Uniwersytet Wrocławski

Zarządzanie bezpieczeństwem informacji i ochrona danych osobowych

Zarys wykładu

Dominika Kuźnicka-Błaszkowska
Justyna Węgrzyn

Wrocław 2025

Zarządzanie bezpieczeństwem informacji i ochrona danych osobowych. Zarys wykładu

Prace Naukowe
Wydziału Prawa, Administracji i Ekonomii
Uniwersytetu Wrocławskiego

Seria: **e-Podręczniki** Nr 5

https://doi.org/10.34616/151693
Dostęp online:
https://bibliotekacyfrowa.pl/dlibra/publication/159168

Dominika Kuźnicka-Błaszkowska
Uniwersytet Wrocławski
Wydział Prawa, Administracji i Ekonomii
ORCID: 0000-0001-8804-569X

Justyna Węgrzyn
Uniwersytet Wrocławski
Wydział Prawa, Administracji i Ekonomii
ORCID: 0000-0002-7996-9441

Zarządzanie bezpieczeństwem informacji i ochrona danych osobowych. Zarys wykładu

Wrocław 2025

Korekta: *Wojciech Nowakowski*
Wykonanie okładki: *Agnieszka Buszewska*
Skład i opracowanie techniczne: *Maciej Torz*

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

ISBN 978-83-68169-09-6 (online)
ISBN 978-83-68169-10-2 (druk)

Spis treści

Wykaz skrótów

Akty prawne

EKPC	–	Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.)
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.)
k.p.k.	–	ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz. U. z 2025 r. poz. 304)
KPP UE	–	Karta praw podstawowych Unii Europejskiej (wersja skonsolidowana Dz. Urz. UE C 202/389 z 7.06.2016 r.)
MPPOiP	–	Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 16 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167)
PDPC	–	Powszechna Deklaracja Praw Człowieka przyjęta w formie rezolucji Zgromadzenia Ogólnego ONZ dnia 10 grudnia 1948 r.
RODO	–	rozporządzenie Parlamentu Europejskiego i Rady 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.)
r.k.t.	–	rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. Nr 288, poz. 1692)
TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana Dz. Urz. UE C 202/47 z 7.06.2016 r.)
u.d.i.p.	–	ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902)
u.o.i.n.	–	ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (t.j. Dz. U. z 2024 r. poz. 1222)
u.p.a.	–	ustawa z dnia 26 maja 1982 r. – Prawo o adwokaturze (t.j. Dz. U. z 2024 r. poz. 1564)
u.r.p.	–	ustawa z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz. U. z 2024 r. poz. 499)

Organy

ABW	–	Agencja Bezpieczeństwa Wewnętrznego
ETPCz	–	Europejski Trybunał Praw Człowieka
IOD	–	Inspektor Ochrony Danych
NSA	–	Naczelny Sąd Administracyjny
PUODO	–	Prezes Urzędu Ochrony Danych Osobowych
SN	–	Sąd Najwyższy
TK	–	Trybunał Konstytucyjny
TSUE	–	Trybunał Sprawiedliwości Unii Europejskiej
UODO	–	Urząd Ochrony Danych Osobowych

UOKiK – Urząd Ochrony Konkurencji i Konsumentów
WSA – Wojewódzki Sąd Administracyjny

Przedmowa

Od wielu lat mamy przyjemność prowadzić zajęcia z zakresu zarządzania bezpieczeństwem informacji i ochrony danych osobowych. W codziennej praktyce dydaktycznej dostrzegałyśmy dotkliwy brak publikacji, która w przystępny sposób przybliżałaby podstawy tej niezwykle istotnej dziedziny osobom dopiero rozpoczynającym edukacyjną i zawodową drogę. Dostępne na rynku pozycje, choć często bardzo wartościowe, adresowane są głównie do profesjonalistów i osób mających doświadczenie w tym obszarze.

Niniejszy podręcznik powstał z myślą o studentach i wszystkich tych, którzy chcą zrozumieć, czym jest bezpieczeństwo informacji i jak chronić dane w dzisiejszym świecie. Stanowi on zarys wykładu, będący punktem wyjścia do dalszych, pogłębionych studiów. Zdecydowałyśmy się udostępnić go w wolnym dostępie, aby dotrzeć do jak najszerszego grona odbiorców – niezależnie od ich możliwości finansowych czy miejsca zamieszkania. Mamy nadzieję, że stanie się on pomocnym przewodnikiem w zdobywaniu wiedzy i budowaniu świadomości na temat roli informacji we współczesnym społeczeństwie.

Autorki

Rozdział I

Znaczenie informacji i istota bezpieczeństwa informacji

1.1. Pojęcie informacji i jej znaczenie

Informacja od zawsze była i w dalszym ciągu jest „cennym dobrem", ponieważ to dzięki niej podejmowane są różnego rodzaju decyzje zarówno w sferze publicznej, jak i prywatnej. Dlatego może w skuteczny sposób być wykorzystywana w celu zdobycia przewagi czy to politycznej, czy biznesowej. „Informacja jest pojęciem bardzo pojemnym i wieloznacznym. Stanowi jednocześnie obiekt badań naukowych i praktycznych, dlatego też jest przedmiotem zainteresowania wielu specjalistów z różnych dziedzin. Próba zdefiniowania informacji w sposób jednolity wydaje się być z góry skazana na niepowodzenie. Nic więc dziwnego, że każda dyscyplina badawcza we właściwy sobie sposób definiuje pojęcie informacji"[1]. Mając powyższe na względzie, należy w pierwszej kolejności odnieść się do powszechnego znaczenia terminu informacja, a następnie do jego przykładów występujących w wybranych dziedzinach nauki, z uwzględnieniem aspektu prawnego.

Informacja z łacińskiego *informatio* oznacza „wyobrażenie, wyjaśnienie, zawiadomienie"[2]. W języku potocznym informacja to „kon-

---

[1] J. Węgrzyn, *Prawo konsumenta do informacji w Konstytucji RP i w prawie unijnym*, Wrocław 2013, s. 18.

[2] Encyklopedia PWN, hasło: *informacja*, https://encyklopedia.pwn.pl/haslo/informacja;3914686.html [dostęp: 24.06.2025].

statacja stanu rzeczy, wiadomość”[3]. Z kolei źródło informacji to miejsce jej pochodzenia, punkt wyjścia[4]. Źródłem informacji może być np. „dokument pisany w którym jest ona zawarta, człowiek dysponujący pewną wiedzą, która nie znalazła odzwierciedlenia w materiale pisanym”[5], plik komputerowy, dysk przenośny, nagranie dźwięku, obraz lub infografika.

W filozofii „informację określa się jako odbicie (odwzorowanie) różnorodności cechującej otaczającą rzeczywistość (obiekt, zdarzenie, proces, zjawisko). […]. W biologii może to być zbiór sygnałów, w psychologii – bodźce odbierane z otoczenia przez człowieka, w fizyce i chemii informacją będzie struktura lub sama obecność nieokreśloności jej stanu”[6]. Z kolei w naukach prawnych informacji przypisuje się różne znaczenia. Zdaniem G. Szpor „informacja jest przenaszalnym dobrem niematerialnym zmniejszającym niepewność”[7]. M. Maciejewski definiuje zaś informację jako „utrwalony w dowolny sposób (także w pamięci człowieka) komunikat (wiedza, świadomość) o jakimś fakcie. Innymi słowy, jest to zgromadzona, zakodowana wiedza o czymś, zakodowany komunikat o fakcie. Komunikat może być utrwalony w sposób materialny (także elektroniczny – na nośniku danych) i niemożliwy do odczytania przez inne osoby – w pamięci człowieka”[8]. Według J. Rzucidły informacje „są

[3] *Ibidem*.

[4] *Słownik języka polskiego*, hasło: informacja, https://sjp.pl/%C5%BAr%C3%B3d%C5%82o [dostęp: 24.06.2025].

[5] M. Jaśkowska, *Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego*, Toruń 2002, s. 25.

[6] B. Stefanowicz, *Informacja*, s. 7, plik z dostępem do pracy: https://depot.ceon.pl/handle/123456789/4341?show=full [dostęp: 24.06.2025].

[7] G. Szpor, [w:] I. Lipowicz, Z. Niewiadomski, K. Strzyczkowski, G. Szpor, *Prawo administracyjne. Część materialna*, Warszawa 2004, s. 97. Podaję za: P. Fajgielski, *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław 2007, s. 14.

[8] M. Maciejewski, *Prawo informacji – zagadnienia podstawowe*, [w:] W. Góralczyk (red.), *Prawo informacji. Prawo do informacji*, Warszawa 2006, s. 31.

to dane (znaki w postaci liter, cyfr, impulsów elektrycznych, które nadają się do przetwarzania), odnoszące się do podmiotów, przedmiotów, działań, faktów czy stanów, stanowiąc czynnik motywujący działania jednostek lub efekt tych działań"[9].

Duże problemy występują w przypadku próby stworzenia prawnej definicji informacji. Chociaż ustawodawca użył tego terminu nie tylko w Konstytucji i u.d.i.p., ale również w kodeksie karnym[10] czy prawie prasowym[11], w żadnym z tych aktów nie wskazał legalnej definicji pojęcia „informacja". Sąd Najwyższy w rozważaniach na temat znaczenia pojęcia „informacji" na gruncie prawa konstytucyjnego ograniczył się jedynie do dosyć enigmatycznego stwierdzenia, że „na gruncie prawa konstytucyjnego informacja rozumiana jest jako składowa część prawa do informacji, ważny składnik wolności wypowiedzi, prasy i słowa"[12].

Mając na względzie brak uniwersalnej definicji informacji, a także wiele jej znaczeń w różnych obszarach nauki, można przyjąć na potrzeby niniejszego podręcznika, że **informacja** to „jakiekolwiek dane, które pozyskane, posiadane, wytwarzane jak również przetwarzane są przez […] osoby, w związku ze świadczeniem […] usług albo realizacją obowiązków nałożonych w drodze ustawy (np. funkcjonariusze publiczni)"[13]. Natomiast źródłem informacji jest „nie tylko każdy dokument w sensie prawnym, utrwalony w jakiejkolwiek postaci, czy materiał urzędowy[14], ale w ogóle dane utrwalone w jakiejkolwiek postaci, choćby nie przyjęły one sformalizowanej

---

[9] J. Rzucidło, *Elektroniczny rząd. Aspekty konstytucyjnoprawne*, Warszawa 2015, s. 42.

[10] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. z 2025 r. poz. 383).

[11] Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (t.j. Dz. U. z 2018 r. poz. 914).

[12] Uchwała SN z dnia 22 stycznia 2003 r., I KZP 43/02, LEX.

[13] M. Jabłoński, J. Węgrzyn, *Ochrona tajemnic osób wykonujących prawnicze zawody zaufania publicznego*, Wrocław 2018, s. 43.

[14] Np. wyrok WSA w Warszawie z dnia 3 stycznia 2011 r., II SAB/Wa 264/10; wyrok NSA z dnia 18 września 2008 r., I OSK 315/08.

postaci dokumentu”[15] (np. przedmiot, którym może być narzędzie użyte w związku z popełnieniem przestępstwa).

Informacja ma istotne znaczenie w każdej sferze życia prywatnego, zawodowego, politycznego czy gospodarczego. Bez względu więc na to, czy mamy do czynienia z konsumentem, pacjentem, petentem, przedsiębiorcą, osobą wykonującą zawód zaufania publicznego (np. adwokatem, prokuratorem, sędzią, lekarzem), organem czy funkcjonariuszem publicznym – dla każdego z tych podmiotów informacja jest niezbędna do prawidłowego podejmowania decyzji.

Społeczeństwo nie jest w stanie funkcjonować bez informacji. Jest ona traktowana jako narzędzie, które pozwala człowiekowi żyć i przetrwać. Gromadzenie, utrwalanie, przetwarzanie informacji ma zasadnicze znaczenie w procesie poznawczym. Informacja odgrywała znaczącą rolę w życiu społeczno-politycznym już w czasach antycznych. W starożytnym Rzymie stanowiła oręż w walce o polityczne stanowiska, władca zbierał informacje o swoich poddanych i ich planowanych dochodach, a sami poddani byli żywo zainteresowani tym, co w danym czasie dzieje się w państwie i jakie są zamiary sprawujących władzę[16].

Informacja jest również niezbędna do realizacji podstawowych praw i wolności (np. tzw. *Miranda warning*, czyli informacje przekazywane zatrzymanym na temat ich praw), podejmowania świadomych wyborów politycznych czy osobistych. Społeczeństwo informacyjne opiera się na swobodnym przepływie informacji, która jest podstawą dla dalszego rozwoju cywilizacji. W sektorze prywatnym informacja posiada wartość materialną, pomaga budować przewagę konkurencyjną przedsiębiorstwa, zdobywać nowych klientów, a jej odpowiednie wykorzystanie może doprowadzić do wzrostu (lub analogicznie – spadku) obrotów. Wykorzystywanie fałszywych informacji czy to w postaci tzw. *deepfaków*, czy tradycyjnych form dezinformacji może

[15] M. Jabłoński, J. Węgrzyn, *Ochrona tajemnic…*, s. 43.

[16] Zob. M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice*, Wrocław 2002, s. 9.

doprowadzić do znacznych szkód w sektorze prywatnym, a w przypadku sektora publicznego – wręcz w sposób negatywny wpłynąć na funkcjonowanie państwa[17].

W zależności jednak od sytuacji, w której informacja ma zostać wykorzystana, musi ona posiadać pewne cechy charakterystyczne konieczne przy podejmowaniu decyzji. Na przykład w obrocie konsumenckim informacja musi być „prawdziwa (tzn. niewprowadzająca w błąd), zrozumiała (tj. prosta w odbiorze, niebudząca wątpliwości) i kompletna (tzn. zawierająca wszystkie dane, jakie przedsiębiorca jest obowiązany przekazać konsumentowi)"[18]. W otoczeniu biznesowym informacja „musi mieć charakterystyczne cechy, m.in.:

- aktualność;
- operatywność;
- musi dotyczyć przyszłych okresów i nie tracić jednocześnie związku z teraźniejszością;
- powinna być zrozumiała dla odbiorcy (decydenta);
- musi być dokładna i precyzyjna;
- powinna posiadać pewne źródła pozyskania"[19].

---

[17] J. Botha, H. Pieterse, *Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security*; T. Dobber *et al.*, *Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?*, „The International Journal of Press/Politics" 2021, t. 26 nr 1, https://doi.org/10.1177/1940161220944364; J.T. Hancock, J.N. Bailenson, *The Social Impact of Deepfakes*, „Cyberpsychology, Behavior, and Social Networking" 2021, t. 24, nr 3, https://doi.org/10.1089/cyber.2021.29208.jth; T. Lee, *The global rise of „fake news" and the threat to democratic elections in the USA*, „Public Administration and Policy" 2019, t. 22, nr 1, https://doi.org/10.1108/PAP-04-2019-0008; T. Matthews, *Deepfakes, Fake Barns, and Knowledge from Videos*, „Synthese" 2023, t. 201, nr 2, https://doi.org/10.1007/s11229-022-04033-x; L. Verdoliva, *Media Forensics and DeepFakes: An Overview*, „IEEE Journal of Selected Topics in Signal Processing" 2020, t. 14, nr 5, https://doi.org/10.1109/JSTSP.2020.3002101.

[18] J. Węgrzyn, *op. cit.*, s. 83.

[19] P. Prusiński, *Informacje jako strategiczne aktywa przedsiębiorstw*, [w:] J.J. Brdulak, P. Sobczak (red.), *Wybrane problemy zarządzania bezpieczeństwem informacji*, Warszawa 2014, s. 17.

Natomiast w przypadku funkcjonowania organów państwa i jego funkcjonariuszy publicznych wszelkie podejmowane przez nich działania opierają się na „odpowiednich prawnie zdefiniowanych procedurach pozyskiwania i udostępniania informacji". Dopiero ich zastosowanie pozwala np. na pozyskanie informacji, które muszą być m.in. dokładne, rzetelne i kompleksowe w celu prawidłowego podjęcia decyzji. Tak jest np. w przypadku postępowania sprawdzającego prowadzonego przez policję. Czynności podjęte w ramach tego postępowania „mogą polegać w szczególności na zażądaniu od zawiadamiającego przedstawienia dodatkowych dokumentów lub pozyskaniu informacji niezbędnych dla prawidłowej oceny zdarzenia, którego dotyczy zawiadomienie. Ta faza procesu, określana jako postępowanie sprawdzające, ma za zadanie wyeliminowanie przypadków zbędnego wszczynania i prowadzenia postępowania przygotowawczego, w sytuacji, gdy nie było ku temu podstaw. Przeprowadzenie czynności sprawdzających jest możliwe także w wypadku uzyskania informacji z innego źródła niż zawiadomienie o przestępstwie, w szczególności, gdy organ ścigania dysponuje własnymi informacjami o możliwości zaistnienia przestępstwa"[20].

1.2. Pojęcie i istota bezpieczeństwa informacji

Termin **bezpieczeństwo** z łacińskiego *sine cura = securitas* oznacza „bez pieczy". „W potocznym rozumieniu bezpieczeństwo jest ujmowane jako brak zagrożeń, zaś w definicjach słownikowych zazwyczaj występuje ujęcie utożsamiające bezpieczeństwo z pewnością, stanem przeciwstawnym zagrożeniom. Oznacza to, że termin ten można rozumieć jako synonim braku zagrożeń, ochronę przed

[20] Z. Brodzisz, *Komentarz do art. 307*, [w:] J. Skorupka (red.), *Kodeks postępowania karnego. Komentarz*, Warszawa 2023, Legalis.

zagrożeniami a także jako pewność, będącą wynikiem niewystępowania zagrożeń i (lub) skutecznych działań w celu zapobiegania im lub ich usunięcia”[21].

Mając na względzie powyższą definicję, należy podkreślić, że jest ona równie pojemna i wieloznaczna jak definicja informacji. Obejmuje swoim zakresem m.in. **bezpieczeństwo**:

- informacji (infosec);
- informacyjne;
- cyberprzestrzeni;
- ekologiczne;
- globalne;
- kooperacyjne;
- międzynarodowe;
- militarne;
- narodowe;
- państwa;
- publiczne;
- teleinformatyczne[22].

Jak wynika ze wskazanego wyżej wyliczenia, mającego charakter przykładowy, **bezpieczeństwo informacyjne** i **bezpieczeństwo informacji** nie są pojęciami tożsamymi. **Bezpieczeństwo informacyjne** „dotyczy informacji, we wszystkich etapach ich wytwarzania, przetwarzania, przechowywania i przesyłania, realizowane poprzez przeciwdziałanie przed bezprawnym dostępem i jakąkolwiek ingerencją w dane, informacje i systemy informacyjne. Obejmuje metody i narzędzia ochrony zasobów informacyjnych, takie jak: antywirusową ochronę komputerów i ich zasobów; zabezpieczenie techniczne

[21] R. Zięba, *O tożsamości nauk o bezpieczeństwie*, „Zeszyty Naukowe AON” 2012, nr 1(86), s. 7.

[22] Zob. J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, *Słownik terminów z zakresu bezpieczeństwa*, Toruń 2020, s. 20 i n.

wszelkich postaci danych osobowych w zakresie identyfikacji i tożsamości, tajemnicy lekarskiej, poufności bankowej, karalności, gwarancji tajemnicy korespondencji sieciowej; ochronę parametrów komputerów zarządzających systemami w przemyśle, bankowości, ochronie zdrowia, energetyce i łączności; procedury reagowania na ataki; ochronę prawną zasobów i systemów informacyjnych. Współcześnie przenika i krzyżuje się z wszystkimi dziedzinami bezpieczeństwa państwa"[23]. Z kolei **bezpieczeństwo informacji (infosec)** definiowane jest jako „stan i proces w ramach którego zapewnia się w całym cyklu życia informacji (powstanie, przekazanie, przetworzenie, kopiowanie, wykorzystywanie, przechowywanie, gromadzenie, niszczenie), osiąganie i utrzymywanie z uwzględnieniem obowiązujących standardów bezpieczeństwa na pożądanym przez dany podmiot poziomie, takich jej fundamentalnych właściwości, jak: dostępność, użyteczność, integralność i poufność"[24]. Innymi słowy bezpieczeństwo informacji to „ochrona informacji przed nieuprawnionym: dostępem, nielegalnym wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją, rejestracją oraz zniszczeniem. Zapewnia się przez ochronę fizyczną, elektromagnetyczną i transmisji, a także przez kryptografię oraz uniemożliwienie dostępu do urządzeń i sieci"[25].

Mając powyższe na względzie – nie budzi wątpliwości, że istota bezpieczeństwa informacji sprowadza się do zapewnienia będącym w posiadaniu danej organizacji danym odpowiedniej ochrony. Osiągnięcie tego celu wymaga wzięcia pod uwagę kluczowych cech (elementów) bezpieczeństwa informacji, o czym szerzej w kolejnym punkcie podręcznika.

---

[23] *Ibidem*, s. 24.

[24] W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, [w:] M. Kubiak, S. Topolewski (red.), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce–Warszawa 2016, s. 30.

[25] J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, *op. cit.*, s. 24.

1.3. Elementy bezpieczeństwa informacji

Odnosząc się do bezpieczeństwa informacji, należy mieć na uwadze jego trzy cechy szczególne: poufność, integralność i dostępność. Powszechnie określane są one jako **triada CIA** (z języka angielskiego: *confidentiality*, *integrity*, *availability*).

Poufność, jako pierwszy z elementów triady CIA, przejawia się w zapewnieniu tego, aby dostęp do danych miały wyłącznie osoby uprawnione. Osiągnięcie tego celu jest możliwe przez wdrożenie odpowiednich środków bezpieczeństwa, takich jak np. hasła, pseudonimizacja, szyfrowanie, programy służące do obrony przed atakami, szkolenia pracowników. Należy bowiem mieć na uwadze, że z naruszeniem poufności będziemy mieli do czynienia w różnych przypadkach. Zalicza się do nich m.in.:

- kradzież hasła, niezabezpieczonej pamięci przenośnej laptopa czy dokumentacji;
- wysłanie wiadomości e-mail z załącznikiem zawierającym dane osobowe do niewłaściwej osoby bez uprzedniego zaszyfrowania.

Drugim elementem triady jest **integralność**, która wiąże się w zagwarantowaniem tego, aby będące w posiadaniu danego podmiotu dane były prawdziwe i zabezpieczone przed ich nieupoważnionym przekształceniem, usunięciem lub dodaniem. Osiągnięcie tego celu wymaga wdrożenia nie tylko środków, które zapobiegną nieautoryzowanym zmianom danych, ale także zapewnią możliwość przywrócenia ich poprawnej wersji (stanu). Może to być m.in. oprogramowanie służące do kontroli, tworzenie kopii zapasowych, a także stosowanie mechanizmów uprawnień użytkowników, np. w taki sposób, aby uprawniona osoba miała możliwość odczytu i wprowadzenia zmian w pliku, natomiast inny użytkownik lub użytkownicy jedynie możliwość jego odczytu[26]. Zapewnieniu integralności służą

[26] J. Andress, *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*, Gliwice 2022, s. 22.

także wdrożone w danej organizacji procedury i polityki bezpieczeństwa, które określają różne sposoby postępowania.

