań nad Elektroniczną Administracją została utworzona w dniu 1 czerwca 2017 r. jako jednostka naukowo-dydaktyczna. Działa w ramach Instytutu Nauk Administracyjnych na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Kierownikiem Pracowni jest dr Maciej Błażewski, a jej członkami są: dr Łukasz Prus, dr Witold Małecki oraz mgr Piotr Janiak.

Działania Pracowni skupiają się na prowadzeniu badań naukowych, pracy dydaktycznej oraz działalności popularyzującej wyniki badań naukowych.

Członkowie Pracowni prowadzą badania naukowe nad wykorzystaniem narzędzi technologii informacyjno-komunikacyjnej. Badania dotyczą m.in. podstawowych zagadnień, takich jak zasady funkcjonowania elektronicznej administracji oraz środki komunikacji elektronicznej. Badania obejmują także analizę stosowania nowych technologii przy wykorzystaniu konkretnych działań przez podmioty publiczne, jak prowadzenie konsultacji społecznych, współpraca z organizacjami pozarządowymi oraz udział w procesie budowlanym.

Działalność dydaktyczna koncentruje się na prowadzeniu przez członków Pracowni wykładów z przedmiotu Informatyzacji administracji publicznej na Studiach Administracji.

Pracownia Badań nad Elektroniczną Administracją prowadzi także działalność popularyzującą wyniki badań naukowych. W tym celu organizuje konferencje naukowe oraz prowadzi portal elektroniczny – www.egov.uni.wroc.pl

Noty o autorach

Dr Maciej Błażewski – adiunkt w Zakładzie Prawa Administracyjnego Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Kierownik Pracowni Badań nad Elektroniczną Administracją. Skupia się na prowadzeniu badań z zakresu: elektronicznej administracji, ochrony danych osobowych, prawa administracyjnego, prawa samorządu terytorialnego, prawa organizacji pozarządowych oraz prawa budowlanego. Jest autorem oraz współautorem wielu monografii naukowych, a także kilkudziesięciu innych opracowań naukowych, w tym artykułów naukowych oraz rozdziałów w opracowaniach zbiorowych. Jest także radcą prawnym. mail: maciej.blazewski@uwr.edu.pl

Dr Jolanta Behr – adiunkt w Zakładzie Prawa Administracyjnego Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Autorka monografii, rozdziałów w monografiach i artykułów w czasopismach naukowych z listy ministerialnej. Jest również radcą prawnym. mail: jolanta.behr@uwr.edu.pl

DOLNY ŚLĄSK

ISBN 978-83-66066-24-3 (druk)
ISBN 978-83-66066-25-0 (online)