Ostatnim elementem triady jest **dostępność**. Cecha ta – jak sama nazwa sugeruje – polega na zapewnieniu w każdym czasie dostępu do danych osobom upoważnionym (w tym osobie, której dane dotyczą). Osiągnięcie tego celu wymaga podjęcia różnych działań, które zapobiegać będą m.in. awariom urządzeń, przeciążeniom systemu informacyjnego, nieprawidłowemu funkcjonowaniu oprogramowania czy atakom hakerskim.

Mając na względzie wskazane elementy składające się na triadę CIA, należy wyjaśnić, jak odnoszą się one do bezpieczeństwa. Za przykład posłuży sytuacja dotycząca przesyłki taśm wraz z kopiami zapasowymi, na których przechowywane są „jedyne istniejące, niezaszyfrowane kopie pewnych wrażliwych danych. Gdyby taka przesyłka zaginęła podczas transportu, zdarzenie to powinno zostać zakwalifikowane jako incydent bezpieczeństwa. Może on oznaczać naruszenie poufności, ponieważ pliki danych nie były zaszyfrowane. Brak szyfrowania może również powodować problemy z integralnością"[27]. Nawet jeśli po pewnym czasie odzyskano by zagubione taśmy, nie byłoby pewności, czy nie doszło do modyfikacji ich zawartości[28]. Również w przypadku dostępności pojawia się problem, „ponieważ nie istnieją inne kopie zapasowe plików (no chyba że taśmy zostaną odzyskane)"[29].

Rozwinięciem triady CIA jest **model zwany heksadą Parkera**, który ma zastosowanie do bardziej złożonych sytuacji. Model ten poza punktami właściwymi dla triady CIA składa się dodatkowo z takich elementów, jak: posiadanie, autentyczność i użyteczność[30].

---

[27] *Ibidem*.
[28] *Ibidem*.
[29] *Ibidem*.
[30] *Ibidem*, s. 23.

Posiadanie sprowadza się do fizycznego posiadania nośnika wraz z zamieszczonymi na nim danymi. Do opisania tego atrybutu posłuży wskazany wyżej przykład przesyłki taśm wraz z kopiami zapasowymi. Załóżmy, że niektóre z tych taśm „były zaszyfrowane, a inne nie. W takiej sytuacji atrybut posiadania umożliwia bardziej precyzyjne opisanie zakresu incydentu, ponieważ utrata zaszyfrowanych taśm powoduje problem z posiadaniem, ale nie zagraża poufności, natomiast taśmy niezaszyfrowane powodują problem w dziedzinie każdego z tych atrybutów”[31].

Autentyczność w tym modelu „pozwala stwierdzić, czy dane zostały przypisane do odpowiedniego właściciela lub twórcy”[32]. Atrybut ten wymaga więc potwierdzenia tożsamości użytkownika w celu udostępnienia mu odpowiednich zasobów informacji. Z kolei **użyteczność** dotyczy tego, „w jaki sposób dane są użyteczne dla użytkownika. Użyteczność to jedyny atrybut heksady Parkera, który niekoniecznie ma charakter binarny, ponieważ w zależności od danych i ich formatu mogą istnieć różne stopnie ich użyteczności. Jest to nieco abstrakcyjna koncepcja, ale okazuje się ona zaskakująco przydatna przy omawianiu pewnych sytuacji w kontekście bezpieczeństwa. Aby to zilustrować, powróćmy raz jeszcze do przykładu z transportem taśm zawierających kopie zapasowe danych i ponownie wyobraźmy sobie, że niektóre z nich były zaszyfrowane, a inne nie. Dla […] niepowołanej osoby zaszyfrowane taśmy będą prawdopodobnie bardzo mało użyteczne, bo po prostu odczytanie danych nie będzie możliwe. Z kolei taśmy niezaszyfrowane będą dla [niej – przyp. aut.] znaczniej bardziej użyteczne, ponieważ […] nieuprawniona osoba będzie mogła bez żadnych problemów uzyskać dostęp do danych”[33].

---

[31] *Ibidem*, s. 24.
[32] *Ibidem*.
[33] *Ibidem*.

Mając na względzie triadę CIA oraz heksadę Parkera, należy podkreślić, że modele te odgrywają ważną rolę w procesie zapewnienia odpowiedniego bezpieczeństwa informacji. Uwzględnienie elementów składowych tych modeli pozwala bowiem ustalić, który z nich jest szczególnie zagrożony w danej organizacji, co w konsekwencji pozwala na wdrożenie właściwych środków zapewniających bezpieczne przetwarzanie i ochronę informacji.

Rozdział II

Ochrona informacji niejawnych a tajemnice prawnie chronione

2.1. Podstawowe zasady ochrony informacji niejawnych

2.1.1. Zakres stosowania ustawy o ochronie informacji niejawnych

Zgodnie z art. 1 ust. 1 u.o.i.n.[34] **informacje niejawne** to takie, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne. W prezentowanym ujęciu do informacji niejawnych zalicza się także informacje będące w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania[35].

W orzecznictwie sądów administracyjnych wskazuje się na dwa elementy charakterystyczne do przyznania informacji statusu niejawnej, tj. element materialny i element formalny. Ten pierwszy określa art. 1 ust. 1 u.o.i.n. poprzez wskazanie możliwości powstania określonej szkody lub zagrożenia dóbr[36]. Z kolei drugi przejawia się

---

[34] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2024 r. poz. 1222).

[35] Zob. wyrok NSA z dnia 24 kwietnia 2018 r., I OSK 1422/16.

[36] Wyrok NSA z dnia 6 lipca 2017 r., I OSK 932/16.

w nadaniu informacji określonej klauzuli tajności[37], o czym w kolejnym punkcie niniejszego podręcznika. Należy jednak mieć na uwadze, że zgodnie z treścią art. 5 u.o.i.n. klauzulę tajności „można nadać tylko informacjom niejawnym w znaczeniu materialnym"[38].

W kontekście zakresu przedmiotowego u.o.i.n. ustawodawca określił **zasady ochrony informacji niejawnych**, które dotyczą:

1) klasyfikowania informacji niejawnych;
2) organizowania ochrony informacji niejawnych;
3) przetwarzania informacji niejawnych;
4) postępowania sprawdzającego prowadzonego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy (tzw. postępowanie sprawdzające lub kontrolne postępowanie sprawdzające);
5) postępowania prowadzonego w celu ustalenia, czy przedsiębiorca[39] nim objęty zapewnia warunki do ochrony informacji niejawnych (tzw. postępowanie bezpieczeństwa przemysłowego);
6) organizacji kontroli stanu zabezpieczenia informacji niejawnych;
7) ochrony informacji niejawnych w systemach teleinformatycznych;
8) stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych[40].

   Ponadto, ustawodawca wskazał, że:

   – przepisy u.o.i.n. nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych[41];

---

[37] *Ibidem*.

[38] *Ibidem*.

[39] Przedsiębiorcą jest przedsiębiorca w rozumieniu ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców lub każda inna jednostka organizacyjna, niezależnie od formy własności, którzy w ramach prowadzonej działalności gospodarczej zamierzają realizować lub realizują związane z dostępem do informacji niejawnych umowy lub zadania wynikające z przepisów prawa, art. 2 pkt 13 u.o.i.n.

[40] Art. 1 ust. 1 u.o.i.n.

[41] Art. 1 ust. 3 u.o.i.n.

– do danych osobowych stanowiących informacje niejawne nie stosuje się przepisów o ochronie danych osobowych[42];
– do danych osobowych stanowiących informacje niejawne stosuje się przepisy u.o.i.n.[43]

Wskazane powyżej zasady mają zastosowanie do różnych kategorii podmiotów, co sprawia, że mamy do czynienia z szerokim zakresem podmiotowym. Przesądza o tym już treść art. 1 ust. 2 pkt 1 u.o.i.n., w którym wymienia się otwarty katalog organów władzy publicznej. Ustawodawca wymienił tu w szczególności: Sejm i Senat, Prezydenta RP, organy administracji rządowej, organy jednostek samorządu terytorialnego, a także inne podległe im jednostki organizacyjne lub przez nie nadzorowane, sądy i trybunały, organy kontroli państwowej i ochrony prawa. Wśród pozostałych wymienionych w art. 1 ust. 2 pkt 2–6 kategorii podmiotów są także: jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane; Narodowy Bank Polski; państwowe osoby prawne i inne niż wyżej wymienione państwowe jednostki organizacyjne; jednostki organizacyjne podległe organom władzy publicznej lub nadzorowane przez te organy; przedsiębiorcy zamierzający ubiegać się albo ubiegający się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujący takie umowy albo wykonujący na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

2.1.2. Klasyfikacja informacji niejawnych

Jak wynika z rozwiązań przyjętych na gruncie u.o.i.n., informacja ma charakter niejawny wówczas, gdy zostanie jej nadana jedna z **czterech klauzul tajności**, a mianowicie: **ściśle tajne, tajne,**

[42] Art. 1 ust. 4 u.o.i.n.
[43] Art. 1 ust. 5 u.o.i.n.

poufne lub zastrzeżone. Należy jednak mieć na uwadze, iż nośnikiem wskazanego rodzaju informacji może być dokument lub materiał, a to oznacza, że nie tylko informacja, ale także nośnik podlega ochronie. W myśl art. 2 pkt 3 u.o.i.n. **dokumentem** jest każda utrwalona informacja niejawna. Na tle tego przepisu dostrzega się przyjętą przez ustawodawcę „formułę otwartego sposobu utrwalenia. Należy w związku z tym przyjąć, że chodzi tu o wszelkie dostępne obecnie sposoby utrwalenia informacji (w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej itd.). Przepis ten nie eliminuje jednocześnie możliwości – w razie pojawienia się nowych, obecnie nieznanych technik – zakwalifikowania ich jako takich, które odpowiadają jego wykładni”[44]. Drugim nośnikiem informacji niejawnych jest **materiał**. Przez termin ten należy rozumieć dokument lub przedmiot albo dowolną ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia[45].

Mając powyższe na względzie, należy podkreślić, że informacjom niejawnym nadaje się klauzulę „**ściśle tajne”**, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
2) zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
3) zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
4) osłabi gotowość obronną Rzeczypospolitej Polskiej;

---

[44] M. Jabłoński, T. Radziszewski, *Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych*, Wrocław 2012, s. 29.

[45] Art. 2 pkt 4 u.o.i.n.

5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
6) zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
7) zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych, osób, którym udzielono środków ochrony i pomocy przewidzianych w ustawie z dnia 28 listopada 2014 r. o ochronie i pomocy dla pokrzywdzonego i świadka, albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, lub osób dla nich najbliższych[46].

Do informacji objętych klauzulą „**ściśle tajne"** zaliczono m.in.: akta postępowań weryfikacyjnych sporządzone przez Komisję Weryfikacyjną utworzoną na podstawie ustawy z dnia 9 czerwca 2006 r. Przepisy wprowadzające ustawę o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego; nośniki informatyczne – zawierające materiały uzyskane w wyniku realizacji zadań zespołów roboczych członków Komisji Weryfikacyjnej (wyrok NSA z dnia 29 kwietnia 2016 r., I OSK 252/15); informacje o pracownikach i współpracownikach oraz operacjach i działaniach prowadzonych przez cywilne służby wywiadowcze państwa; informacje o trwającej operacji wywiadowczej realizowanej przez polskie wojskowe służby wywiadowcze przy udziale służb sojuszniczych, prowadzonej poza terytorium RP, które to informacje zawierają dane co

[46] Art. 5 ust. 1 u.o.i.n.

do form i metod pracy operacyjnej tych służb oraz osób uczestniczących w działaniach (postanowienie SN – Izba Karna z 30 października 2014 r., I KZP 19/14).

Z kolei klauzulę „**tajne"** nadaje się informacjom niejawnym, jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
2) pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
3) zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;
4) utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
5) w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
6) przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej[47].

We wskazanym wyżej ujęciu do informacji objętych klauzulą „**tajne"** zaliczono np. opis form i metod pracy operacyjnej służb wywiadowczych państwa (postanowienie SN – Izba Karna z 30 października 2014 r., I KZP 19/14); informację dotyczącą mechanizmów działania sprawców przy dokonywaniu przestępstw w związku z obrotem paliwami wykonaną w oparciu o dane uzyskane w toku przeprowadzonych i toczących się postępowań procesowo-operacyjnych Policji (wyrok SN – Izba Karna z dnia 8 lutego 2018 r., V KK 224/17).

[47] Art. 5 ust. 2 u.o.i.n.

Kolejna klauzula „**poufne”** nadawana jest informacjom niejawnych, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej[48];
2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
3) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
6) zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej[49].

Przykładem informacji objętych klauzulą **„poufne”** jest m.in. dokument dotyczący przyjętej przez rząd RP strategii negocjacyjnej podczas rozpoczynających się międzynarodowych prac związanych z jedną z najważniejszych spraw z zakresu ochrony środowiska i przemysłu (wyrok WSA w Warszawie z dnia 11 października 2017 r., II SA/Wa 2218/16); dokument ABW dotyczący odmowy uznania cudzoziemca za obywatela polskiego (wyrok NSA z dnia 7 lutego 2023 r., II OSK 2780/21).

Ostatnia przewidziana w u.o.i.n. klauzula tajności to **„zastrzeżone”**. Nadawana ona jest informacjom niejawnym, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie

---

[48] Zob. wyrok NSA z dnia 26 marca 2013 r., I OSK 2863/12.

[49] Art. 5 ust. 3 u.o.i.n.

może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli[50], wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej[51].

Do informacji oznaczonych klauzulą **„zastrzeżone"** zalicza się np.: raport odnoszący się do jednej ze strategicznych gałęzi gospodarki Polski, tj. górnictwa miedzi, który to raport dotyczy postępowania o udzielenie koncesji na wydobywanie tego surowca (wyrok WSA w Warszawie z dnia 18 marca 2015 r., II SA/Wa 2243/14); procedury ochrony i poruszania się kolumny zabezpieczonej przez Biuro Ochrony Rządu[52] (wyrok WSA w Warszawie z dnia 3 grudnia 2018 r., II SA/Wa 772/18).

Jak wynika z powyższych rozwiązań przyjętych na tle art. 5 u.o.i.n., „ustawodawca dla wartościowania przesłanki uznania konkretnej informacji za niejawną posłużył się kryterium szkody. W zależności od tego, jaki skutek miałoby lub ma udostępnienie informacji, wyróżniona została:

- «wyjątkowo poważna szkoda» przy nadaniu klauzuli «ściśle tajne»;
- «poważna szkoda» przy nadaniu klauzuli «tajne»;
- «szkoda» przy nadaniu klauzuli «poufne»;
- «szkodliwy wpływ» przy nadaniu klauzuli «zastrzeżone»"[53].

Z treści wskazanego wyżej przepisu „wnika więc, że nie jest wystarczające wystąpienie samego zagrożenia definiowanego przez ustawodawcę przez odwołanie się do szeregu pojęć (w tym również takich, które nie są na gruncie prawa zdefiniowane bądź są defi-

[50] Zob. wyrok WSA w Krakowie z dnia 15 września 2017 r., II SA/Kr 1043/17.

[51] Art. 5 ust. 4 u.o.i.n.

[52] Obecna Służba Ochrony Państwa powstała na mocy ustawy z dnia 28 grudnia 2017 r. o Służbie Ochrony Państwa (t.j. Dz. U. z 2024 r. poz. 325).

[53] M. Jabłoński, T. Radziszewski, *op. cit.*, s. 42.

niowane różnorodnie). Dla nadania konkretnej informacji klauzuli tajności warunkiem *sine qua non* jest wykazanie również, że ujawnienie w takiej sytuacji przedmiotowej informacji może mieć lub ma (w zależności od klauzuli) negatywny skutek w postaci zaistnienia szkody"[54]. Nie ulega więc wątpliwości, że „stosując przepisy ustawy o ochronie informacji niejawnych konieczne jest stosowanie wykładni celowościowej i ustalenie, jaka była intencja ustawodawcy przy tworzeniu określonych przepisów oraz czy ujawnienie żądanych we wniosku informacji zagraża interesom państwa, porządkowi prawnemu, bezpieczeństwu funkcjonariuszy czy też bezpieczeństwu prowadzonych przez nich operacji"[55].

2.1.3. Procedura nadania i zniesienia klauzuli tajności

Nadanie informacjom niejawnym klauzuli tajności „ściśle tajne", „tajne", „poufne" lub „zastrzeżone" wymaga przeprowadzenia procedury, o której mowa w przepisach u.o.i.n. Kluczowe w tej kwestii znaczenie ma art. 6 u.o.i.n., który określa:

- podmiot nadający klauzulę tajności (ust. 1);
- czas ochrony informacji objętych klauzulą tajności (ust. 2);
- procedurę zniesienia lub zmiany klauzuli tajności (ust. 3 i 5–7);
- obowiązek przeprowadzenia przeglądu materiałów podlegających ochronie (ust. 4);
- możliwość oznaczenia różnymi klauzulami tajności poszczególnych części materiału (ust. 8);
- upoważnienie ustawowe do wydania przez Prezesa Rady Ministrów rozporządzenia regulującego sposób oznaczenia materiałów, umieszczania na nich klauzul tajności, a także tryb i sposób zmiany znoszenia nadanej klauzuli (ust. 9–10).

---

[54] *Ibidem*, s. 42 i n.

[55] Wyrok NSA z dnia 27 września 2019 r., I OSK 2687/17.

Mając powyższe na względzie, należy podkreślić, że w myśl art. 6 ust. 1 u.o.i.n. **klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału**[56]. W praktyce oznacza to, że „każdorazowo […] podmiot uprawniony do nadania klauzuli tajności winien badać, czy z punktu widzenia celu ochrony informacji niejawnych nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej"[57].

Nadanie klauzuli tajności to proces, który wymaga odpowiedniego oznaczenia materiału, tj. w sposób wyraźny i w pełnym brzmieniu. Wymogi te określone zostały w rozporządzeniu Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczenia materiału i umieszczenia na nich klauzuli tajności[58]. Zgodnie z treścią § 3 ust. 2 r.k.t. w sytuacji, gdy poszczególnym częściom materiału zostały nadane różne klauzule tajności bądź gdy niektóre z tych części są jawne, wyodrębnione części oddziela się oznaczeniem odpowiedniej klauzuli tajności wskazanej w pełnym brzmieniu lub określeniem „jawne". Części materiału zawierające tekst lub obraz oddziela się przez odpowiednie ich oznaczenie przed rozpoczęciem i po zakończeniu tekstu lub obrazu. Natomiast jeżeli poszczególnym częściom materiału nadano różne klauzule tajności, materiał oznacza się klauzulą co najmniej równą najwyższej klauzuli

[56] Zgodnie z art. 2 pkt 3 u.o.i.n. dokumentem jest każda utrwalona informacja niejawna. Materiałem jest zaś dokument lub przedmiot albo dowolna ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytworzenia (art. 2 pkt 4 u.o.i.n.).

[57] Wyrok WSA w Warszawie z dnia 8 grudnia 2011 r., II SA/Wa 1844/11.

[58] Dz. U. z 2011 r. Nr 288, poz. 1692.

tajności, jaką nadano części materiału (§ 3 ust. 3 r.k.t.). W procedurze tej stosuje się następujące oznaczenia:

1) „00" – dla klauzuli „ściśle tajne";
2) „0" – dla klauzuli „tajne";
3) „Pf" – dla klauzuli „poufne";
4) „Z" – dla klauzuli „zastrzeżone".

Procedura dotycząca nadania klauzuli tajności odnosi się zarówno do dokumentu nieelektronicznego, jak i elektronicznego. Przez ten pierwszy należy rozumieć dokument utrwalony na nośniku innym niż informatyczny nośnik danych, o ile ze względu na organizację obiegu informacji niejawnych podlega rejestracji (§ 2 pkt 4 r.k.t.).

Oznaczenie dokumentu nieelektronicznego utrwalonego w formie pisma odbywa się w następujący sposób:

1) na każdej stronie umieszcza się:
   a) na środku, jako pierwszy element w nagłówku strony, klauzulę tajności;
   b) numer egzemplarza, a w przypadku gdy dokument wykonano w jednym egzemplarzu, napis „egz. pojedynczy";
   c) sygnaturę literowo-cyfrową, na którą składają się: literowe oznaczenie jednostki lub komórki organizacyjnej, symbol oznaczenia klauzuli tajności, numer, pod którym ten dokument został zarejestrowany, i rok, w którym dokonano rejestracji, a także, w zależności od potrzeb, inne oznaczenia ułatwiające ustalenie miejsca wykonania dokumentu w jednostce lub komórce organizacyjnej lub też jego przynależność do określonej sprawy;
   d) numer strony oraz liczbę stron całego dokumentu;
   e) na środku, jako ostatni element w stopce strony, klauzulę tajności (§ 5 ust. 1 pkt 1 r.k.t.);
2) na pierwszej stronie umieszcza się również:
   a) nazwę jednostki lub komórki organizacyjnej;
   b) nazwę miejscowości i datę podpisania dokumentu;

c) w przypadku dokumentu, któremu nadano bieg korespondencyjny, imię i nazwisko lub nazwę stanowiska adresata; w przypadku wielu adresatów dokumentu, któremu nadano bieg korespondencyjny, dopuszcza się możliwość umieszczenia jedynie adnotacji „adresaci według rozdzielnika" (§ 5 ust. 1 pkt 2 r.k.t.);

3) na ostatniej stronie pod treścią umieszcza się również:
   a) liczbę załączników;
   b) liczbę stron lub innych jednostek miary wszystkich załączników lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary;
   c) klauzule tajności załączników z numerami, pod jakimi zostały zarejestrowane, oraz liczbę stron każdego załącznika lub informację określającą rodzaj załączonego materiału i jego odpowiednią jednostkę miary;
   d) w przypadku, gdy adresatowi wysyła się inną liczbę załączników niż pozostawia w aktach, dodatkowo napis „tylko adresat" – jeżeli załączniki mają być przekazane adresatowi bez pozostawienia ich w aktach lub napis „do zwrotu" – jeżeli załączniki mają zostać zwrócone nadawcy;
   e) stanowisko oraz imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do jego podpisania;
   f) liczbę wykonanych egzemplarzy;
   g) adresatów poszczególnych egzemplarzy dokumentu lub adnotację „adresaci według rozdzielnika";
   h) dyspozycję „ad acta" w przypadku egzemplarza pozostającego w aktach nadawcy;
   i) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę (§ 5 ust. 1 pkt 3 r.k.t).

Mając powyższe na względzie, należy jednak podkreślić, że w przypadku dokumentu nieelektronicznego utrwalonego w formie pisma, któremu nadano klauzulę tajności „zastrzeżone", dopuszcza się odstą-

pienie od umieszczenia oznaczeń wskazanych w § 5 ust. 1 pkt 1 lit. b oraz pkt 3 lit. f–i. Za wyjątkiem wskazanych wyżej oznaczeń, na dokumencie nieelektronicznym można zamieścić dyspozycję dotyczącą:

1) braku zgody na kopiowanie lub tłumaczenie części albo całości dokumentu;
2) braku zgody na udzielanie informacji o treści dokumentu;
3) określenia daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności całości lub części dokumentu (§ 7 ust. 1 r.k.t.).

W razie gdy dokument nieelektroniczny stanowi załącznik, wówczas na pierwszej stronie umieszcza się dodatkowo informację: „Załącznik nr … do dokumentu nr … z dnia …" (§ 9 ust. 1 r.k.t.). Natomiast gdy wraz z dokumentem przesyła się załączniki zawierające informacje niejawne, to:

1) dokument oznacza się klauzulą tajności nie niższą niż najwyższa klauzula tajności załączników;
2) na dokumencie – jeżeli po trwałym odłączeniu załączników dokument jest jawny albo jego klauzula tajności jest inna niż określona zgodnie z pkt 1 – na każdej stronie pod numerem egzemplarza umieszcza się adnotację o jawności albo klauzuli tajności dokumentu po odłączeniu załączników (§ 9 ust. 2 r.k.t.).

Jak zostało wskazane już wcześniej, procedura nadania informacjom klauzuli tajności dotyczy także **dokumentu elektronicznego**, przez który należy rozumieć dokument utrwalony na informatycznym nośniku danych lub przetwarzany w systemie teleinformatycznym, o ile ze względu na organizację obiegu informacji niejawnych podlega rejestracji (§ 2 pkt 3 r.k.t.). Dokument, o którym mowa, oznacza się w ten sposób, że jego metryka[59] zawiera następujące informacje:

[59] Metryka dokumentu elektronicznego to zestaw informacji o dokumencie elektronicznym, powiązanych z dokumentem lub umieszczonych na nim, stanowiących jego oznaczenie (§ 2 pkt 5 r.k.t.).

1) klauzulę tajności;
2) sygnaturę literowo-cyfrową (identycznie jak przy dokumencie nieelektronicznym);
3) nazwę jednostki lub komórki organizacyjnej;
4) datę rejestracji dokumentu;
5) w przypadku dokumentu, któremu nadano bieg korespondencyjny, wskazanie adresatów przez podanie imion i nazwisk lub nazw ich stanowisk;
6) klauzule tajności załączników wraz z numerami, pod jakimi zostały zarejestrowane;
7) stanowisko, imię i nazwisko lub inne oznaczenie wskazujące osobę uprawnioną do podpisania dokumentu;
8) imię i nazwisko lub inne oznaczenie wskazujące wykonawcę;
9) nazwę nadaną dokumentowi lub określenie, czego dokument dotyczy (§ 6 ust. 1 r.k.t.).

Ponadto w przypadku dokumentu elektronicznego dyspozycję dotyczącą:

1) braku zgody na kopiowanie lub tłumaczenie części albo całości dokumentu;
2) braku zgody na udzielanie informacji o treści dokumentu;
3) określenia daty lub wydarzenia, po którym nastąpi zniesienie lub zmiana klauzuli tajności całości lub części dokumentu,

   można zamieścić w jego metryce (§ 7 r.k.t.). W metryce dokumentu elektronicznego umieszcza się także informację: „Załącznik nr … do dokumentu nr … z dnia …", gdy dokument elektroniczny stanowi załącznik. Poza tym gdy wraz z dokumentem przesyła się załączniki zawierające informacje niejawne, to w metryce dokumentu umieszcza się:
   - informacje o klauzuli tajności dokumentu, która nie może być niższa niż najwyższa klauzula tajności załączników, a także
   - adnotację o jawności albo klauzuli tajności dokumentu, jeżeli po trwałym odłączeniu załączników dokument jest jawny

albo klauzula tajności jest inna niż określona w poprzednim odniesieniu (§ 9 ust. 3 r.k.t.)[60].

Informacje, którym nadano klauzulę tajności, podlegają ochronie do czasu jej zniesienia lub zmiany. Osoba uprawniona do nadania klauzuli może określić datę (np. 1.07.2025 r.) lub wydarzenie (np. finał siatkówki Ligi Narodów), po którym nastąpi zniesienie lub zmiana klauzuli tajności (art. 6 ust. 2 u.o.i.n.). Czynności te (zniesienie lub zmiana klauzuli tajności) są możliwe wyłącznie po wyrażeniu pisemnej zgody przez osobę uprawnioną do nadania klauzuli tajności albo jej przełożonego w przypadku ustania lub zmiany ustawowych przesłanek ochrony, o których mowa w art. 5 u.o.i.n. W przypadku informacji niejawnych objętych klauzulą „ściśle tajne" pisemną zgodę wyraża kierownik jednostki organizacyjnej, w której materiałowi została nadana klauzula tajności (art. 6 ust. 5 u.o.i.n.). W sytuacji gdy doszło do zniesienia lub zmiany klauzuli tajności, kolejnym etapem procedury jest podjęcie czynności polegających na naniesieniu odpowiednich zmian w oznaczeniu materiału i poinformowaniu o nich odbiorców. Jeżeli odbiorcy materiału przekazali go kolejnym odbiorcom, to wówczas są oni odpowiedzialni za poinformowanie ich o zniesieniu lub zmianie klauzuli tajności (art. 6 ust. 6 u.o.i.n.).

Tryb i sposób zmiany lub znoszenia nadanej klauzuli reguluje wskazane już wcześniej rozporządzenie Prezesa Rady Ministrów (r.k.t.).

---

[60] W tym miejscu warto wspomnieć, że w przypadku materiałów innych niż dokument nieelektroniczny lub elektroniczny klauzulę tajności i sygnaturę literowo-cyfrową umieszcza się przez ostemplowanie, nadrukowanie, wpisanie odręczne, trwałe dołączenie metek, nalepek, kalkomanii lub w inny widoczny sposób, w szczególności na ich obudowie lub opakowaniu. Z kolei materiał, który ze względu na organizację obiegu informacji niejawnych nie podlega rejestracji, oznacza się w sposób zapewniający jednoznaczną identyfikację jego klauzuli tajności, w szczególności przez jej umieszczenie na materiale. Utrwalenie informacji niejawnych w formie dźwięku lub obrazu poprzedza się i kończy informacją o nadanej klauzuli tajności, o ile istnieją takie możliwości (§ 10 r.k.t.).

W myśl jego postanowień zgody na zniesienie lub zmianę klauzuli tajności udziela się w odrębnym dokumencie podlegającym rejestracji lub przez oznaczenie w postaci umieszczenia informacji:

1) na dokumencie – w przypadku dokumentu nieelektronicznego;
2) w metryce dokumentu – w przypadku dokumentu elektronicznego (§ 12 r.k.t.).

Jeżeli chodzi o dokument nieelektroniczny utrwalony w formie pisma, to oznaczenia zniesienia na nim klauzuli tajności dokonuje się następująco:

1) skreśla się wszystkie dotychczasowe oznaczenia znoszonej klauzuli tajności;
2) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli tajności umieszcza się napis „Zniesiono klauzulę tajności" oraz datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności (§ 13 ust. 1 r.k.t.).

Z kolei w przypadku zmiany klauzuli tajności oznaczenia dokonuje się w następujący sposób:

1) skreśla się wszystkie dotychczasowe oznaczenia klauzuli tajności;
2) nad skreślonymi oznaczeniami klauzuli tajności umieszcza się oznaczenie nowej klauzuli tajności;
3) nad pierwszym w kolejności skreślonym oznaczeniem klauzuli umieszcza się datę, podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tych adnotacji oraz wskazuje się podstawę dokonania czynności (§ 13 ust. 2 r.k.t.).

Skreśleń i adnotacji dokonują kierownik kancelarii tajnej, kierownik archiwum lub jego zastępca, kierownik innej niż kancelaria tajna komórki, w której są rejestrowane materiały niejawne, albo inne osoby upoważnione przez nich lub przez kierownika jednostki organizacyjnej (§ 13 ust. 3 r.k.t.). Czynności, o których mowa, dokonuje się kolorem czerwonym, w sposób czytelny. Wycieranie, wywabianie lub zmazywanie klauzul tajności i dokonywanych zmian jest

niedozwolone (§ 13 ust. 4 r.k.t.). Natomiast oznaczenie zmiany lub zniesienia klauzuli tajności dokumentu elektronicznego umieszcza się w jego metryce.

W przypadku gdy dokument nieelektroniczny wytworzony został w wyniku kopiowania lub tłumaczenia, na dokumencie umieszcza się:

1) w przypadku kopii – na pierwszej stronie sygnaturę literowo-cyfrową;
2) w pozostałych przypadkach – odpowiednio oznaczenia, o których mowa w § 5;
3) na wszystkich stronach:
   a) w przypadku kopiowania napis „Wydruk", „Kopia", „Odpis", „Wyciąg" albo „Wypis";
   b) w przypadku tłumaczenia napis „Tłumaczenie z języka (nazwa języka)" oraz podpis, imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą tłumaczenia;
4) na ostatniej stronie w przypadku kopiowania dodatkowo potwierdzenie zgodności z oryginałem zawierające:
   a) napis „Za zgodność";
   b) odcisk pieczęci z nazwą jednostki lub komórki organizacyjnej, w której wytworzono dokument;
   c) podpis, imię i nazwisko lub inne oznaczenie wskazujące kierownika jednostki lub komórki organizacyjnej, w której dokonano kopiowania, albo osobę przez niego upoważnioną (§ 15 ust. 1 r.k.t.).

Poza tym należy zwrócić uwagę, że wytworzenie dokumentu w wyniku kopiowania lub tłumaczenia dokumentu nieelektronicznego odnotowuje się na ostatniej stronie dokumentu kopiowanego lub tłumaczonego przez umieszczenie informacji o:

1) nazwie jednostki lub komórki organizacyjnej, w której wytworzono dokument;
2) liczbie egzemplarzy dokumentu wytworzonego;

3) dacie wytworzenia dokumentu;
4) numerze, pod jakim wytworzony dokument został zarejestrowany (§ 15 ust. 2 r.k.t.).

Wskazane w pkt 1–3 informacje umieszcza się przed wytworzeniem dokumentu w wyniku kopiowania lub tłumaczenia, natomiast numer, pod jakim został on zarejestrowany, umieszcza się po wytworzeniu (§ 15 ust. 3 r.k.t.). W przypadku zaś kopiowania lub tłumaczenia dokumentu elektronicznego informacje wymienione powyżej w pkt 1–4 umieszcza się w jego metryce (§ 15 ust. 4 r.k.t.). W metryce dokumentu elektronicznego wytworzonego w wyniku kopiowania lub tłumaczenia umieszcza się:

1) informacje, o których mowa w § 6;
2) odpowiednio informację: „Odwzorowanie cyfrowe", „Kopia", „Odpis", „Wyciąg", „Wypis" albo „Tłumaczenie języka (nazwa języka)";
3) imię i nazwisko lub inne oznaczenie wskazujące osobę dokonującą kopiowania albo tłumaczenia (§ 15 ust. 5 r.k.t.)[61].

Odnosząc się do procedury nadania oraz zniesienia lub zmiany klauzuli tajności, należy zwrócić uwagę na wynikający z art. 6 ust. 4 u.o.i.n. **obowiązek dokonywania okresowego przeglądu.** Przegląd materiałów przeprowadzany jest przez kierowników jednostek organizacyjnych nie rzadziej niż raz na 5 lat w celu ustalenia, czy spełniają one ustawowe przesłanki ochrony. Ustawodawca wskazał jednak, że chronione bez względu na upływ czasu są:

1) dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji, uprawnionych do wykonywania na podstawie ustawy czynności operacyjno-rozpoznawczych jako funkcjonariuszy, żołnierzy lub pracowników wykonujących te czynności;

---

[61] W przypadku dokumentu o klauzuli „zastrzeżone" dopuszcza się odstąpienie od umieszczenia oznaczeń, o których mowa w ust. 1 pkt 3 i 4, ust. 2 i 4 oraz ust. 5 pkt 2 i 3 (§ 15 ust. 6 r.k.t.).

2) dane mogące doprowadzić do identyfikacji osób, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych służbom i instytucjom uprawnionym do ich wykonywania na podstawie ustawy;
3) informacje niejawne uzyskane od organów innych państw lub organizacji międzynarodowych, jeżeli taki był warunek ich udostępnienia (art. 7 ust. 1 u.o.i.n.).

Poza tym ustawodawca przewidział **wyjątki od bezterminowej ochrony**. Jak wynika bowiem z treści art. 7 ust. 2 u.o.i.n., ochronie nie podlegają dane wskazane powyżej w pkt 1 i 2, zawarte w dokumentach, zbiorach danych, rejestrach i kartotekach, a także w aktach funkcjonariuszy i żołnierzy organów bezpieczeństwa państwa, przekazanych do Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu na podstawie przepisów:

1) ustawy z dnia 18 grudnia 1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (Dz. U. z 2023 r. poz. 102);
2) ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów (Dz. U. z 2023 r. poz. 342, 497, 1195 i 1872)
   – chyba że nadano im klauzulę tajności w wyniku przeglądu, o którym mowa w art. 19 ustawy z dnia 29 kwietnia 2016 r. o zmianie ustawy o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu oraz niektórych innych ustaw (Dz. U. poz. 749), lub przeglądu, o którym mowa w art. 6 ust. 4.

Za wyjątkiem wskazanych wyżej kwestii należy zwrócić także uwagę na **zasady dostępu do informacji niejawnych** objętych klauzulą tajności, które wyrażone zostały w art. 8 u.o.i.n. Zgodnie z tym przepisem informacje, o których mowa:

1) mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności[62];
2) muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności[63];
3) muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

Jak wynika z orzecznictwa sądów administracyjnych, do realizacji ochrony wynikającej z art. 8 u.o.i.n. niezbędne są dwa elementy, tj. materialny i formalny. „Element materialny określa art. 1 ust. 1 ustawy o ochronie informacji niejawnych, wskazujący na możliwość powstania określonej szkody czy zagrożenia dóbr. Element formalny wyraża się w nadanej klauzuli tajności. Jednocześnie, zgodnie z art. 5 ustawy o ochronie informacji niejawnych, klauzulę taką można nadać tylko informacjom niejawnym w znaczeniu materialnym”[64]. Należy

[62] WSA w Warszawie zawrócił uwagę, że „bez formalnego zniesienia klauzuli, zgodnie z przepisami ustawy o ochronie informacji niejawnych, przekazanie informacji niejawnych stronie skarżącej będzie stanowiło udostępnienie informacji niejawnych podmiotowi nieuprawnionemu, a tym samym będzie stanowiło naruszenie przepisu art. 8 ust. 1. tej ustawy”, wyrok WSA w Warszawie z dnia 10 października 2017 r., II SA/Wa 203/17.

[63] Zob. wyrok WSA w Warszawie z dnia 6 października 2016 r., II SA/Wa 885/16.

[64] Wyrok NSA z dnia 6 lipca 2017 r., I OSK 932/16. Argumentację tę podzielił także WSA w Warszawie w wyroku z dnia 4 marca 2019 r., II SA/Wa 1722/18: „Dla szerszej ochrony, wynikającej z art. 8 ustawy o ochronie informacji niejawnych, niezbędne są dwa elementy: materialny i formalny. Element materialny określa art. 1 ust. 1 tej ustawy, wskazujący na możliwość powstania określonej szkody, czy zagrożeniu dóbr. Element formalny wyraża się w nadanej klauzuli tajności. Jednocześnie, zgodnie z art. 5 cyt. ustawy, klauzulę taką można nadać tylko informacjom niejawnym

przy tym pamiętać, że przepisy u.o.i.n. powinny być „interpretowane w sposób wysoce restrykcyjny; ich wykładnia powinna zmierzać w kierunku zawężającym, a nigdy w kierunku rozszerzającym”[65].

2.2. Podstawowe zagadnienia dotyczące tajemnic prawnie chronionych

2.2.1. Pojęcie tajemnicy i jej rodzaje

Zgodnie z definicją zawartą w *Słowniku języka polskiego* **tajemnica** oznacza:

1) „«sekret; też: nieujawnianie czegoś»
2) «wiadomość, której poznanie lub ujawnienie jest zakazane przez prawo»
3) «rzecz, której się nie rozumie lub nie umie wyjaśnić»
4) «najlepszy lub jedyny sposób na osiągnięcie czegoś»”[66].

Pomimo różnych określeń tego terminu nie ulega wątpliwości, że to zaprezentowane jako drugie jest najbardziej właściwe z prawnego punktu widzenia. Należy jednak zauważyć, że na gruncie polskiego ustawodawstwa wyróżnia się następujące **rodzaje tajemnic**:

– tajemnice zawodowe,
– tajemnice prawnie chronione/tajemnice ustawowo chronione,

---

w znaczeniu materialnym. W ocenie WSA w Warszawie wskazać należy przy tym, że również w dotychczasowym orzecznictwie sądowoadministracyjnym przyjmuje się zgodnie, iż informacja niejawna chroniona jest bez względu na to, czy osoba uprawniona uznała za stosowne oznaczyć ją odpowiednią klauzulą, albowiem informacja jest niejawna z uwagi na zagrożenia wynikające z jej treści, a nie w wyniku klasyfikacji (zob. m.in. wyrok NSA z dnia 21 września 2012 r., I OSK 1393/12; podobnie: wyrok NSA z dnia 18 sierpnia 2015 r., I OSK 1679/14, orzeczenia.nsa.gov.pl)”.

[65] Wyrok WSA w Warszawie z dnia 27 kwietnia 2020 r., II SA/Wa 2543/19.

[66] *Słownik języka polskiego PWN*, hasło: *tajemnica*, https://sjp.pwn.pl/sjp/tajemnica;2528548.html [dostęp: 24.06.2025].

bez jakiegokolwiek ich zdefiniowania. Brak definicji legalnej tych terminów sprawia, że osoby zajmujące się tą problematyką we właściwy sobie sposób dokonują ich interpretacji. Mając powyższe na względzie, „wydaje się, że najszerszym pojęciem jest odwołanie się do zwrotu **«tajemnica prawnie chroniona»**. W istocie oznacza bowiem konieczność uwzględnienia w sferze funkcjonowania konkretnego organu (instytucji), funkcjonariusza publicznego lub osoby wykonującej wskazany zawód wszystkich prawnie zdefiniowanych tajemnic, a więc tych, które mają charakter powszechny (np. ochrona danych osobowych, czy jeszcze szerzej prywatności), jak również tych, które objęte zostają tajemnicą na podstawie odrębnych przepisów ustawowych w oparciu o przesłanki specyficzne, które mogą bezpośrednio nie odnosić się do aktualnego dysponenta tejże informacji (jej źródeł). W praktyce okazuje się, że obowiązek ochrony informacji może wiązać się z koniecznością ochrony takich danych, które przez ustawodawcę traktowane są jako informacje:

- objęte tajemnicą,
- niejawne,
- konfidencjonalne,
- poufne,
- służbowe,
- chronione jako prywatne”[67].

Przykładem tajemnicy prawnie chronionej jest tajemnica skarbowa, tajemnica statystyczna. Zdecydowanie węższe ujęcie należy przypisać **tajemnicy zawodowej**, przez którą „rozumie się spoczywający na konkretnej osobie obowiązek ochrony przed nieuprawnionym dostępem przez osoby (podmioty) trzecie określonych przedmiotowo (indywidualnie, rodzajowo bądź kompleksowo) informacji pozyskanych lub wytworzonych w związku z wykonywaniem przez tę osobę zawodem (służbą i czynnościami, które w jej

[67] M. Jabłoński, J. Węgrzyn, *Ochrona tajemnic…*, s. 92.

ramach są podejmowane). Podkreśla się przy tym jednocześnie, że cechą charakterystyczną takiego zawodu/służby (a tym samym tajemnicy zawodowej) jest ochrona zaufania, co do osoby zawód taki wykonującej, której powierza się (dostarcza) konkretnych informacji i jej źródeł"[68]. W prezentowanym wyżej ujęciu tajemnicą zawodową jest m.in. tajemnica adwokacka, tajemnica radcowska, tajemnica prokuratorska, tajemnica sędziowska, tajemnica lekarska, tajemnica dziennikarska.

[68] *Ibidem*, s. 95.

Rozdział III

Aksjologia ochrony prywatności i danych osobowych

3.1. Pojęcie prywatności

Prywatność i ochrona danych osobowych to dwa pojęcia, które chociaż często stosowane są naprzemiennie i niezwykle do siebie zbliżone, posiadają odrębne katalogi normatywnych gwarancji. Prawo do prywatności prawdopodobnie po raz pierwszy zostało wspomniane już w Starym Testamencie, w pismach proroka Micheasza (4,4), który utożsamiał prawo człowieka do osobistego życia ze szczęściem każdego usadowionego przy swojej winnicy i pod drzewem figowym, gdzie nikt nie będzie mu zakłócał spokoju[69]. Judaizm nie jest jednak jedyną religią, która rozpoznała prawo do prywatności. Ramajana, jedna z najstarszych ksiąg hinduistycznych, również podkreśla wagę prywatności w życiu jednostki[70]. Także Koran, święta księga Islamu, wskazuje, że prywatność jednostki nie jest własnością publiczną i nikt nie ma prawa jej naruszać bez zgody jednostki[71].

---

[69] W. Szyszkowski, *Rozważania o prywatności*, [w:] L. Antonowicz *et al.* (red.), *Wybrane problemy prawa konstytucyjnego*, Lublin 1985, s. 187.

[70] V. Kumar Gupta, *The right to privacy in India: A comparative study with global implications*, „International Journal of Law, Justice and Jurisprudence" 2024, vol. 4(1), s. 242.

[71] M. Sherwani, *The Right to Privacy under International Law and Islamic Law: A Comparative Legal Analysis*, „Kardan Journal of Social Sciences and Humanities" 2018, vol. 1, iss. 1, s. 35.

Bardziej nam współczesna definicja prywatności została opracowana przez sędziego T. Cooleya, który w swojej praktyce orzeczniczej wskazywał, że prawo do prywatności to prawo jednostki do całkowitej niezależności, prawo do bycia pozostawionym samemu sobie (*right to be let alone*)[72]. Twórca tej koncepcji rozpatrywał ją jedynie w ogólny sposób, w kontekście dóbr osobistych oraz w przypadku czynów karalnych, takich jak napaść i pobicie[73]. T. Cooley nie rozwinął ani nie rozpromował w sposób dostateczny tej koncepcji – wskazuje się, że popularność zyskała ona dzięki pracom S.D. Warrena i L.D. Brandeisa, którzy w swoich opracowaniach zgodnie podkreślali, że to właśnie Cooley był autorem koncepcji prawa do prywatności jako *right to be let alone*.

Po II wojnie światowej dyskusja na temat prywatności i praw podmiotowych z nią związanych rozgorzała na nowo z niespotykaną wcześniej siłą. Wskazywano, że **rozwój nowych technologii komputerowych jest głównym zagrożeniem dla prywatności jednostki**[74]. W latach 60. XX w. sformułowana została nowa definicja prywatności jako „roszczenie osób, grup lub instytucji do samodzielnego zadecydowania: kiedy, jak i w jakim zakresie informacje o nich są przekazywane innym"[75]. Jej autor, A. Westin, uważał, że **prywatność to dobrowolne i tymczasowe wycofanie się jednostki z ogółu społeczeństwa** za pomocą środków fizycznych

[72] T. Cooley, *A Treatise On The Law Of Torts*, 1st ed., Callaghan & Company 1880.

[73] G.B. Cope, Jr., *Toward a Right of Privacy as a Matter of State Constitutional Law*, „Florida State University Law Review" 1977, vol. 5, iss. 4, s. 647.

[74] J. Holvast, *History of Privacy*, http://opendl.ifip-tc6.org/db/conf/ifip9-6/fidis2008/Holvast08.pdf [dostęp: 24.06.2025].

[75] A.F. Westin, *Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part I, The Current Impact of Surveillance on Privacy, Disclosure, and Surveillance*, „Columbia Law Review" 1966, vol. 66, s. 1003–1050; A.F. Westin, *Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part II, Balancing the Conflicting demands of Privacy, Disclosure, and Surveillance*, „Columbia Law Review" 1966, vol. 66, s. 1205–1253; *idem*, *Privacy & Freedom*, London–Sydney–Toronto 1967.

lub psychologicznych poprzez stan samotności bądź uczestnictwo w niewielkich gwarantujących intymność grupach lub gdy jednostka fizycznie przebywa w dużej grupie, w której może zachować anonimowość i dystans.

Współcześnie stworzenie uniwersalnej definicji prywatności lub prawa do prywatności wydaje się być niemożliwe. Zauważają to nie tylko przedstawiciele polskiej doktryny („dokładne ustalenie zakresu prywatności jest uważane za niewykonalne”[76]), ale również międzynarodowe organy sądownicze („pojęcie «życia prywatnego» jest pojęciem szerokim, niepodatnym na wyczerpujące definicje”[77]). Prawo do ochrony życia prywatnego łączy w sobie wiele koncepcji, a pojęcie prywatności ma wiele znaczeń[78]. Rozwój Internetu, a szczególnie social mediów miał ogromny wpływ na to, w jaki sposób jednostki i społeczeństwo rozumieją prawo. Chociaż narzędzia te w znaczny sposób zmieniły (ułatwiły) funkcjonowanie w globalnym społeczeństwie, niosą one również określone zagrożenia, takie jak np. wykorzystywanie danych osobowych do targetowania jednostek przez bigtechy, tworzenie baniek informacyjnych[79], *deepfakes*, pola-

[76] J. Panowicz-Lipska, [w:] M. Gutowski (red.), *Kodeks cywilny*, t. I: *Komentarz. Art. 1–449[11]*, Warszawa 2016, s. 122; zob. również: J. Sobczak, *Prawo do prywatności, wolność słowa i druku*, [w:] L. Wiśniewski (red.), *Wolności i prawa jednostki oraz ich gwarancje w praktyce*, Warszawa 2006, s. 152.

[77] Europejski Trybunał Praw Człowieka podkreślił ten fakt w ponad 30 wyrokach, m.in. w: wyroku ETPCz z dnia 12 czerwca 2003 r. w sprawie *Van Kuck przeciwko Niemcom*, skarga nr 35968/04; wyroku z dnia 4 grudnia 2008 r. w sprawie *S. i Marper przeciwko Wielkiej Brytanii*, skarga nr 30562/04 i 30566/04; wyroku z dnia 12 stycznia 2010 r. w sprawie *Gillan i Quinton przeciwko Wielkiej Brytanii*, skarga nr 4158/05 i in.

[78] I. Dobosz, *Tajemnica korespondencji jako dobro osobiste i jej ochrona w prawie cywilnym*, Kraków 1989, s. 59.

[79] Bańka filtrująca lub inaczej bańka informacyjna to pojęcie stworzone przez E. Parisela i po raz pierwszy opisane w książce *The Filter Bubble: What the Internet Is Hiding from You* (Viking, 2011). Ukazuje on, jak odpowiednie algorytmy Facebooka i Google’a odcinają nas od informacji, które mogłyby być niezgodne z naszym punktem widzenia. Stworzenie bańki informacyjnej wiąże się z pierwotnym zebraniem

ryzację społeczeństwa, wykorzystywanie nieletnich i osób podatnych na manipulację. Ostatnie lata pokazują, że nawet tak duże i silne organizacje, jak Unia Europejska, nie są w stanie w pełni poradzić sobie z wyzwaniami, jakie przed nimi stawia sztuczna inteligencja i social media. Narzędzia te ułatwiają życie jednostki, prowadzenie działalności gospodarczej, zrzeszanie się w społecznościach czy wyrażanie swoich poglądów. Rozwój Internetu doprowadził również do zatarcia się różnicy pomiędzy tym, co publiczne, a tym, co prywatne, i w związku z tym zmienił paradygmat pojęcia prywatności. Nie ulega jednak wątpliwości, że prywatność jest dobrem, które należy chronić niezależnie od systemu politycznego obowiązującego w państwie, klimatu gospodarczego czy aktywności poszczególnych jednostek.

3.2. Ochrona prywatności i ochrona danych osobowych w uniwersalnym systemie ochrony praw człowieka

Podstawowym aktem o charakterze międzynarodowym, który w najszerszym zakresie przyznaje jednostce prawo do prywatności, jest Powszechna Deklaracja Praw Człowieka (PDPC). Zakłada ona, że nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe ani w jego korespondencję, ani też uwłaczać jego

dużej ilości danych na temat preferencji użytkownika, odwiedzanych przez niego stron internetowych, reakcji na pojawiające się w sieci informacje. Algorytmy zbudowane są w taki sposób, aby prezentować użytkownikowi jedynie takie treści, które wywołują u niego pozytywne reakcje, budować poczucie bezpieczeństwa i przynależności do określonej grupy społecznej. Powoduje to u użytkownika przekonanie, że z jego poglądami utożsamia się większość społeczeństwa, ogranicza jego dostęp do nowych informacji i oznacza jego zamknięcie się na czynniki zewnętrzne; zob. M. Klimowicz, *Przekłuj swoją bańkę*, „Magazyn opinii Pismo", 3.09.2019, https://magazynpismo.pl/przekluj-swoja-banke/?fbclid=IwAR0wwvqEveYnmZ99YSxOMVAHkQijaQcE0OE-QbheUjn8TMTAX_FALSfPOZU [dostęp: 24.06.2025].

honorowi lub dobremu imieniu. Zgodnie z brzmieniem art. 12 PDPC każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu. W PDPC nie ma powszechnie przyjętej i akceptowalnej definicji pojęcia prywatności lub życia prywatnego. Jednocześnie w trakcie prac nad przyjęciem oficjalnego tekstu Deklaracji ścierały się różne teorie na temat tego, jakie wartości w sferze prawa do prywatności PDPC powinna chronić[80].

Praktycznie od chwili powstania PDPC, z uwagi na jej pierwotnie niewiążący charakter[81], rozważano przyjęcie na szczeblu międzynarodowym dokumentu, co do którego obowiązywania nie byłoby wątpliwości. Takim dokumentem stał się Międzynarodowy Pakt Praw Obywatelskich i Politycznych. Postanowienia w nim zawarte w zakresie prawa do prywatności są niemal identyczne jak te w PDPC.

Państwa-strony Międzynarodowego Paktu Praw Obywatelskich i Politycznych na gruncie art. 17 są zobowiązane do powstrzymania się przed samowolną lub bezprawną ingerencją w życie prywatne jednostki, jej dom, korespondencję, a także przed bezprawnymi zamachami na jej cześć i dobre imię, oraz są zobowiązane do ochrony tych wartości. Komitet Praw Człowieka wskazuje, że ochrona powinna być zagwarantowana zarówno przed atakami ze strony

---

[80] O. Diggelmann, M.N. Cleis, *How the Right to Privacy Become a Human Right*, „Human Rights Law Review" 2014, vol. 14, iss. 3, s. 441–458, https://doi.org/10.1093/hrlr/ngu014 [dostęp: 24.06.2025].

[81] Co do zasady deklaracja nie ma charakteru wiążącego, ponieważ nie stanowi ona umowy międzynarodowej. Utrudnione zatem było dochodzenie na jej podstawie roszczeń związanych z ochroną praw i wolności. Jednocześnie w doktrynie praw człowieka funkcjonuje pogląd, zgodnie z którym Deklaracja stanowi przykład zwyczaju międzynarodowego z uwagi na wykształcenie się długotrwałej praktyki państw w tym zakresie (*usus*) oraz przekonanie o zgodności z prawem (*opinio iuris vel necessitas*). Więcej o zwyczaju międzynarodowym zob. W. Czapliński, A. Wyrozumska, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 2014, s. 102; R. Bierzanek, J. Symonides, *Prawo międzynarodowe publiczne*, Warszawa 2005, s. 106–109; M. Suploveda *et al.*, *Human rights reference handbook*, Costa Rica 2004, s. 23–24.

organów państwowych, jak i podmiotów prywatnych[82]. Komitet Praw Człowieka generalnie odgrywa dużą rolę w zakresie interpretowania elementów składowych prawa do prywatności, jak również obowiązków spoczywających na państwie oraz możliwości legalnej ingerencji w to prawo. Wydane przez Komitet wytyczne i decyzje stanowią dobrą bazę do podjęcia próby sprecyzowania granic prawa do prywatności w systemie uniwersalnej ochrony praw człowieka.

Katalog wymieniony w art. 17 MPPOiP nie jest katalogiem zamkniętym, a Komitet Praw Człowieka wielokrotnie interpretował zakres ochrony w sposób rozszerzający. W sprawie *Coeriel i Aurik przeciwko Holandii* stwierdził, że **pojęcie prywatności odnosi się do sfery życia człowieka, w której może on swobodnie wyrażać swoją tożsamość zarówno przez wchodzenie w relacje z innymi, jak i samodzielnie**[83]. Oznacza to, że ochrona prywatności w rozumieniu Paktu nie ogranicza się jedynie do ochrony strefy autonomii czy intymności jednostki, ale **odnosi się również do swobody kształtowania relacji jednostki z innymi członkami społeczeństwa**[84]. Takie podejście związane jest z szeroko pojętą **autonomią informacyjną jednostki, jej prawem do samodzielnego decydowania o tym, jakie informacje chce przekazywać poszczególnym kręgom odbiorców**. Na marginesie można zaznaczyć, że również Naczelny Sąd Administracyjny w ostatnim czasie wskazuje, że autonomia informacyjna jednostki powinna być rozumiana w sposób szeroki[85].

---

[82] Komitet Praw Człowieka ONZ, *Komentarz Generalny nr 16*, 8.04.1998, https://www.refworld.org/docid/453883f922.html [dostęp: 24.06.2025].

[83] Decyzja Komitetu Praw Człowieka z 31 października 1994 r. w sprawie *Coeriel i Aurik p. Holandii*, nr 453/1991.

[84] A. Gliszczyńska-Grabias, K. Sękowska-Kozłowska, *Komentarz do art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych*, [w:] R. Wieruszowski (red.), *Międzynarodowy Pakt Praw Obywatelskich i Politycznych. Komentarz*, Warszawa 2012, s. 373.

[85] Wyrok NSA z dnia 10 października 2024 r., III OSK 4804/21.

Podobnie jak w przypadku wielu innych praw i wolności, ochrona prywatności na gruncie art. 17 MPPOiP **nie ma charakteru absolutnego, jednak ingerencja w prywatność jednostki nie może być arbitralna lub bezprawna**[86]. Komentowany przepis nie zawiera jednak w sobie ani definicji, ani przykładowego katalogu zachowań uznawanych za arbitralne lub bezprawne. Komitet Praw Człowieka w Komentarzu Generalnym nr 16 wskazał, że „bezprawna ingerencja" oznacza, iż „żadna ingerencja nie może mieć miejsca za wyjątkiem przypadków przewidzianych przez prawo. Ingerencja, do której upoważnione jest państwo, może nastąpić tylko na podstawie prawa, które musi być zgodne z postanowieniami, celami i zasadami Paktu"[87]. Z kolei „arbitralna ingerencja" to taka, która jest „dokonywana na podstawie prawa. Wprowadzenie koncepcji arbitralności ma na celu zagwarantowanie, że nawet interwencja dokonywana na podstawie prawa powinna następować w zgodzie z celami i zasadami Paktu i powinna w każdym przypadku znajdować uzasadnienie w danych okolicznościach"[88].

Każdorazowo ingerencja w prywatność powinna być proporcjonalna, biorąc pod uwagę aspekty ilościowe i jakościowe działań podmiotów publicznych. W przypadku arbitralnej ingerencji często podkreśla się element „kapryśności" i bada, czy dana ingerencja (chociażby zgodna z prawem) zawierała elementy „niesprawiedliwości, nieprzewidywalności i nieracjonalności"[89]. Ograniczenia dopuszczalnej na gruncie art. 17 MPPOiP ingerencji w prawo do prywatności mają na celu powstrzymanie podmiotów publicznych przed nadużywaniem dyskrecjonalnej władzy przyznanej przez prawo lub manipulacją procedurami prawnymi.

---

[86] Komitet Praw Człowieka ONZ, *Komentarz Generalny nr 16…*

[87] *Ibidem*.

[88] *Ibidem*.

[89] M. Nowak, *U.N. Covenant on Civil and Political Rights, CCPR Commentary*, Kehl–Strassburg–Arlington 2005, s. 382–383.

Komentarz Generalny nr 16 zawiera również trafne spostrzeżenia związane z pozyskiwaniem i przechowywaniem danych osobowych, wskazując, że obowiązki państw-stron na gruncie art. 17 obejmują również **przyjęcie regulacji prawnych wzmacniających ochronę jednostki przed nadmiernym przetwarzaniem danych osobowych**. Przyjęte prawo powinno zawierać skuteczne środki zapewniające, że informacje dotyczące życia prywatnego jednostki nie zostaną udostępnione podmiotom nieuprawnionym i nie będą wykorzystywane do celów niezgodnych z MPPOiP. Zdaniem Komitetu Praw Człowieka skuteczna ochrona wymaga wyposażenia jednostki w uprawnienia związane z uzyskiwaniem informacji (które powinny być przekazane w zrozumiałej formie) na temat sposobu przetwarzania danych oraz żądaniem ich usunięcia w określonych przypadkach.

Komitet Praw Człowieka wielokrotnie zwracał również uwagę na fakt, że **współcześnie to państwa-strony gromadzą więcej danych osobowych, niż jest to konieczne w demokratycznym społeczeństwie**. Podkreśla się, iż dane na temat nieletnich powinny być zbierane przez państwo w szczególnie uzasadnionych przypadkach[90], jak również wskazuje na konieczność istnienia niezależnego organu nadzorczego, który powinien kontrolować i nadzorować sposób i zakres danych zbieranych przez organy władzy publicznej, dając gwarancję bezstronności i skuteczności[91]. W tym kontekście warto również wspomnieć, że zdaniem Komitetu Praw Człowieka państwa-strony nie powinny w nadmierny sposób gromadzić da-

[90] Uwagi końcowe do sprawozdania Francji z 2008 r., CCPR/C/FRA/CO/4, pkt 22.

[91] Na marginesie można wskazać, że te same wymagania stawiane są organom nadzorczym na gruncie RODO, jednocześnie obowiązek powołania takiego organu wynika wprost z obowiązujących przepisów prawa Unii Europejskiej, podczas gdy w przypadku MPPOiP obowiązek ten nie wynika z treści Paktu, ale z praktyki Komitetu Praw Człowieka. Zob. uwagi końcowe do sprawozdania Szwecji z 2009 r., CCPR/C/SWE/CO/6, pkt 18.

nych biometrycznych czy danych DNA, szczególnie biorąc pod uwagę poważne konsekwencje dla prawa do prywatności zagwarantowanego przez art. 17 MPPOiP[92].

W systemie uniwersalnej ochrony praw jednostki obok Komitetu Praw Człowieka ustanowiono również Specjalnego Sprawozdawcę ds. prawa do prywatności, którego jednym z głównych zadań jest ochrona prywatności w erze cyfrowej. Specjalny Sprawozdawca opracowuje wytyczne związane z ochroną prawa do prywatności w zmieniających się warunkach cyfrowych, w tym np. w kontekście sztucznej inteligencji.

W 2018 r. Wysoki Komisarz ONZ do spraw Praw Człowieka udostępnił raport na temat prywatności w cyfrowym świecie[93]. Zdaniem autorów raportu pojęcie prywatności należy rozumieć jako domniemanie, że jednostka powinna posiadać obszar autonomicznego rozwoju, interakcji i wolności, „sferę prywatną", w której dopuszcza się bądź nie kontakt z innymi, wolną od ingerencji państwa i od nadmiernej, nieproszonej ingerencji ze strony niezachęcanych do niej podmiotów prywatnych[94]. Zgodnie z raportem **w sferze cyfrowej szczególną wagę odgrywa prywatność informacyjna, czyli dotycząca informacji, która bądź to istnieje w Internecie, bądź pochodzi z dostępnych publiczne informacji na temat danej osoby**[95]. Ochronie podlegają również metadane, biorąc pod uwagę, że po ich zebraniu i przeanalizowaniu odbiorca może

[92] Badania DNA, zdaniem Komitetu, powinny być wykonywane tylko wtedy, kiedy jest to stosowne i konieczne dla określenie więzów rodzinnych, od których zależy udzielenie jednostce konkretnego uprawnienia (np. zezwolenia na pobyt), zob. CCPR/C/SWE/CO/6, pkt 18; uwagi końcowe do sprawozdania Kanady z 1999 r., A/54/50 v. I, pkt 238; Uwagi końcowe do sprawozdania Danii z 2001 r., A/56/49 v. II, pkt 16.

[93] Raport Wysokiego Komisarza ONZ ds. Praw Człowieka z 3 sierpnia 2018 r. „Prawo do prywatności w świecie cyfrowym", A/HRC/39/29.

[94] *Ibidem*.

[95] *Ibidem*.

uzyskać informacje na temat zachowania, relacji społecznych, preferencji jednostki w o wiele szerszym kontekście, niż gdyby przeanalizował jedynie treść informacji przekazywanych bezpośrednio przez jednostkę[96]. Wskazuje się również, że ochrona prywatności nie jest ograniczona tylko to wyodrębnionych, „prywatnych" sfer, takich jak dom czy mieszkanie, ale rozszerza się również na sferę publiczną i informacje publicznie dostępne, np. w przypadku stosowania monitoringu wizyjnego[97]. Również w przypadku udostępnienia informacji w mediach społecznościowych może dojść do ingerencji w prawo do prywatności jednostki[98]. Zdaniem autorów raportu **do ingerencji w prywatność dochodzi zawsze, gdy jednostka traci kontrolę nad zakresem i ilością informacji jej dotyczących, które są przetwarzane przez podmioty trzecie**[99]. W przypadku podmiotów prywatnych za główne zagrożenia uznano: zbieranie „cyfrowych śladów", przekazywanie danych pomiędzy podmiotami skupionymi w grupach kapitałowych i w przypadku przejęć i fuzji, zbieranie danych biometrycznych czy rosnące możliwości analizy danych[100]. W przypadku ingerencji ze strony podmiotów publicznych w raporcie wymienia się takie naruszenia, jak: masowa inwigilacja, udostępnianie danych zebranych przez podmioty publiczne podmiotom prywatnym, ataki hakerskie, próby osłabienia zabezpieczeń stosowanych przez dostawców usług skierowanych do podmiotów prywatnych czy transgraniczne przekazywanie danych[101].

Chociaż uniwersalny system praw człowieka tradycyjnie uznawany jest za trzon gwarancji przyznawanych każdej jednostce, co-

[96] *Ibidem*.
[97] *Ibidem*.
[98] *Ibidem*.
[99] *Ibidem*.
[100] *Ibidem*.
[101] *Ibidem*.

raz częściej oceniany jest on jako nieefektywny. Dużo większą rolę w tym zakresie odgrywają gwarancje zawarte w regionalnych systemach ochrony praw człowieka, takich jak np. Rada Europy.

3.3. Ochrona danych osobowych w Radzie Europy

3.3.1. Europejska Konwencja Praw Człowieka

Europejska Konwencja o ochronie praw człowieka i podstawowych wolności w art. 8 przyznaje każdemu prawo do ochrony prywatności, w tym nienaruszalności mieszkania i tajemnicy korespondencji. Podobnie jak w przypadku MPPOiP regulacja zawarta w Konwencji jest dosyć skąpa, a ogromną rolę w odczytywaniu treści prawa do prywatności odegrał Europejski Trybunał Praw Człowieka. Prawo do prywatności w systemie Rady Europy nie ma charakteru absolutnego. Już w ust. 2 art. 8 EKPC zawarto klauzulę limitacyjną, która zakreśla ramy dopuszczalnej ingerencji państwa w prawo jednostki. Zgodnie z jej treścią **niedopuszczalna jest ingerencja władzy publicznej w korzystanie z prawa do prywatności z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób**. Wynika z tego, że ingerencja w prawo do prywatności, która wprost jest przewidziana w ustawie i która jest konieczna w demokratycznym społeczeństwie dla ochrony celów przewidzianych w ust. 2 art. 8 EKPC, jest dopuszczalna.

Zgodnie z art. 8 Konwencji każdy ma prawo do ochrony ze strony państwa swojego życia prywatnego i rodzinnego, mieszkania i korespondencji. Pojęcia użyte w EKPC mają szeroki i wymykający się defini-

cjom charakter, zatem Trybunał każdorazowo orzeka o ich znaczeniu, biorąc pod uwagę okoliczności konkretnej sprawy[102]. Prawo do prywatności w myśl Konwencji obejmuje nie tylko prawo do życia w sposób zgodny z własnym sumieniem i prawo do bycia pozostawionym samemu sobie, ale również prawo do nawiązywania i utrzymywania stosunków z innymi w celu rozwoju własnej osobowości, jak również prawo do autonomii indywidualnej[103]. Europejski Trybunał Praw Człowieka uważa, że, podobnie jak w przypadku MPPOiP, prywatność jednostki powinna być również chroniona w sferze publicznej, np. w zawodowej aktywności jednostki[104], a prawo do ochrony prywatności przysługuje wszystkim osobom, nawet tym publicznie znanym[105].

Trybunał wielokrotnie rozstrzygał w sprawach związanych z negatywnym obowiązkiem państw-stron Konwencji powstrzymania się od ingerencji w prywatność jednostki poza zakresem dopuszczalnym w art. 8 ust. 2 EKPC. Podkreślano, że akt normatywny umożliwiający ingerencję w prawa jednostki na gruncie porządku prawnego państwa-sygnatariusza Konwencji powinien określać w sposób ścisły zakres i granicę ewentualnej ingerencji, precyzując nie tylko sposoby ingerencji, ale również czas jej trwania oraz przesłanki ją umożliwiające[106] (i warunkujące jej zaprzestanie[107])

---

[102] Wyrok ETPCz z dnia 25 marca 1993 r. w sprawie *Costello-Roberts p. Wielkiej Brytanii*, skarga nr 13134/87.

[103] Wyrok ETPCz z dnia 24 lutego 1998 r. w sprawie *Botta p. Włochom*, skarga nr 32647/96; wyrok ETPCz z dnia 6 lutego 2001 r. w sprawie *Bensaid p. Wielkiej Brytanii*, skarga nr 44599/98.

[104] Wyrok ETPCz z dnia 28 listopada 2017 r. w sprawie *Antović i Mirković p. Czarnogórze*, skarga nr 70838/13.

[105] Wyrok ETPCz z dnia 24 czerwca 2004 r. w sprawie *Caroline von Hannover p. Niemcom*, skarga nr 59320/00.

[106] Wyrok ETPCz z dnia 24 kwietnia 1990 r. w sprawie *Kruslin p. Francji*, skarga nr 11801/85; wyrok ETPCz z dnia 25 marca 1998 r. w sprawie *Kopp p. Szwajcarii*, skarga nr 23224/94; wyrok ETPCz z dnia 16 lutego 2000 r. w sprawie *Amann p. Szwajcarii*, skarga nr 27798/95.

[107] Wyrok ETPCz z dnia 4 grudnia 2005 r. w sprawie *Roman Zakharov p. Rosji*, skarga nr 47143/06.

oraz zakres swobodnego uznania organu dopuszczającego się ingerencji[108].

Prawo krajowe powinno w sposób enumeratywny wskazywać, jakie środki mogą podjąć jego organy, ingerując w prawo do prywatności jednostki, włączając w to informacje, czy do ingerencji może dochodzić np. poprzez wykorzystywanie narzędzi geolokalizacyjnych, odczytywanie wiadomości SMS, kontrolę korespondencji (również elektronicznej poszkodowanego), czy stosując inne, bardziej tradycyjne formy nadzoru[109]. Ponadto prawo państwa członkowskiego powinno określać, jakie dane mogą być przetwarzane przez jego organy, ze szczególnym uwzględnieniem warunków przetwarzania danych wrażliwych, takich jak np. informacje dotyczące zdrowia[110]. Kluczowe jest, aby ustawodawca najpierw określił, czy zbierane dane w jakikolwiek sposób są istotne dla osiągnięcia założonego celu[111].

Chociaż art. 8 EKPC nie odnosi się w sposób bezpośredni do uprawnień jednostki związanych z ochroną danych osobowych i dostępem do niej, to już bogate orzecznictwo Europejskiego Trybunału Praw Człowieka w sposób jednolity wskazuje na określone uprawnienia i obowiązki związane z przetwarzaniem danych osobowych. Trybunał stoi na stanowisku, że **chociaż prawo do ochrony danych osobowych wpisuje się w prawo do prywatności określone w art. 8 EKPC, każdorazowo należy zbadać, czy dane informacje o jednostce, przetwarzane przez państwo, dotyczą rzeczywiście prywatnej sfery życia jednostki**[112]. W dotychczasowym orzecznic-

---

[108] Wyrok ETPCz z dnia 22 grudnia 2005 r. w sprawie *Wisse p. Francji*, skarga nr 71611/01.

[109] Wyrok ETPCz z dnia 8 lutego 2018 w sprawie *Ben Faiza p. Francji*, skarga nr 31446/12; wyrok ETPCz z dnia 22 października 2002 r. w sprawie *Taylor-Sabori p. Wielkiej Brytanii*, skarga nr 47114/99.

[110] Wyrok ETPCz z dnia 29 kwietnia 2014 w sprawie *L.H. p. Łotwie*, skarga nr 52019/07.

[111] Skarga nr 52019/07.

[112] Skarga nr 30562/04.

twie za dane osobowe uznano m.in. dane pozyskane przy użyciu narzędzi geolokalizacyjnych, adres IP[113], informacje pozyskane z bilingów telefonicznych czy monitoringu poczty e-mail[114], próbki DNA[115], nagranie głosu[116].

Orzecznictwo Trybunału dotyczące przetwarzania danych osobowych wskazuje m.in., że potrzeba odpowiedniej ochrony danych jest większa szczególnie w przypadkach, gdy przetwarzanie prowadzi do zautomatyzowanego podejmowania decyzji, zwłaszcza jeśli dochodzi do tego w sferze odpowiedzialności karnej[117]. Osoba, której dane dotyczą, na gruncie art. 8 EKPC ma prawo do sprzeciwu przeciwko przetwarzaniu danych nieprawidłowych bądź nieprawdziwych[118], jak również, z pewnymi wyjątkami, prawo żądania zaprzestania przetwarzania i usunięcia danych (również gdy przetwarzane dane są prawidłowe)[119].

Gdy prawo państwa-strony Konwencji nie przewiduje możliwości usunięcia danych bądź jego realizacja jest uzależniona od decyzji organu publicznego, należy dążyć do zapewnienia równowagi pomiędzy ochroną prywatności jednostki a uzasadnionym interesem publicznym[120]. Balans między tymi dwiema wartościami powinien

---

[113] Wyrok ETPCz z dnia 24 kwietnia 2018 r. w sprawie *Benedik p. Słowenii*, skarga nr 62357/14.

[114] Skarga nr 61496/08.

[115] Wyrok ETPCz z dnia 14 kwietnia 2020 r. w sprawie *Dragan Petrović p. Serbii*, skarga nr 75229/10.

[116] Wyrok ETPCz z dnia 25 września 2001 r. w sprawie *P.G. i J.H. p. Wielkiej Brytanii*, skarga nr 44787/98; wyrok ETPCz z dnia 31 maja 2005 r. w sprawie *Vetter p. Francji*, skarga nr 59842/00.

[117] Skarga nr 30562/04.

[118] Wyrok ETPCz z dnia 18 października 2011 r. w sprawie *Khelili p. Szwajcarii*, skarga nr 16188/07.

[119] Wyrok ETPCz z dnia 17 grudnia 2009 r. w sprawie *B.B. p. Francji*, skarga nr 5335/06; wyrok ETPCz z dnia 17 grudnia 2009 r. w sprawie *Gardel p. Francji* i *M.B. p. Francji*, skarga nr 22115/06.

[120] Wyrok ETPCz z dnia 18 kwietnia 2013 r. w sprawie *M.K. p. Francji*, skarga nr 19522/09; wyrok ETPCz z dnia 13 listopada 2012 r. w sprawie *M.M. p. Wielkiej*

być również wzięty pod uwagę przy ustalaniu maksymalnego dopuszczalnego terminu przetwarzania danych w określonym celu[121]. Jednocześnie w przypadku, gdy przetwarzanie nie służy nadal celowi, dla którego zostało pierwotnie rozpoczęte, państwo-strona EKPC powinno zaprzestać dalszych działań[122]. Ma to znaczenie zwłaszcza w przypadku przetwarzania danych o szczególnym charakterze, takich jak np. poglądy polityczne jednostki[123]. W kontekście danych wrażliwych Trybunał wskazywał, że przetwarzanie danych osobowych dotyczących zdrowia ma nie tylko wyjątkowe znaczenie dla prywatności, ale również dla wzmocnienia zaufania jednostki do opieki zdrowotnej (niezależnie czy finansowanej ze środków publicznych czy odbywającej się w sektorze prywatnym), w związku z czym państwo-strona Konwencji powinno stworzyć odpowiednie gwarancje zapobiegające nieuprawnionemu ujawnieniu rzeczonych danych osobowych[124]. Niezależnie od podstawy przetwarzania danych osobowych organy państwa powinny wdrożyć takie środki organizacyjno-techniczne, które zabezpieczą przetwarzane dane przed nieusprawiedliwionym ujawnieniem[125].

Analizując orzecznictwo Europejskiego Trybunału Praw Człowieka, można stwierdzić, że pomimo braku wyrażonych wprost gwarancji ochrony danych osobowych w art. 8 EKPC Konwencja w sposób skuteczny chroni zarówno prywatność, jak i prawo do ochrony danych

---

Brytanii, skarga nr 24029/07; wyrok ETPCz z dnia 22 czerwca 2017 r. w sprawie *Aycaguer p. Francji*, skarga nr 8806/12.

[121] Wyrok ETPCz z dnia 18 września 2014 r. w sprawie *Brunet p. Francji*, skarga nr 21010/10.

[122] Wyrok ETPCz z dnia 7 czerwca 2016 r. w sprawie *Karabeyoğlu p. Turcji*, skarga nr 26012/11.

[123] Wyrok ETPCz z dnia 24 stycznia 2019 r. w sprawie *Catt p. Wielkiej Brytanii*, skarga nr 43514/15.

[124] Skarga nr 22009/93.

[125] Wyrok ETPCz z dnia 27 sierpnia 1997 r. w sprawie *M.S. p. Szwecji*, skarga nr 20837/92; wyrok ETPCz z dnia 28 stycznia 2003 r. w sprawie *Peck p. Wielkiej Brytanii*, skarga nr 44647/98.

osobowych jednostki. Bez wątpienia orzecznictwo ETPCz jest spójne z poglądami przedstawianymi przez Trybunał Sprawiedliwości Unii Europejskiej, jak również pozostałe organy Unii Europejskiej.

3.3.2. Konwencja 108

Rozwój nowoczesnych technologii spowodował konieczność zrewidowania dotychczasowych poglądów na temat ochrony danych osobowych i prywatności. Doprowadziło to do uchwalenia przez państwa członkowskie Rady Europy w 1981 r. Konwencji o ochronie danych osobowych[126], a następnie zmodernizowanej Konwencji 108[127] w 2018 r., którą obecnie (marzec 2025) podpisało 46 państw[128].

Konwencja 108+ jest jedynym istniejącym traktatem międzynarodowym dotyczącym prawa jednostek do ochrony ich danych osobowych. Uzasadniając potrzebę zmodernizowania Konwencji 108, podkreślano, że chociaż wywarła ona znaczny wpływ na przetwarzanie danych osobowych w Europie i poza nią, konieczne jest wprowadzenie takich rozwiązań, które pozwolą lepiej chronić prawa podstawowe jednostki, szczególnie w świetle wyzwań związanych z rozwojem nowych technologii, globalizacją i przekazywaniem danych osobowych ponad granicami państw[129]. Wprowadzone zmiany mają na celu

---

[126] 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), dalej również „Konwencja 108".

[127] Ustawa z dnia 16 października 2019 r. o ratyfikacji Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonego w Strasburgu dnia 10 października 2018 r. (Dz. U. z 2019 r. poz. 2284), dalej również „Konwencja 108+".

[128] Chart of signatures and ratifications of Treaty 223, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223 [dostęp: 24.06.2025].

[129] Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series – No. 223, https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a [dostęp: 24.06.2025].

zachowanie neutralności technologicznej, ale również zapewnienie spójności z innymi aktami prawnymi Rady Europy. Otwarty charakter traktatu (mogą do niego przystąpić wszystkie państwa Rady Europy) ma sprzyjać stworzeniu uniwersalnego standardu ochrony. Jednocześnie treść Konwencji 108+ zachowuje generalny i abstrakcyjny charakter, co pozwala na wypracowanie szczegółowych rozwiązań w wybranych sektorach gospodarki, wymagających przetwarzania danych osobowych dla ich efektywnego funkcjonowania.

Konwencja 108 zobowiązuje państwa-strony do przyjęcia takich regulacji wewnętrznych, które zapewnią minimalny poziom harmonizacji prawa. Ma ona zastosowanie zarówno do przetwarzania danych osobowych w relacjach prywatnych, jak i publicznych i jest ograniczona jedynie do automatycznego przetwarzania danych. Konwencja 108 wprowadza szereg zasad, jakim muszą sprostać podmioty, które chcą przetwarzać dane osobowe, w tym pozyskiwanie danych tylko w sposób legalny, przetwarzanie jedynie dla określonych celów i nieużywanie w innych celach niż te, dla których zostały pierwotnie zebrane. Przetwarzana powinna być jedynie taka ilość danych, która jest niezbędna do wypełnienia określonych celów. Dane osobowe powinny być aktualne oraz przetwarzane w sposób, który umożliwi ich usunięcie, jeśli ich przetwarzanie nie będzie dłużej konieczne dla osiągnięcia wyznaczonych celów.

Rada Europy przyjęła również szereg regulacji i rekomendacji związanych z przetwarzaniem danych osobowych w konkretnych sektorach. Odnoszą się one do różnych dziedzin życia i rozwijają zasady wynikające z Konwencji 108 i 108+. Precyzują treść zasad ogólnych oraz wprowadzają dodatkowe warunki przetwarzania danych osobowych w działalności policji, relacjach pracowniczych, sektorze telekomunikacji i marketingu bezpośredniego[130]. Nie mają

[130] Zob. F. Boehm, *Information sharing and data protection in the area of freedom, security and justice. Towards harmonised data protection principles for informa-*

one jednak charakteru umowy międzynarodowej, są raczej zbiorem wytycznych uzgodnionych przez Komitet Ministrów Rady Europy.

Porozumienie zawarte pomiędzy Unią Europejską a Radą Europy zakłada, że przy pracach nad rozwojem praw podstawowych w Unii będzie ona odwoływać się do dorobku wypracowanego przez Radę Europy[131], zatem również do orzecznictwa ETPCz w za-

---

tion exchange at EU-level, Berlin–Heidelberg 2012, s. 92–106. Należą do nich m.in.: Rezolucja (73) 22 Komitetu Ministrów z dnia 26 września 1973 r. o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze prywatnym; Rekomendacja (83) 3 Komitetu Ministrów Rady Europy z dnia 22 lutego 1983 r. dotycząca ochrony użytkowników skomputeryzowanych usług informacji prawniczej; Rekomendacja (83) 10 Komitetu Ministrów dla Państw Członkowskich z dnia 23 września 1983 r. w sprawie ochrony danych osobowych gromadzonych i przetwarzanych dla celów badań naukowych i statystycznych; Rekomendacja (85) 20 Komitetu Ministrów dla Państw Członkowskich z dnia 23 stycznia 1986 r. w sprawie ochrony prywatności w Internecie, wytyczne w sprawie danych osobowych używanych dla celów zabezpieczeń społecznych; Rekomendacja (87) 15 Komitetu Ministrów Rady Europy z dnia 17 września 1987 r. o ochronie danych osobowych wykorzystywanych w sektorze Policji; Rekomendacja (89) 2 w sprawie ochrony danych osobowych wykorzystywanych w procesie zatrudnienia oraz memorandum wyjaśniające Komitetu Ministrów dla Państw Członkowskich z dnia 18 stycznia 1989 r. w sprawie ochrony danych osobowych wykorzystywanych dla potrzeb zatrudnienia; Rekomendacja (90) 19 i memorandum wyjaśniające Komitetu Ministrów dla Państw Członkowskich z dnia 13 września 1990 r. w sprawie ochrony danych osobowych wykorzystywanych do płatności i innych pokrewnych operacji; Rekomendacja (95) 4 wraz z memorandum wyjaśniającym z dnia 7 lutego 1995 r. dotycząca ochrony danych osobowych w dziedzinie usług telekomunikacyjnych ze szczególnym uwzględnieniem usług telefonicznych; Rekomendacja (81) 1 Komitetu Ministrów dla Państw Członkowskich z dnia 23 stycznia 1981 r. w sprawie regulacji mających zastosowanie do zautomatyzowania banków danych medycznych; Rekomendacja (84) 10 Komitetu Ministrów Rady Europy z dnia 21 czerwca 1984 r. w sprawie rejestrów karnych i rehabilitacji osób skazanych; Rekomendacja (89) 4 Komitetu Ministrów z dnia 6 marca 1989 r. w sprawie zbierania danych epidemiologicznych w ramach podstawowej opieki medycznej; Rekomendacja 9 (2002) Komitetu Ministrów dla Państw Członkowskich z dnia 18 września 2002 r. w sprawie ochrony danych osobowych gromadzonych i przetwarzanych dla celów ubezpieczeniowych. Zob. więcej: J. Sobczak, [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2013, s. 269–273.

[131] Porozumienie pomiędzy Radą Europy a Unią Europejską zawarte w dniu 10 maja 2007 r., CM (2007)74.

kresie odczytywania treści art. 8 Konwencji, jak i do postanowień Konwencji 108 i Konwencji 108+. Wynika z tego, że interpretacja przepisów RODO oraz innych unijnych aktów prawnych związanych z ochroną danych osobowych jednostki powinna odbywać się z uwzględnieniem Europejskiej Konwencji Praw Człowieka oraz działalności ETPCz. Prowadzi to również do wniosku, że interpretacje dokonywane w systemie Rady Europy oraz wysiłki podejmowane przez tę organizację na rzecz rozwoju praw podstawowych mają fundamentalny wpływ na dalszy rozwój praw i wolności jednostki.

3.4. Ochrona danych osobowych w Unii Europejskiej

3.4.1. Prawo pierwotne Unii Europejskiej

Dopiero w latach 90. XX w. kwestia ochrony danych osobowych zaczęła odgrywać donioślejszą rolę w pracach Wspólnoty Europejskiej. Doprowadziło to do ukształtowania regionalnego, niezależnego (choć silnie związanego z Radą Europy) systemu ochrony praw podstawowych, w tym również prawa do prywatności[132]. Początkowo prawo do prywatności czy ochrony danych osobowych nie pojawiało się w dokumentach traktatowych lub prawie wtórnym, jednak **wraz z ukształtowaniem się prawa pretoriańskiego ochrona prawa do prywatności coraz częściej stanowiła istotną część debaty publicznej**[133], aż do uznania jej przez Trybunał Sprawiedli-

[132] J. Sobczak, [w:] A. Wróbel (red.), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. 1, Warszawa 2012, s. 313; A. Gonschior, *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej*, [w:] D. Kornobis-Romanowska (red.), *Aktualne problemy prawa Unii Europejskiej i prawa międzynarodowego – aspekty teoretyczne i praktyczne*, Wrocław 2017, s. 241.

[133] M. Jabłoński, K. Wygoda, *Dostęp do informacji*…, s. 101.

wości Unii Europejskiej za część zasad ogólnych[134]. Koncepcja ta następnie była wielokrotnie rozwijana aż do kluczowego momentu dla rozwoju ochrony praw podstawowych, a zatem i prawa do prywatności – uznania praw zawartych w Karcie praw podstawowych na mocy art. 6 Traktatu o Unii Europejskiej (TUE) w wersji traktatu z Lizbony[135], kiedy to prawa podstawowe zostały usystematyzowane, a Karta praw podstawowych[136] zyskała taką samą moc prawną jak traktaty.

Artykuł 8 KPP zapewnia każdemu ochronę jego danych osobowych. **Dane te powinny być przetwarzane w sposób rzetelny, jedynie w określonych celach, za zgodą osoby, której dotyczą, lub na podstawie innych uzasadnionych podstaw prawnych**. Prawo do ochrony danych osobowych gwarantuje również prawo dostępu i sprostowania danych. Artykuł 8 KPP oparty jest przede wszystkim na treści art. 286 Traktatu ustanawiającego Wspólnotę Europejską[137] (obecnie art. 16 TFUE), na nieobowiązującej już dyrektywie 95/46/WE, art. 8 EKPC oraz Konwencji 108 jak również licznych konwencjach Rady Europy[138]. Artykułu 8 KPP nie można interpretować w oderwaniu od jej art. 7, przepis ten odnosi się bowiem do ochrony prywatności, pozostającej w ścisłym związku z ochroną danych osobowych. Według TSUE wspólna interpretacja art. 7 i art. 8 KPP prowadzi do uznania uprawnienia do ochrony „życia prywatnego w kontekście przetwarzania danych osobowych"[139].

---

[134] Wyrok TSUE z dnia 12 listopada 1969 r. *Erich Stauder przeciwko Stadt Ulm – Sozialamt*, sygn. 26–69; zob. również J. Braciak, *Prawo do prywatności*, Warszawa 2004, s. 103.

[135] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie dnia 13 grudnia 2007 r. (Dz. U. z 2009 r. Nr 203, poz. 1569), dalej: „Traktat z Lizbony".

[136] Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 326/02 z 26.10.2012 r.), dalej również: „KPP".

[137] Traktat ustanawiający Wspólnotę Europejską (wersja skonsolidowana 2006) (Dz. Urz. UE CE 321/1, 29.12.2006 r.).

[138] J. Sobczak, [w:] A. Wróbel (red.), *Karta Praw Podstawowych…*, s. 259.

[139] TSUE w wyrokach w sprawach połączonych C-92/09 i C-93/09 *Volker und Marcus Schecke GbR i Hartman Eifert*; na marginesie należy dodać, że zdaniem

Traktat o funkcjonowaniu Unii Europejskiej w art. 16 przyznaje każdej jednostce prawo do ochrony danych jej dotyczących. Biorąc pod uwagę dotychczasowy dorobek legislacyjny Unii Europejskiej, pojęcie „danych osobowych" należy rozumieć zgodnie z art. 4 ust. 1 RODO. Ochrona przyznana w art. 16 TFUE jest niemal odwzorowaniem art. 8 KPP. Norma prawna art. 16 TSUE ma skutek bezpośredni, co znaczy, że nawet przy braku regulacji niższego rzędu jednostka może się na nią powołać przed organami UE i państw członkowskich w przypadku bezprawnej ingerencji w jej prawo do ochrony danych osobowych[140]. Ustęp 2 powołanego przepisu wskazuje natomiast, że Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne UE oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa UE, a także zasady dotyczące swobodnego przepływu takich danych.

Ochrona przewidziana art. 16 TFUE ma zastosowanie zarówno w relacjach pomiędzy jednostką a organami Unii Europejskiej i państw członkowskich, jak również w stosunkach prywatnoprawnych[141]. Przede wszystkim zagwarantowanie realizacji prawa do prywatności w pierwszej kolejności spoczywa w rękach krajowych organów stosujących prawo; dopiero gdy nie mogą samodzielnie zagwarantować odpowiedniego stosowania, wkracza TSUE. Nałożony na Komisję Europejską wymóg przyjęcia odpowied-

---

TSUE wykładnia przepisów konstytucyjnych państw członkowskich, która byłaby sprzeczna z treścią art. 8 EKPCz, stanowi naruszenie prawa wspólnotowego UE, wyrok TSUE z dnia 20 maja 2003 r. w sprawach połączonych C-465/00, C-138/01 i C-139/01.

[140] J. Sobczak [w:] A. Wróbel (red.), *Traktat…*, s. 329.

[141] M. Kawecki, T. Osiej, *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa 2017, s. 2; A. Grzelak, *Projekt reformy ochrony danych osobowych – czy rzeczywiście powstaje jednolity i spójny system?*, „Kwartalnik Kolegium Ekonomiczno-Społecznego «Studia i Prace»" 2014, nr 4, s. 95.

niej regulacji nie wyklucza podjęcia przez państwa członkowskie określonych kroków legislacyjnych, tak jak miało to miejsce w okresie obowiązywania dyrektywy 95/46/WE. To właśnie państwa członkowskie są przede wszystkim odpowiedzialne za ustanowienie niezależnych organów nadzoru, które w pierwszej kolejności reagują na zgłoszenia osób fizycznych w zakresie naruszenia bądź ryzyka naruszenia ich prawa do prywatności, podejmują zadania kontrolno-nadzorcze oraz prowadzą działania edukacyjne[142].

3.4.2. Prawo wtórne Unii Europejskiej

Rozporządzenie o ochronie danych osobowych

Rozporządzenie o ochronie danych osobowych (RODO) zastąpiło długo obowiązującą dyrektywę 95/46/WE. Zadaniem tego rozporządzenia jest **wzmocnienie prawa jednostki w świecie cyfrowym**. Jednak jej twórcy założyli osiągnięcie również szeregu innych, bardzo ambitnych celów.

Głównym celem RODO (jak wskazuje motyw 3 regulacji) jest wzmocnienie i zharmonizowanie ochrony podstawowych wolności i praw osób fizycznych w związku z czynnościami przetwarzania danych osobowych oraz zapewnienie swobodnego przepływu danych między państwami członkowskimi. Przyznana na gruncie RODO ochrona traktowana jest w sposób rozszerzający, celem rozporządzenia jest ochrona wszelkich wolności i praw wchodzących w zakres autonomii jednostki[143]. Jednocześnie, jak pokazują decy-

---

[142] Zob. H. Hijmans, *The European Union as a guardian of Internet privacy. The story of art 16 TFEU*, Switzerland 2016, s. 127–131; M. Kotzur, [w:] R. Geiger, D.E. Khan, M. Kotzur, *European Union Treaties. a commentary*, Monachium, 2015, s. 232–233.

[143] M. Jabłoński, *W procesie definiowania gwarancji niezależności i spójności krajowego systemu ochrony danych osobowych*, [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017, s. 64.

zje organów nadzorczych oraz orzecznictwo sądów, ochrony przewidzianej na gruncie RODO nie należy ograniczać jedynie do praw informacyjnych. **Przepisy RODO powinny być interpretowane w taki sposób, aby zapewnić ochronę jak najszerszego katalogu praw i wolności**, włączając w to m.in. prawa majątkowe[144] czy ochronę przed napastowaniem seksualnym[145]. Prawodawca unijny w RODO widzi szansę na zapewnienie bezpieczeństwa przetwarzania danych osobowych w Internecie oraz zwiększenia zaufania obywateli do usług cyfrowych.

Prace, które odbywały się w Komisji Europejskiej przed przyjęciem RODO, sugerują, że **miało ono na celu nie tylko zapewnić zwiększenie ochrony praw osób fizycznych, ale również poszerzenie możliwości biznesowych poprzez ułatwienie swobodnego przepływu danych na jednolitym rynku cyfrowym**. Ustawodawca unijny zwraca na to uwagę już w motywie 2 rozporządzenia, wskazując, że ma ono na celu „przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także do pomyślności ludzi". Ponadto w motywie 5 zauważono, że „szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. […] Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych". Ujednolicenie przepisów dotyczących danych osobo-

---

[144] Decyzja duńskiego organu nadzorczego z dnia 6 września 2021 r., nr 2020-31-3586; OLG Köln z 14.07.2022, nr 15 U 137/21.

[145] D. Kuźnicka-Błaszkowska, *European Union: The Role of the GDPR in Preventing Sexual Abuse*, „European Data Protection Law Review" 2022, nr 8(4), s. 511–516 i przywołane tam decyzje organów nadzorczych.

wych pozwoli na większą swobodę w prowadzeniu działalności gospodarczej i zniweluje część ograniczeń związanych z dotychczas odmiennymi zasadami przetwarzania danych w państwach członkowskich. RODO ma również służyć rozwojowi zdrowej konkurencji w warunkach gospodarczych. W motywie 10 podkreślono, że **celem rozporządzenia jest wysoki i spójny stopień ochrony osób fizycznych oraz usunięcie przeszkód w przepływie danych osobowych w Unii Europejskiej**.

Kolejnym celem regulacji, który odczytać można tym razem z motywu 7, jest nie tylko zapewnienie stabilnych i spójnych ram ochrony danych w Unii Europejskiej, ale również **wyposażenie organów administracji publicznej w narzędzia umożliwiające skuteczne egzekwowanie przepisów** w tym zakresie. Zdaniem unijnego prawodawcy przyczyni się to do budowy zaufania, niezbędnego do rozwoju gospodarki cyfrowej na rynku wewnętrznym. Zgodnie z motywami RODO nie jest możliwe przyznanie jednostkom pełnej kontroli nad ich danymi osobowymi bez wyposażenia organów nadzorczych w pakiet kompleksowych i skutecznych kompetencji. Postulat ten zgłaszany był już w 1979 r.[146] i już wtedy podkreślano konieczność zagwarantowania niezależności tych organów. Wraz z wejściem w życie RODO dostrzeżono, że **skuteczna ochrona praw jednostki nie jest możliwa bez powołania właściwego organu nadzorczego w pełni niezależnego od pozostałych organów władzy publicznej**[147].

---

[146] Rezolucja Parlamentu Europejskiego z dnia 8 maja 1979 r. w sprawie ochrony praw jednostek w odniesieniu do postępu technicznego w dziedzinie automatycznego przetwarzania danych PE z dnia 8 maja 1979 r. (Dz. U. WE C 140 z 1979 r.).

[147] M. Rojszczak, *Reforma krajowych przepisów o ochronie danych a kwestia niezależności organów nadzorczych na tle rozporządzenia 2016/679 i dyrektywy 2002/58 – uwagi krytyczne*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, nr 4(7), s. 71; D. Kuźnicka, *Organ nadzorczy w RODO: nowe wyzwanie w zakresie administracji publicznej?*, [w:] M. Pisz, M. Przychodzki, M. Radajewski (red.), *Zagadnienia współczesnego prawa publicznego*, Poznań 2018, s. 91–107.

Obecnie (czerwiec 2025), po ponad 7 latach stosowania RODO, wydaje się, że chociaż cel i idea przyświecające twórcom rozporządzenia były słuszne, nie można z całą pewnością stwierdzić, że nadal prowadzą do właściwych rozwiązań. Z pewnością praktyka ochrony danych osobowych tylko w ograniczonym zakresie została ujednolicona, a organy nadzorcze wciąż w różny sposób interpretują zakres ochrony. Wielość użytych w regulacji pojęć niedookreślonych powoduje, że jej stosowanie jest utrudnione[148]. Po drugie, koszt poniesiony przez podmioty prywatne w związku z dostosowaniem funkcjonowania organizacji do przepisów RODO był ogromny, a co więcej – nakładane przez organy kary pieniężne odbijają się na wartości przedsiębiorców na giełdzie. Niestety, RODO nie doprowadziło do znaczących zmian w zakresie ochrony prywatności i danych osobowych jednostki w relacjach z organami państwa, a ograniczenie maksymalnej wysokości kary administracyjnej, która może być nałożona na podmiot publiczny, powoduje, że koszty nieprzestrzegania mogą być niższe od kosztów wdrożenia. RODO stało się również punktem zapalnym w relacjach pomiędzy Unią Europejską a jej partnerami handlowymi, powodując spadek atrakcyjności rynku wspólnotowego dla zagranicznych inwestorów.

Inne akty prawa wtórnego

Rozporządzenie o ochronie danych osobowych nie jest jedynym aktem prawa wtórnego Unii Europejskiej, które reguluje kwestie ochrony danych osobowych. Odnosi się do niej szereg innych aktów prawnych, które w praktyce regulują funkcjonowanie wielu różnych gałęzi gospodarki. Spośród wielu regulacji można wyróżnić:

1) dyrektywę 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności han-

[148] Zob. M. Jabłoński, D. Kuźnicka-Błaszkowska, *„Disproportionate Effort" in the Meaning of Article 14 of the General Data Protection Regulation*, „Przegląd Prawa Konstytucyjnego" 2021, nr 6, s. 505–518.

dlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz. Urz. WE L 178/1 z 17.07.2000 r.);
2) dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. WE L 201/37 z 31.07.2002 r.);
3) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 295/39 z 21.11.2018 r.);
4) dyrektywę policyjną;
5) akt o zarządzaniu danymi, akt o usługach cyfrowych, akt o sztucznej inteligencji, rozporządzenie w sprawie europejskiej przestrzeni danych dotyczących zdrowia, Europejski kodeks łączności elektronicznej;
6) Konwencję Wykonawczą do układu z Schengen z dnia 14 czerwca 1985 roku między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (Dz. Urz. WE L 239/19 z 22.09.2000 r.).

Z powyższych rozważań wynika, że podstawa prawna ochrony danych osobowych w Unii Europejskiej jest zróżnicowana, co skutkuje odmiennymi zasadami i restrykcyjnymi trybami przyjmowania środków gwarantujących ochronę danych osobowych w poszczególnych obszarach, które pozostają w kompetencjach Unii Europejskiej[149].

[149] D. Kornobis-Romanowska, *Rozporządzenie o ochronie danych osobowych – charakter prawny, zakres stosowania i skutek w prawie krajowym państw członkowskich*, [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda (red.), *op. cit.*, s. 20.

3.5. Specyfika polskiego systemu źródeł prawa w zakresie informacji i ochrony danych osobowych

Wskazane w powyższych punktach niniejszego rozdziału akty prawne są częścią polskiego systemy źródeł prawa, który ma charakter dualistyczny, ponieważ dzieli się na **źródła prawa powszechnie i wewnętrznie obowiązujące**. Podział źródeł prawa, a także ich hierarchia wynika z postanowień Konstytucji RP[150], które omówione zostały w tej części podręcznika z uwzględnieniem wybranych regulacji odnoszących się do informacji i ochrony danych osobowych.

Podstawowe wyliczenie źródeł prawa powszechnie obowiązującego, które na potrzeby niniejszego podręcznika jest wystarczające, określone zostało w art. 87 Konstytucji RP. Zgodnie z tym przepisem źródłami takimi są:

- Konstytucja;
- ustawy;
- ratyfikowane umowy międzynarodowe;
- rozporządzenia;
- akty prawa miejscowego.

Jak wynika z przyjętych rozwiązań, **Konstytucja** jest nadrzędnym aktem w systemie źródeł prawa. Gwarantuje ona jednostce m.in. wolność informacyjną, która dotyczy „w szczególności prawa dostępu do informacji publicznej, które jest nie tylko podstawowym gwarantem kształtowania się społeczeństwa obywatelskiego, ale także skutecznym sposobem permanentnej kontroli inicjowanej w każdym czasie przez jednostkę bądź inny podmiot prawa. Trzeba jednak pamiętać, że działalność państwa wiąże się z koniecznością zapewnienia jego bezpieczeństwa zarówno w aspekcie wewnętrznym, jak i zewnętrznym. Kolizja między sferą wolności a klasyczną

[150] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.).

przesłanką ograniczenia wolności i praw musi skutkować przyjęciem określonego rodzaju rozwiązań zgodnych ze standardami, na których opiera się funkcjonowanie demokratycznego państwa"[151]. Jednym z elementów charakterystycznych dla demokratycznego państwa jest jawność jego działania. Przejawia się ona m.in. w zagwarantowaniu jednostce szeregu uprawnień informacyjnych, takich jak np.:

- wolność prasy i środków społecznego przekazu (art. 14 Konstytucji RP)[152];
- wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji (art. 54 Konstytucji RP)[153];
- prawo do informacji publicznej (art. 61 Konstytucji RP)[154];

---

[151] M. Jabłoński, T. Radziszewski, *op. cit.*, s. 18.

[152] Art. 14 Konstytucji RP „Rzeczpospolita Polska zapewnia wolność prasy i innych środków społecznego przekazu".

[153] Art. 54 Konstytucji RP:

„Ust. 1. Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji.

Ust. 2. Cenzura prewencyjna środków społecznego przekazu oraz koncesjonowanie prasy są zakazane. Ustawa może wprowadzić obowiązek uprzedniego uzyskania koncesji na prowadzenie stacji radiowej lub telewizyjnej".

[154] Art. 61 Konstytucji RP:

„Ust. 1. Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa.

Ust. 2. Prawo do uzyskiwania informacji obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu.

Ust. 3. Ograniczenie prawa, o który mowa w ust. 1 i 2, może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa.

Ust. 4. Tryb udzielania informacji, o których mowa w ust. 1 i 2, określają ustawy, a w odniesieniu do Sejmu i Senatu ich regulaminy".

– prawo do informacji o stanie i ochronie środowiska (art. 74 ust. 3 Konstytucji RP)[155].

„Ponadto do szeroko rozumianej «autonomii informacyjnej jednostki» zaliczyć trzeba także:

– prawo do prywatności (art. 47 Konstytucji RP)[156]
– wolność i ochronę tajemnicy komunikowania się (art. 49 Konstytucji RP)[157]
– nienaruszalność miru domowego (art. 50 Konstytucji RP)[158]
– prawo do ochrony danych osobowych (art. 51 Konstytucji RP[159])"[160].

Ustawa to kolejny akt prawa powszechnie obowiązującego, który musi być zgodny z postanowieniami Konstytucji RP. Akt ten pochodzi od parlamentu i jest „uchwalany przezeń w specjalnej procedurze (zwanej procedurą ustawodawczą), posiadający (co do zasady) nie-

[155] Art. 74 ust. 3 Konstytucji RP „Każdy ma prawo do informacji o stanie i ochronie środowiska".

[156] Art. 47 Konstytucji RP „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz decydowania o swoim życiu osobistym".

[157] Art. 49 Konstytucji RP „Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony".

[158] Art. 50 Konstytucji RP „Zapewnia się nienaruszalność mieszkania. Przeszukanie mieszkania, pomieszczenia lub pojazdu może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony".

[159] Art. 51 Konstytucji RP:

„Ust. 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

Ust. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

Ust. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.

Ust. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

Ust. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa".

[160] M. Jabłoński, T. Radziszewski, *op. cit.*, s. 18.

ograniczony zakres przedmiotowy i uzyskujący moc obowiązującą pod warunkiem prawidłowego ogłoszenia”[161]. Aktem wykonawczym do ustawy jest natomiast **rozporządzenie**, które zajmuje przedostatnie miejsce w podstawowej hierarchii źródeł prawa. Jego uwzględnienie w tym miejscu jest celowe, ponieważ, jak wynika z treści art. 92 Konstytucji RP, to rozporządzenia są wydawane przez organy wskazane w Konstytucji[162], na podstawie szczegółowego upoważnienia zawartego w ustawie i w celu jej wykonania. Upoważnienie powinno określać organ właściwy do wydania rozporządzenia i zakres spraw przekazanych do uregulowania oraz wytyczne dotyczące treści aktu[163]. Ponadto, co należy podkreślić, organ upoważniony do wydania rozporządzenia nie może przekazać swoich kompetencji w tym zakresie innemu organowi (tzw. zakaz subdelegacji).

Biorąc powyższe pod uwagę, a także liczbę regulacji ustawowych i rozporządzeń wykonawczych odnoszących się do zagadnienia informacji, bezpieczeństwa informacji i ochrony danych osobowych, należy zaznaczyć, że wskazany poniżej katalog aktów prawnych ma charakter jedynie przykładowy. **W obszarze informacji** są to m.in.:

1) ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902). Na podstawie art. 9 ust. 5 tej ustawy wydane zostało:

---

[161] M. Bernaczyk, *Źródła prawa*, [w:] *Konstytucja i prawo konstytucyjne. Zarys wykładu*, Warszawa 2021, s. 186.

[162] Organy upoważnione do wydawania rozporządzeń to:

– Prezydent RP (art. 142 ust. 1 Konstytucji RP);

– Rada Ministrów (art. 146 ust. 4 pkt 2 Konstytucji RP);

– Prezes Rady Ministrów (art. 148 pkt 3 Konstytucji RP);

– Minister kierujący określonym działem administracji rządowej (art. 149 ust. 2 Konstytucji RP);

– Przewodniczący określonych w ustawach komitetów (art. 149 ust. 3 Konstytucji RP);

– Krajowa Rada Radiofonii i Telewizji (art. 213 ust. 2 Konstytucji RP).

[163] M. Bernaczyk, *op. cit.*, s. 193 i n.; L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2019, s. 154 i n.

2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. z 2007 r. Nr 10, poz. 68);
3) ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystaniu informacji sektora publicznego (t.j. Dz. U. z 2023 r. poz. 1524). Na podstawie art. 34 ust. 7 tej ustawy wydane zostało:
4) rozporządzenie Rady Ministrów z dnia 21 listopada 2022 r. w sprawie portalu danych (Dz. U. z 2022 r. poz. 2415);
5) ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (t.j. Dz. U. z 2024 r. poz. 1940). Na podstawie art. 23 ust. 2 tej ustawy wydane zostało:
6) rozporządzenie Ministra Środowiska z dnia 22 września 2010 r. w sprawie wzoru oraz zawartości i układu publicznie dostępnego wykazu danych o dokumentach zawierających informacje o środowisku i jego ochronie (Dz. U. z 2010 r. Nr 186, poz. 1249).

W obszarze bezpieczeństwa informacji są to m.in.:

1) ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2024 r. poz. 1222). Na podstawie:
2) art. 12 ust. 6 tej ustawy wydane zostało: rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzenia kontroli stanu zabezpieczenia informacji niejawnych (Dz. U. z 2011 r. Nr 93, poz. 541);
3) art. 47 ust. 5 tej ustawy wydane zostało: rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. Nr 271, poz. 1603);
4) ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1222). Na podstawie art. 14 ust. 4 tej ustawy zostało wydane:

5) rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiadających za cyberbezpieczeństwo (Dz. U. z 2019 r. poz. 2479);
6) ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 1717). Na podstawie art. 18 tej ustawy zostało wydane:
7) rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773).

W obszarze ochrony danych osobowych[164] jest to m.in.:

1) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781);
2) ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2023 r. poz. 1206). Ustawa ta stanowi implementację dyrektywy 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 uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.05.2016 r., s. 89).

---

[164] Zob. na ten temat M. Błażewski, J. Behr, *Środki prawne ochrony danych osobowych*, Wrocław 2018, s. 41 i n.

Poza wskazanymi wyżej aktami prawnymi odnoszącymi się do ochrony danych osobowych należy wymienić także tzw. RODO, czyli 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., s. 1 ze zm.). Rozporządzenie to nie jest ani ustawą, ani umową międzynarodową. Jest to akt wtórny Unii Europejskiej[165], którego cechą charakterystyczną jest to, że wiąże ono w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich. W razie jego kolizji z ustawami ma ono (rozporządzenie unijne) pierwszeństwo, co bezpośrednio wynika z treści art. 91 ust. 3 Konstytucji RP[166].

Ratyfikowane umowy międzynarodowe to kolejne źródło prawa powszechnie obowiązującego. Istotną cechą jest ich ratyfikacja, której dokonuje Prezydent RP[167] „w formie aktu urzędowego podlegającego kontrasygnacie, po uprzednim przedłożeniu Prezydentowi umowy międzynarodowej przez Radę Ministrów wraz z projektem

[165] Akty prawne UE dzielą się na akty pierwotne i wtórne. Te pierwsze obejmują „układy (umowy międzynarodowe) tworzące Unię Europejską, aneksy do nich, traktaty je nowelizujące, traktaty o przystąpieniu nowych państw do UE, traktaty z państwami nienależącymi do UE" (B. Banaszak, *Prawo konstytucyjne*, Warszawa 2015, s. 127). Drugie zaś obejmują:

– rozporządzenia;

– dyrektywy – wiążą każde państwo członkowskie, do którego są kierowane, w odniesieniu do rezultatu, który ma być osiągnięty, pozostawiają jednak organom krajowym swobodę wyboru formy i środków;

– decyzje – wiążą w całości. Decyzja, która wskazuje adresatów, wiąże tylko tych adresatów (art. 288 Traktatu o funkcjonowaniu Unii Europejskiej, wersja skonsolidowana: Dz. Urz. UE C 202/47 z 7.06.2016 r.).

[166] Art. 91 ust. 3 Konstytucji stanowi: „Jeżeli wynika to z ratyfikowanej przez Rzeczpospolitą Polską umowy konstytuującej organizację międzynarodową, prawo przez nią stanowione jest stosowane bezpośrednio, mając pierwszeństwo w przypadku kolizji z ustawami".

[167] Art. 133 ust. 1 pkt 1 Konstytucji RP.

dokumentu ratyfikacyjnego. Uwzględniwszy prawo międzynarodowe i krajowy stan prawny, należy przyjąć, że jest to akt międzynarodowy, przez który Prezydent RP wyraża w imieniu państwa na płaszczyźnie międzynarodowej ostateczną zgodę na związanie się traktatem (umową)"[168]. Patrząc przez pryzmat postanowień Konstytucji RP, możemy zauważyć, że ustrojodawca w ramach ratyfikowanych umów międzynarodowych przewidział następujące tryby ich ratyfikacji:

1) umowy międzynarodowe ratyfikowane za uprzednią zgodą wyrażoną w ustawie (art. 89 ust. 1 Konstytucji RP);
2) umowy międzynarodowe ratyfikowane bez uprzedniej zgody wyrażonej w ustawie (art. 89 ust. 2 Konstytucji RP);
3) umowa międzynarodowa dotycząca przekazania organizacji międzynarodowej lub organowi międzynarodowemu kompetencji organów władzy państwowej w niektórych sprawach, na której ratyfikację udzielona została zgoda w ustawie (art. 90 ust. 1 i 2 Konstytucji RP) lub referendum ogólnokrajowym (art. 90 ust. 3 Konstytucji RP).

Wskazane wyżej tryby nie pozostają bez wpływu na miejsce w hierarchii źródeł prawa ratyfikowanych umów międzynarodowych. Należy bowiem podkreślić, że ratyfikowane umowy międzynarodowe przyjęte w trybie, o którym mowa w pkt 1 i 3, mają pierwszeństwo przed ustawami, jeżeli ustawy nie da się pogodzić z umową. Z kolei ratyfikowane umowy międzynarodowe przyjęte we wskazanym w pkt 2 trybie zajmują w tej hierarchii miejsce po ustawie, ale przed rozporządzeniami wykonawczymi.

Mając powyższe na względzie, należy podkreślić, że do **umów międzynarodowych w obszarze informacji** zalicza się m.in.:

1) 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);

---

[168] M. Bernaczyk, *op. cit.*, s. 203.

2) Konwencję o ochronie praw człowieka i podstawowych wolności sporządzoną w Rzymie dnia 4 listopada 1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.).

W obszarze bezpieczeństwa informacji jest to m.in.:

1) Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli dnia 6 marca 1997 r. (Dz. U. z 2000 r. Nr 64, poz. 740);
2) Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Albanii w sprawie wzajemnej ochrony informacji niejawnych, podpisana w Tiranie dnia 21 września 2004 r. (Dz. U. z 2005 r. Nr 247, poz. 2093).

W obszarze ochrony danych osobowych jest to m.in.:

1) Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych podpisana w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25 ze zm.);
2) Karta praw podstawowych Unii Europejskiej (wersja skonsolidowana Dz. Urz. UE C 202/389 z 7.06.2016 r.).

Ostatnim źródłem prawa powszechnie obowiązującego są **akty prawa miejscowego**, które obowiązują na obszarze działania organów, które je ustanowiły. Akty te są wydawane przez organy samorządu terytorialnego oraz terenowe organy administracji rządowej na podstawie i w granicach upoważnień zawartych w ustawie. Zasady i tryb wydawania aktów prawa miejscowego określa ustawa. Z uwagi na specyfikę tego źródła prawa ustawodawca nie przekazał do uregulowania kwestii informacji, bezpieczeństwa informacji i ochrony danych osobowych w formie aktów prawa miejscowego.

Na dualistyczny system źródeł prawa składają się – jak zostało to podkreślone już wcześniej – **akty prawa powszechnie obowiązującego oraz akty prawa wewnętrznego**. Te ostatnie mają następujące cechy:

- obowiązują tylko jednostki organizacyjne podległe organowi wydającemu te akty;
- wydawane są na podstawie ustawy;
- nie mogą stanowić podstawy decyzji wobec obywateli, osób prawnych oraz innych podmiotów;
- muszą być zgodne z powszechnie obowiązującym prawem[169].

Należy przy tym zaznaczyć, że „kompetencja do stanowienia aktów prawa wewnętrznego ma charakter otwarty zarówno z punktu widzenia podmiotowego, jak i przedmiotowego"[170]. Dlatego też wymienione w art. 93 ust. 1 formy tych aktów i podmioty uprawnione do ich wydawania (uchwały Rady Ministrów, zarządzenia Prezesa Rady Ministrów) mają charakter jedynie przykładowy. **Przykładami aktów wewnętrznie obowiązujących w obszarze bezpieczeństwa informacji i ochrony danych osobowych** są:

1) Zarządzenie Prezesa Urzędu Ochrony Konkurencji i Konsumentów z dnia 3 września 2021 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Ochrony Konkurencji i Konsumentów (Dz. Urz. UOKiK z 2021 r., poz. 2 ze zm.);
2) Zarządzenie Prezesa Urzędu Ochrony Konkurencji i Konsumentów z dnia 7 września 2021 r., w sprawie podstawowych zasad bezpieczeństwa informacji w Urzędzie Ochrony Konkurencji i Konsumentów (Polityka Bezpieczeństwa Informacji) (Dz. Urz. UOKiK z 2021 r., poz. 3);
3) Zarządzenie Nr 79/2018 Rektora Uniwersytetu Wrocławskiego z dnia 13 czerwca 2018 r. w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim[171].

---

[169] Art. 93 Konstytucji RP.
[170] L. Garlicki, *op. cit.*, s. 159.
[171] Zarządzenie dostępne na https://bip.uni.wroc.pl [dostęp: 24.06.2025].

Rozdział IV

Podstawowe definicje dotyczące ochrony danych osobowych

Ochrona danych osobowych została w sposób kompleksowy uregulowana przez unijnego i polskiego prawodawcę. W wyniku tych działań ramy prawne zawierają kompletną siatkę pojęciową, której znajomość jest niezbędna w celu zapewnienia odpowiedniego standardu ochrony dla praw i wolności jednostki.

4.1. Dane osobowe

Podstawowym pojęciem funkcjonującym na gruncie RODO jest pojęcie „danych osobowych". Oznacza ono **informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej** („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności 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[172]. Zidentyfikowaną osobą jest taka, która jest znana administratorowi

[172] Art. 4 pkt 1 RODO.

lub którą można zidentyfikować od razu[173] bez podejmowania dodatkowych działań[174]. Za możliwą do zidentyfikowania należy uznać taką osobę, która będzie możliwa do bezpośredniego lub pośredniego zidentyfikowania[175].

Jednocześnie ocena, czy dana informacja ma charakter danych osobowych, każdorazowo powinna odbywać się przy uwzględnieniu okoliczności faktycznych (ocena *ad casus*). Dla przykładu: nie ma wątpliwości, że w przypadku, gdy dana baza danych zawiera imię i nazwisko oraz numer telefonu podmiotu danych, ten ostatni będzie stanowił daną osobową. W przypadku jednak, gdy baza danych zawiera wyłącznie numery telefonów, może się to okazać niewystarczające, aby doprowadzić do identyfikacji osoby fizycznej, zatem taka informacja w tym konkretnym przypadku nie będzie stanowić danych osobowych[176]. Warto zwrócić uwagę, że na gruncie RODO ochronie podlegają dane osobowe jedynie osób fizycznych, żywych – przepisów rozporządzenia nie stosuje się do danych osobowych osób zmarłych (chociaż niektóre z organów nadzorczych podjęły próby stosowania przepisów rozporządzenia w przypadku osób zmarłych). Podejście to jest zbieżne z dotychczasową praktyką wykształconą również w Polsce[177]. Możliwe jest przyjęcie przez pań-

---

[173] D. Bach-Golecka, R. Stankiewicz (red.), *Organizacja systemu ochrony zdrowia. System Prawa Medycznego*, t. 3, Warszawa 2020.

[174] D. Lubasz, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 165.

[175] E. Kuczkowska, *Glosa aprobująca do wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 13 kwietnia 2021 r., sygn. akt II SA/Wa 1898/20*, „Roczniki Administracji i Prawa" 2021, z. 3, s. 273.

[176] Wyrok WSA w Warszawie z dnia 13 kwietnia 2021 r., II SA/Wa 1898/20; zob. również P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018.

[177] E. Żywucka-Kozłowska, R. Dziembowski, *Dane osobowe zmarłego. Uwagi na gruncie prawa i tradycji społecznej*, „Kortowski Przegląd Prawniczy" 2022, nr 4, https://doi.org/10.31648/kpp.8527.

stwo przepisów chroniących dane osobowe osób zmarłych, jednak w Polsce dotychczas one nie powstały.

Należy się zgodzić z tezą wyrażoną przez Sąd Apelacyjny w Szczecinie, że **żeby uznać określone informacje za dane osobowe nie jest konieczne, aby prowadziły one do wskazania z imienia i nazwiska konkretnej osoby. Wystarczy, że umożliwią one wyodrębnienie jej spośród innych osób, w sposób, który umożliwi wywieranie na nią określonego wpływu**[178].

W definiowaniu pojęcia danych osobowych w systemie Unii Europejskiej sporą rolę odegrały zarówno Europejski Trybunał Praw Człowieka, Trybunał Sprawiedliwości Unii Europejskiej, jak również organy państw członkowskich. Ten pierwszy w swoim dotychczasowym orzecznictwie uznał, że za dane osobowe należy uznać m.in. dane pozyskane przy użyciu narzędzi geolokalizacyjnych, adres IP[179], informacje pozyskane z bilingów telefonicznych czy monitoringu poczty e-mail[180], próbki DNA[181], nagranie głosu[182]. TSUE wskazuje z kolei, że za dane osobowe należy uznać m.in. odręczny podpis osoby fizycznej[183] czy ciąg znaków alfanumerycznych, do których przypisane są preferencje użytkowników Internetu[184].

Warto zwrócić uwagę, że o znaczeniu danych osobowych we współczesnym świecie przesądza m.in. to, że, **szczególnie w przypadku usług cyfrowych, stanowią one ekwiwalent zapłaty za**

---

[178] Wyrok Sądu Apelacyjnego w Szczecinie z dnia 10 lipca 2024 r., I ACa 1400/22.

[179] Wyrok ETPCz z dnia 24 kwietnia 2018 r. w sprawie *Benedik p. Słowenii*, skarga nr 62357/14.

[180] Skarga nr 61496/08.

[181] Wyrok ETPCz z dnia 14 kwietnia 2020 r. w sprawie *Dragan Petrović p. Serbii*, skarga nr 75229/10.

[182] Wyrok ETPCz z dnia 25 września 2001 r. w sprawie *P.G. i J.H. p. Wielkiej Brytanii*, skarga nr 44787/98; wyrok ETPCz z dnia 31 maja 2005 r. w sprawie *Vetter p. Francji*, skarga nr 59842/00.

[183] Wyrok TSUE z dnia 4 października 2024 r., C-200/23.

[184] Wyrok TSUE z dnia 7 marca 2024, C-604/22.

spełnione świadczenie[185]. Niestety ramy niniejszego opracowania nie pozwalają na wyczerpujące omówienie tej kwestii, należy jednak zaznaczyć, że podejście to z jednej strony jest powszechnie stosowane przez biznes, z drugiej – budzi istotne wątpliwości natury prawnej i było wielokrotnie przedmiotem interpretacji i analizy. Kwestia „zapłaty" danymi osobowym za określone usługi cyfrowe doprowadziła do wykształcenia się modelu „pay or ok", będącego przedmiotem krytyki m.in. Europejskiej Rady Ochrony Danych[186].

Z uwagi na ich komercyjną wartość oraz możliwości ich wykorzystania wskazuje się, że dane osobowe są **kluczowym obiektem zainteresowania cyberprzestępców**[187]. Zagrożenie to jest szczególnie widoczne w przypadku indywidualnych użytkowników szeregu serwisów internetowych (np. poprzez wykorzystanie cyfrowych śladów w celu kradzieży tożsamości, ale również mniej wyrafinowane formy przestępstw, takie jak kradzież danych wykorzystywanych do logowania do bankowości elektronicznej). Niemniej, biorąc pod uwagę zakres danych osobowych gromadzonych przez podmioty prywatne i organy publiczne, można stwierdzić, że dane osobowe są jednym z głównych obszarów narażonych na ryzyko w organizacji.

4.2. Szczególne kategorie danych osobowych

Pojęcie szczególnych kategorii danych osobowych na gruncie RODO zostało doprecyzowane poprzez umieszczenie w art. 9 rozporządzenia zamkniętego katalogu danych osobowych, które z uwagi

---

[185] W. Dybka, *Dane osobowe dotyczące konsumenta jako przedmiot świadczenia*, „Kwartalnik Prawa Prywatnego" 2023, z. 1, s. 97.

[186] EDPB, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf [dostęp: 24.06.2025].

[187] J. Kwaśnik, *Dane osobowe jako kluczowy obiekt zainteresowania cyberprzestępców*, „Annales Canonici" 2020, z. 1, s. 25–37.

na swój charakter wymagają wzmożonej ochrony. Unijny prawodawca w motywie 51 RODO zauważa, że „Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności".

W art. 9 znalazł się **generalny zakaz przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby**. Powyższy katalog należy uznać za enumeratywne wyliczenie danych osobowych szczególnych kategorii. Katalog ten **nie może być interpretowany w sposób rozszerzający**[188]. Warto podkreślić, że unijny ustawodawca zdecydował się na zdefiniowanie tylko niektórych z nich, zakładając (być może błędnie), że pozostałe są na tyle jasne, iż nie wymagają dalszej interpretacji.

Za dane szczególnych kategorii uznano m.in. dane osobowe ujawniające pochodzenie rasowe i etniczne. Są to takie informacje, które odnoszą się do zespołu cech zewnętrznych charakterystycznych dla grupy ludzi o wspólnym pochodzeniu[189]. Dane te mogą dotyczyć np. przynależności do mniejszości etnicznej[190]. Jednocześnie, jak wskazuje motyw 51, ochrona informacji o pochodzeniu rasowym

---

[188] D. Kuźnicka-Błaszkowska, M. Jabłoński, *Information on Gender Identity as Personal Data under EU and US Data Protection Models*, „Białostockie Studia Prawnicze" 2024, vol. 29, no. 3, s. 210.

[189] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2021, s. 198.

[190] L. Georgieva, Ch. Kuner, *Article 9*, [w:] Ch. Kuner, L.A. Bygrave, Ch. Docksey, *The EU Generall Data Protection Regulation (GDPR). A Commentary*, Oxford 2020, s. 374.

na gruncie RODO nie stoi w sprzeczności z generalnym nieuznawaniem przez Unię Europejską koncepcji rasy.

Przekonania religijne i światopoglądowe powinny być rozumiane jako informacje ujawniające przynależność do Kościoła lub związku wyznaniowego, organizacji zrzeszającej osoby o podobnych przekonaniach światopoglądowych, jak również zachowania, które świadczą o takiej przynależności (np. modlitwa, określony ubiór czy odmowa spożywania określonych pokarmów)[191].

Szczególnej ochronie podlegają również informacje o przynależności do związków zawodowych, czyli np. oświadczenie o członkostwie, materiały pozyskane z zebrań związkowych, deklaracje założycielskie i im podobne. Rozwiązanie to ma na celu ochronę pracowników przed dyskryminacją, głównie ze strony pracodawców, ale również ze strony aparatu państwowego.

W art. 4 RODO unijny prawodawca zdefiniował pojęcie danych genetycznych, wskazując, że oznaczają one dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej. Ochrona danych genetycznych na podstawie RODO, na etapie jego przyjęcia, była pewną nowością w prawie unijnym. Ujęcie w katalogu informacji podlegających szczególnej ochronie związane jest m.in. z rosnącą liczbą podmiotów, które przetwarzają te dane bądź to w celach naukowych, bądź komercyjnych[192]. Przykładem takich działań są np. komercyjnie dostępne testy genetyczne[193]. Dane genetyczne pochodzą z ludzkich tkanek lub in-

---

[191] *Ibidem*, s. 375.

[192] P. Sukhorolsky, V. Hutsaliuk, *Processing of genetic data under GDPR: unresolved conflict of interests* „Masaryk UniversityJournalof Law and Technology" 2020, t. 14, s. 152.

[193] Zob. więcej A. Marcon, C. Rachul, T. Caulfield, *The consumer representation of DNA ancestry testing on YouTube*, „New Genetics and Society" 2021, nr 2, s. 133–154.

nych próbek biologicznych. Obejmują one próbki krwi, śliny i moczu pobrane od osób, tkanki pobrane ze zwłok w starożytnych badaniach DNA, próbki gleby, wody i skał w badaniach DNA środowiskowego[194]. Grupa Robocza Art. 29 w swoich rekomendacjach dotyczących danych genetycznych wskazuje, że posiadają one następujące cechy:

1) dane genetyczne ujawniają informacje nie tylko o osobie, której dane dotyczą, ale także o jej krewnych i niektórych grupach osób, do których ona należy;
2) z reguły informacje genetyczne są nieznane samemu nosicielowi i nie zależą od jego indywidualnej woli, ponieważ dane genetyczne są niezmienne;
3) dane genetyczne można łatwo uzyskać z surowców;
4) dane genetyczne mogą ujawnić więcej informacji w przyszłości i być wykorzystywane przez coraz większą liczbę agencji do różnych celów[195].

Warto zwrócić uwagę na fakt, że **dane genetyczne mają charakter kolektywny – z ich natury wynika, że łączą się one z więcej niż jedną osobą**[196]. W praktyce rozróżnienie danych genetycznych od danych biometrycznych i danych dotyczących zdrowia może budzić duże trudności[197]. Jednocześnie RODO nie różnicuje w tym zakresie poziomu ochrony, wątpliwości mogą pojawić się dopiero na poziomie prawa krajowego i tylko w bardzo szczegółowych przypadkach[198].

---

[194] P. Quinn, L. Quinn, *Big genetic data and its big data protection challenges*, „Computer Law & Security Review" 2018, vol. 34(5), s. 1000–1018.

[195] Grupa Robocza Art. 29, *Working Document on Genetic Data*, przyjęty 17 marca 2004 r., 12178/03/EN WP 91, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf [dostęp: 24.06.2025].

[196] K. Olejniczak, *Ochrona danych genetycznych – od koncepcji indywidualnej do grupowej*, „Przegląd Prawa Medycznego" 2024, nr. 3, s. 36.

[197] Ł. Drożdżowski, *Zakres ochrony danych genetycznych na gruncie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, „Forum Prawnicze" 2022, nr 4(72), s. 68–69.

[198] *Ibidem*.

„Dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Powszechnie za dane biometryczne uznaje się odciski palców, wzorzec siatkówki, strukturę twarzy, głos, układ żył, wygląd małżowiny usznej, nie jest to jednak katalog zamknięty[199]. Grupa Robocza Art. 29 wskazywała m.in., że danymi biometrycznymi mogą być umiejętności lub inne cechy zachowania[200]. Warto jednak zauważyć, że **nie każde dane behawioralne będą klasyfikowane jako dane biometryczne – nastąpi to jedynie w przypadku, gdy umożliwią one jednoznaczną identyfikację**[201].

Za „dane dotyczące zdrowia" unijny prawodawca uznał dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia. Ta szeroka definicja obejmuje nie tylko informacje o wszelkich chorobach lub nieprawidłowościach w zdrowiu, ale także chroni wszelkie informacje dotyczące zdrowia, niezależnie od tego, czy ujawnione informacje wskazują, że dana osoba jest w dobrym, czy złym stanie zdrowia[202]. Pojęcie danych dotyczących zdrowia obejmuje zarówno dane dotyczące zdrowia psychicznego,

---

[199] K. Gałęzowska, *Dane biometryczne a dane behawioralne*, dodatek „Monitora Prawniczego" 2022, nr 21, s. 9.

[200] Grupa Robocza Art. 29, *Opinia 4/2007 w sprawie pojęcia danych osobowych*, przyjęta 20 czerwca 2007, 01248/07/PL WP 136, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pl.pdf [dostęp: 24.06.2025].

[201] Zob. więcej: A. Krausova, *Online behavior recognition: can we consider it biometric data under gdpr?*, „Masaryk University Journal of Law and Technology" 2018, vol. 12(2), s. 161–178.

[202] D. Kuźnicka-Błaszkowska, J. Joachimska, *When Your Phone Knows You're Pregnant Even If You Don't: Period Tracking Applications and Threats to Privacy*, „Journal of International Women's Studies" 2025, vol. 27, iss. 1, Article 9, s. 3.

jak i fizycznego[203]. Dotyczy to tak obecnego, jak i dającego się przewidzieć przyszłego stanu zdrowia[204].

Dane osobowe dotyczące życia seksualnego pozostają również pod szczególną ochroną. Pojęcie życia seksualnego należy rozumieć w sposób szeroki – obejmuje ono zarówno informacje o podejmowaniu aktywności seksualnej, jak również informacje o wstrzemięźliwości[205]. Dane dotyczące seksualności mogą obejmować informacje takie, jak częstotliwość kontaktów seksualnych lub preferencje dotyczące zachowań seksualnych, ale także zaburzenia seksualne[206].

Dane dotyczące orientacji seksualnej to te, które ujawniają preferencje seksualne jednostki oraz wskazują, czy jest ona heteroseksualna, homoseksualna, biseksualna czy innej orientacji.

Na marginesie należy zauważyć, że informacja o tożsamości płciowej nie stanowi danych szczególnych kategorii[207]. Jednak z uwagi na wysokie ryzyko dla praw i wolności, jakie hipotetycznie niesie ich nieuprawnione ujawnienia, powinny one podlegać zwiększonej ochronie[208]. Jest to sytuacja podobna do numeru PESEL. Chociaż nie stanowi on danych osobowych szczególnej kategorii, to jak zauważa Prezes Urzędu Ochrony Danych Osobowych, ujawnienie numeru PESEL, wraz z takimi informacji, jak imię i nazwisko, stanowi wysokie ryzyko dla praw i wolności jednostki[209].

---

[203] *Ibidem*, s. 4.

[204] *Ibidem*.

[205] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, Legalis.

[206] D. Kuźnicka-Błaszkowska, M. Jabłoński, *Information on Gender Identity…*, s. 211.

[207] Zob. więcej D. Kuźnicka-Błaszkowska, *Informacje o tożsamości płciowej jako dane osobowe*, „ABI Expert" 2022, nr 2, s. 62–64; D. Kuźnicka-Błaszkowska, M. Jabłoński, *Information on Gender Identity…*, s. 207–220.

[208] Decyzja brytyjskiego organu nadzorczego z dnia 5 lipca 2021, https://ico.org.uk/media/action-weve-taken/mpns/2620171/mermaids-mpn-20210705.pdf [dostęp: 24.06.2025].

[209] Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 20 listopada 2018 r., sygn. ZWAD.405.10.2018.

4.3. Administrator

Administratorem w rozumieniu RODO może być osoba fizyczna lub prawna, organ publiczny, jednostka lub innych podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Z „byciem" administratorem wiąże się określony stan faktyczny oraz związane z nim konsekwencje (obowiązki i odpowiedzialność) na gruncie prawa ochrony danych osobowych[210]. Z uznaniem danego podmiotu za administratora nie wiąże się posiadanie danych osobowych, nie zachodzi tutaj stosunek własności zbioru danych w rozumieniu prawa cywilnego.

Aby zostać uznanym za administratora, **wystarczy nawet jednorazowe, tylko w jednym celu pozyskanie danych osobowych przez podmiot, który następnie decyduje o celach i sposobach przetwarzania**[211]. Na gruncie RODO nie jest wymagane, aby dane były przetwarzane w sposób stały lub kilkukrotnie. Naczelny Sąd Administracyjny wskazuje, że **status administratora nie wynika z samego faktu posiadania danych, ale ze sprawowania faktycznej kontroli nad ich przetwarzaniem, obejmującej dwa elementy – decydowanie o celach i środkach przetwarzania danych**[212]. Administratora nie można również wyznaczyć poprzez umowę – umowa powierzenia przetwarzania, w której wskazuje się jeden z podmiotów jako administratora, **nie ma charakteru kreacyjnego, a jedynie deklaratoryjny, potwierdzający sytuację faktyczną**.

Wyjątkiem od zasady określania administratora na podstawie sytuacji faktycznej jest wyznaczenie administratora danych w przepisach prawa – wskazuje na to chociażby art. 4 pkt 7 RODO,

---

[210] B. Fischer *et al.*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie...*
[211] Wyrok NSA z dnia 3 grudnia 2015 r., I OSK 1166/14.
[212] Wyrok NSA z dnia 18 sierpnia 2016 r., I OSK 864/16.

zgodnie z którym „jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania". W przypadku gdy cele oraz sposoby przetwarzania danych wynikają wprost z przepisów obowiązującego prawa, prawodawca może określić w normach prawnych również osobę administratora.

W polskiej rzeczywistości prawnej sytuacja, w której ustawodawca wprost wskazuje administratora bądź chociaż przesłanki, które miałyby pomóc go ustalić, jest niezwykle rzadka[213]. Jeśli dany przepis nie określił osoby administratora, w takim wypadku ten status należy ocenić w świetle definicji zawartej w RODO[214] – to jest jako podmiot, który samodzielnie bądź wspólnie z innym podmiotem decyduje o celu i sposobach przetwarzania danych osobowych.

W przypadku organów publicznych, które przetwarzają dane osobowe w oparciu o art. 6 ust. 1 lit. e) RODO, inaczej należy rozumieć przesłankę decydowania o celach i sposobach przetwarzania danych osobowych[215]. **Podmiot publiczny nie ma bowiem swobody w zakresie decydowania o celach przetwarzania, gdyż są one wyznaczane przez właściwe przepisy prawa**. Cel przetwarzania będzie zatem wyznaczany przez przepisy prawa, ale to administrator będący organem publicznym będzie konkretyzował dany cel, żeby odpowiadał on potrzebom realizowanego przez niego działania[216].

---

[213] Zob. np. K. Witkowska-Nowakowska, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 219; P. Litwiński, [w:] P. Litwiński (red.), P. Barta, M. Kawecki, *op. cit.*, s. 223. M. Jabłoński, J. Węgrzyn, *Prawo dostępu do danych osobowych i ich treści*, Toruń 2023, s. 111 i n.

[214] P. Litwiński, [w:] P. Litwiński (red.), P. Barta, M. Kawecki, *op. cit.*, s. 223.

[215] *Ibidem*, s. 223.

[216] Wyrok NSA z dnia 28 sierpnia 2009 r., I OSK 1472/08.

Administratorem jest zawsze sam organ, a nie obsługujący go urząd[217]. W przypadku podmiotów opiniodawczo-doradczych, z uwagi na fakt, że nie decydują one ani o celu, ani o sposobach przetwarzania danych, nie mogą być uznane za administratora. Istotny jest również fakt, że podmioty opiniodawczo-doradcze, jak również inne jednostki organizacyjne czy organy wewnętrzne niemające zdolności sądowej, nie mogą samodzielne ponosić odpowiedzialności za czynności podejmowane w związku z przetwarzaniem danych. Taka odpowiedzialność nie wystąpi ani w stosunkach administracyjnoprawnych, ani cywilnoprawnych. **Ponoszenie przez administratora osobowych odpowiedzialności za przetwarzanie danych jest nieodłącznie związane z pełnieniem tej roli**[218].

4.4. Podmiot przetwarzający

W procesie przetwarzania danych osobowych obok administratora bardzo często występuje podmiot przetwarzający. Jego obecność w procesie jest w pełni **uzależniona od decyzji administratora o powierzeniu całości lub części operacji przetwarzania podmiotowi trzeciemu**. Podmiot ten wykonuje czynności przetwarzania na polecenie administratora, realizując jego cele, stosując się w tym zakresie do instrukcji wydanych przez administratora dotyczących sposobów przetwarzania danych osobowych.

Poza decyzją administratora pozostaje sytuacja, w której ustawodawca uznaje dany organ za podmiot przetwarzający. Dzieje się tak m.in. w przypadku przetwarzania przez gminę (a konkretnie – radę gminy) danych osobowych kandydatów na ławników i osób ich

---

[217] G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003, s. 55.

[218] Grupa Robocza Art. 29, *Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"*, przyjęta 16.02.2010 r., WP 169.

popierających[219]. Prawo o ustroju sądów powszechnych wskazuje, że w zakresie danych osobowych ławników administratorem są prezesi i dyrektorzy właściwych sądów oraz Minister Sprawiedliwości w zakresie realizowanych zadań[220]. Organ gminy będzie zatem pełnił funkcję podmiotu przetwarzającego. Nie jest to jednak wprost wskazane w przepisach ustawy.

Powierzenie przetwarzania to „stan faktyczny istniejący w konkretnych okolicznościach relacji pomiędzy administratorem lub współadministratorami a podmiotem przetwarzającym (niekiedy podmiotami przetwarzającymi)"[221]. Istotą relacji pomiędzy administratorem a podmiotem przetwarzającym jest wykonywanie czynności „przetwarzania" przez tego ostatniego. Podmiot przetwarzający to podmiot, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi nałożone przez rozporządzenie o ochronie danych, a w szczególności powinien posiadać wiedzę fachową, wiarygodność i zasoby.

---

[219] Art. 160 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (t.j. Dz. U. z 2024 r. poz. 1907).

[220] Art. 175a § 1 ustawy Prawo o ustroju sądów powszechnych.

[221] M. Sakowska-Baryła, *Powierzenie przetwarzania w administracji publicznej* [w:] M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018, s. 108–109.

Rozdział V

Zasady ochrony danych osobowych w ujęciu modelowym i praktycznym

Jak wynika z rozwiązań przyjętych na gruncie art. 5 RODO, do **zasad ochrony danych osobowych** zalicza się:

1) zasadę legalności, rzetelności i przejrzystości przetwarzania;
2) zasad celowości;
3) zasadę minimalizacji danych;
4) zasadę prawidłowości;
5) zasadę ograniczonego czasu przechowywania;
6) zasadę integralności i poufności;
7) zasadę rozliczalności.

Zasady te pełnią kluczową rolę w procesie przetwarzania danych osobowych. Zarówno administrator, jak i podmiot przetwarzający zobowiązani są dokonywać wykładni przepisów RODO w oparciu o wskazane wyżej zasady. Mają one charakter równorzędny, żadna z nich nie powinna być traktowana jako „pierwotna" bądź nadrzędna względem pozostałych. Powinny być one współstosowane, w większości przypadków naruszenie jednej z nich będzie prowadziło do naruszenia kolejnej. W praktyce zasady określone w art. 5 powinno się traktować jak system naczyń połączonych, w którym te zasady wzajemnie na siebie oddziałują i przenikają się. Interpretacja każdej z nich powinna być dokonywana z uwzględnieniem pozostałych. O tym, jak duże znaczenie przypisuje się zasadom dotyczącym przetwarzania danych osobowych, świadczą administracyjne

kary pieniężne nakładane za ich naruszenie przez organ nadzorczy (w Polsce jest nim Prezes Urzędu Ochrony Danych Osobowych) w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa (art. 83 ust. 5 RODO). Należy jednak podkreślić, że w przypadku organów i podmiotów publicznych każde państwo członkowskie może określić wysokość kar administracyjnych (art. 83 ust. 7 RODO)[222]. Kwestie te reguluje art. 102[223] ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. Biorąc pod uwagę dotychczasową praktykę nakładania administracyjnych kar pieniężnych przez organy nadzorcze, można wskazać, że w większości przypadków naruszenie zasad przetwarzania danych osobowych prowadzi do naruszenia co najmniej jednego z pozostałych obowiązków wynikających z RODO[224].

---

[222] Szerzej na ten temat M. Abu Gholeh, D. Kuźnicka-Błaszkowska, *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych osobowych. Aspekty praktyczne*, Warszawa 2020.

[223] Art. 102 „ust. 1. Prezes Urzędu może nałożyć, w drodze decyzji administracyjnej kary pieniężne w wysokości do 100 000 złotych, na:

1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;

2) instytut badawczy;

3) Narodowy Bank Polski.

Ust. 2. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

Ust. 3. Administracyjne kary pieniężne, o których mowa w ust. 1 i 2, Prezes Urzędu nakłada na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679".

[224] Dla przykładu warto przywołać następujące decyzje organów nadzorczych: decyzja włoskiego organu nadzorczego z 12 listopada 2020 r. w sprawie *Vodafone Italia S.p.A.*, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485681 [dostęp: 5.04.2025]; decyzja francuskiego organu nadzorczego z 18 listopada 2020 r. w sprawie *Carrefour France*, https://www.

5.1. Zasada legalności, rzetelności i przejrzystości przetwarzania

Artykuł 5 ust. 1 lit. a) RODO statuuje zasadę legalności, która przejawia się w tym, że dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"). Aby przetwarzanie danych było zgodne z prawem, administrator musi wykazać odpowiednie przesłanki będące podstawą prawną przetwarzania, a także zapewnić „zgodność z pozostałymi przepisami RODO oraz obowiązującymi ustawami i wydanymi na ich podstawie aktami wykonawczymi"[225]. Przesłanki warunkujące legalność przetwarzania określone zostały w odniesieniu do tzw. danych zwykłych w art. 6 RODO oraz w odniesieniu do szczególnych kategorii danych osobowych w art. 9 RODO. Do przesłanek tych zalicza się m.in. wyrażenie zgody na przetwarzanie danych przez osobę, której dane dotyczą (np. w razie przystąpienia do programu lojalnościowego); niezbędność przetwarzania do wykonania umowy, której stroną jest osoba, której dane dotyczą (np. wskutek zawartej umowa z pracodawcą). Zasada legalności obejmuje swoim zakresem również konieczność uwzględnienia normy art. 8 RODO w przypadku przetwarzania danych dzieci w ramach usług społeczeństwa informacyjnego oraz art. 10 RODO w ramach przetwarzania informacji o wyrokach skazujących.

W praktyce naruszenie zasady zgodności z prawem zostało stwierdzone przez PUODO m.in. w wydanej 31 maja 2022 r. decyzji DKN.5131.51.2021. Administracyjna kara pieniężna w kwocie 10 000 zł została nałożona na Stołeczny Ośrodek dla Osób Nietrzeźwych z siedzibą w Warszawie za naruszenie przepisów art. 6 ust. 1

---

legifrance.gouv.fr/cnil/id/CNILTEXT000042563756 [dostęp: 24.06.2025].

[225] M. Dominiak, M. Gawroński, *Zasady przetwarzania danych osobowych*, [w:] M. Gawroński (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa 2018, s. 93.

w związku z art. 5 ust. 1 lit. a) RODO polegające na nagrywaniu i utrwalaniu dźwięku (głosu) w zainstalowanym w tym ośrodku systemie monitoringu, tj. przetwarzaniu bez podstawy prawnej danych osobowych w tym zakresie. Warto zwrócić uwagę, że nie jest to jedyna kara nałożona przez organ nadzorczy w związku z brakiem podstaw prawnych przetwarzania danych osobowych. Analizując decyzje zarówno polskiego organu nadzorczego, jak i innych organów europejskich, można zauważyć, że jest to jedno z częstszych naruszeń popełnianych przez administratorów. Chociaż co do zasady zarówno podmiot przetwarzający, jak i administrator mogą być podmiotem kary administracyjnej w rozumieniu RODO, to w przypadku braku podstaw prawnych przetwarzania trudno wyobrazić sobie, że kara zostanie nałożona na podmiot przetwarzający. Ten ostatni bowiem dokonuje czynności przetwarzania na zlecenie i w ramach swoistego upoważnienia nadanego przez administratora danych. Podmiot przetwarzający nie ma kompetencji do sprawdzania, czy powierzone mu dane osobowe zostały zebrane w sposób zgodny z prawem. Możliwe jest ukształtowanie takiej odpowiedzialności w ramach umowy powierzenia przetwarzania danych, ale praktyka pokazuje, że administratorzy podchodzą raczej niechętnie do tego typu postanowień.

Zasada zgodności z prawem powinna być interpretowana w sposób szeroki i wymaga, aby cały proces przetwarzania odbywał się zgodnie z obowiązującymi ramami prawnymi (zarówno unijnymi, jak i przepisami prawa krajowego). Nie wystarczy do tego jedynie znalezienie odpowiedniej podstawy prawnej przetwarzania. Kwestia ta powinna być rozpatrywana w znacznie szerszym zakresie, odnosząc się przede wszystkim do spełniania wszystkich warunków materialnych, proceduralnych i formalnych związanych z obowiązkami nałożonymi na administratora i podmiot przetwarzający w RODO[226].

[226] K. Wygoda, *Modyfikacja przesłanek dopuszczalności przetwarzania danych zwykłych w oparciu o art. 6 RODO a działania podmiotów sektora publicznego*, [w:]

Rzetelność to kolejny element składowy procesu przetwarzania danych osobowych, który należy rozumieć nie tylko przez pryzmat należytego wypełniania obowiązków przez administratora, ale także przez pryzmat uczciwości[227]. W tym pierwszym znaczeniu rzetelność przejawia się w starannym wypełnianiu przez administratora obowiązków wynikających z przepisów o ochronie danych osobowych. W znaczeniu drugim rzetelność sprowadza się do etycznego postępowania, tzn. takiego, które nie będzie: wprowadzać w błąd; podstępne; oszukańcze; wykorzystywać trudnej sytuacji, ograniczeń lub przymusowego położenia osoby, której dane dotyczą; sprowadzać się do narzucania uciążliwych warunków przetwarzania danych osobowych z uwagi na silniejszą pozycję administratora[228]. „Wprowadzenie w błąd może polegać m.in. na nieprzekazaniu istotnych informacji, które mogą pozwolić podmiotowi danych na uświadomienie sobie konsekwencji udzielenia zgody na przetwarzanie danych. Działanie podstępne może przejawiać się np. w tym, że administrator ukrywa pewne informacje bądź nadmiernie eksponuje inne w celu osiągnięcia zamierzonego skutku (m.in. uzyskania zgody, niekorzystania z uprawnień), pozbawiając podmiot danych możliwości dokonania całościowej oceny. Działanie w sposób oszukańczy może wiązać się m.in. z wyłudzaniem danych osobowych poprzez składanie obietnic, których administrator nie zamierza dotrzymać. Wykorzystanie trudnej sytuacji lub przymusowego położenia może dotyczyć m.in. prób uzyskania przez administratora zgody od osoby, która wskutek szczególnych okoliczności nie ma pełnej swobody decyzyjnej. Z kolei wykorzystywanie silniejszej pozycji może wiązać się

M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017, s. 33.

[227] P. Fajgielski, *Rzetelność jako ogólna zasada przetwarzania danych osobowych*, „Gdańskie Studia Prawnicze" 2021, nr 4(52), s. 15.

[228] *Ibidem*, s. 16.

z postępowaniem, które opiera się na założeniu, że podmiot danych nie ma możliwości wyboru usług świadczonych przez innego administratora”[229].

Przejrzystość to ostatni ze wskazanych w art. 5 ust. 1 lit. a) RODO elementów składających się na proces przetwarzania danych osobowych. Przejawia się on w zapewnieniu przez administratora, aby wszelkie informacje i komunikaty związane z przetwarzaniem danych osobowych były łatwo dostępne, zrozumiałe oraz sformułowane jasnym i prostym językiem dla osoby, której dane dotyczą[230]. W praktyce kryterium przejrzystości realizowane jest w kontekście wypełniania obowiązków informacyjnych ciążących na administratorze, a także praw osób, których dane dotyczą. Obowiązki, o których mowa, skonkretyzowane zostały w art. 13 i art. 14 RODO[231]. Pierwszy z tych przepisów ma zastosowanie w przypadku zbierania danych od osoby, której dane dotyczą. Z kolei drugi w sytuacji pozyskiwania danych osobowych w sposób inny niż od osoby, które dane dotyczą. Realizacja tych obowiązków następuje w postaci klauzul informacyjnych zawierających w szczególności tożsamość i dane kontaktowe administratora, cele oraz podstawę prawną przetwarzania oraz inne informacje mające zapewnić rzetelność i przejrzystość

---

[229] *Ibidem*, s. 16 i n. Zob. także P. Barta, M. Kawecki, P. Litwiński, *Komentarz do art. 5*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021, Legalis.

[230] Motyw 39 RODO.

[231] Zob. na ten temat: P. Litwiński, *Spełnienie obowiązku informacyjnego*, „ABI Expert” 2016, nr 1, s. 40; M. Gumularz, M. Kawecki, *Prawo do poinformowania w przypadku zbierania danych od osoby, której dane dotyczą*, [w:] B. Fisher, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą, na podstawie rodo*, Wrocław 2017, s. 91 i n.; U. Stańczak, *Prawo do poinformowania w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą*, [w:] B. Fisher, M. Sakowska-Baryła (red.), *op. cit.*, s. 117 i n.; M. Więckowska, *Obowiązek informacyjny*, „ABI Expert” 2018, nr 2, s. 48; S. Kowalski, *Realizacja obowiązku informacyjnego*, „ABI Expert” 2020, nr 3, s. 33.

przetwarzania w stosunku do osoby, której dane dotyczą. Administrator musi jednak pamiętać, że gdy przetwarzanie dotyczy dziecka, to wówczas wszelkie informacje i komunikaty powinny być sformułowane jasnym i prostym językiem, aby dziecko mogło je bez trudu zrozumieć[232]. Kryterium przejrzystości widoczne jest także w kontekście realizacji praw osób, których dane dotyczą, o czym szerzej w rozdziale VIII niniejszego opracowania.

O tym, jak duże znaczenie przypisuje się zasadzie rzetelności i przejrzystości, świadczy m.in. wydana przez PUODO decyzja z dnia 15 marca 2019 r., ZSPR.421.3.2018, stwierdzająca naruszenie przez X. Sp. z o.o. przepisów art. 14 ust. 1–3 RODO, polegające na niepodaniu informacji zawartych w art. 14 ust. 1 i 2 RODO wszystkim osobom fizycznym, których dane osobowe X. Sp. z o. o. przetwarza, prowadzącym aktualnie lub w przeszłości jednoosobową działalność gospodarczą, oraz osobom fizycznym, które zawiesiły wykonywanie tej działalności. W wyniku przeprowadzonego postępowania administracyjnego w niniejszej sprawie PUODO:

1) nakazał X. Sp. z o.o. dopełnić obowiązek podania informacji określonych w art. 14 ust. 1 i 2 RODO osobom fizycznym, których dane osobowe X. Sp. z o. o. przetwarza, prowadzącym aktualnie lub w przeszłości jednoosobową działalność gospodarczą, oraz osobom fizycznym, które zawiesiły wykonywanie tej działalność, którym informacje te nie zostały podane – w terminie trzech miesięcy od dnia doręczenia niniejszej decyzji;
2) nałożył na X. Sp. z o.o., za naruszenie stwierdzone w niniejszej decyzji, administracyjną karę pieniężną w wysokości 943 470,00 złotych.

PUODO podkreślił przy tym, że stwierdzone naruszenie ma poważny charakter, dotyczy bowiem „podstawowych praw i wolności osób, których dane Spółka przetwarza, narusza również podstawową

[232] Motyw 58 RODO.

w odniesieniu do przetwarzania danych osobowych zasadę rzetelności i przejrzystości […]. Odnosząc się do zasady przejrzystości – ustanowionej mocą art. 5 ust. 1 lit. a rozporządzenia 2016/679, zgodnie z którym dane muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą – wskazać trzeba, że ma ona kluczowe znaczenie dla rzetelnego przetwarzania danych osobowych, zwłaszcza w kontekście istotnego rozbudowania mocą przepisów rozporządzenia 2016/679 obowiązków dotyczących informowania podmiotów danych i umożliwienia osobom, których dane dotyczą realizacji ich uprawnień. Jednym z aspektów obowiązków informacyjnych wynikających z zasady przejrzystości jest aspekt formalny dotyczący wykonania obowiązku informacyjnego (w tym z art. 14 rozporządzenia 2016/679) w ogóle, a także wypełnienie tego w odpowiednim czasie i formie. Spełnienie obowiązku informacyjnego zgodnie z zasadą przejrzystości ma na celu uświadomienie osobom, których dane dotyczą ryzyk, zasad, zabezpieczeń, i praw związanych z przetwarzaniem danych osobowych oraz sposobów wykonania praw związanych z przetwarzaniem”[233].

5.2. Zasada celowości

Zasada celowości wyrażona została w art. 5 ust. 1 lit. b) RODO. Zgodnie z treścią tego przepisu dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne

[233] Decyzja PUODO z dnia 15 marca 2019 r., ZSPR.421.3.2018. Decyzja dostępna na stronie https://uodo.gov.pl/decyzje/ZSPR.421.3.2018 [dostęp: 24.06.2025].

z pierwotnymi celami („ograniczenie celu")[234]. W praktyce zastosowanie tej zasady (tzw. zasady celowości) wymaga od administratora wykazania, że cel (cele) przetwarzania danych osobowych jest **konkretny** (a więc faktycznie istniejący, realny i jednoznacznie określony), **wyraźny** (czyli zrozumiały dla osoby, której dane dotyczą) i **prawnie uzasadniony** (tzn. mający podstawę prawną). Przetwarzanie więc przez administratora danych osobowych może nastąpić np. w celu zawarcia umowy i ewentualnego dochodzenia roszczeń; do celów marketingu bezpośredniego; w celu przyszłych procesów rekrutacyjnych; w celu dostarczenia newslettera. Obowiązkiem administratora jest zatem wskazanie wszystkich celów przetwarzania. Ich oznaczenie będące wyrazem realizacji zasady celowości pozostaje w bezpośrednim związku z zasadą ograniczonego przechowywania, zasadą minimalizacji danych oraz zasadą legalności. Ponadto służy wypełnieniu obowiązków informacyjnych, o których mowa w art. 13 i 14 RODO. **Odnosząc się do zasady celowości, należy podkreślić, że prawodawca unijny dopuszcza pewne wyjątki od tej zasady**. Polegają one na możliwości dalszego przetwarzania danych osobowych do celów innych niż cele, dla których dane te zostały pierwotnie zebrane, pod warunkiem że służą one do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Przy czym przetwarzanie w wyżej wymienionych celach podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona zrealizować powyższe cele. Jeżeli cele te można zrealizować w drodze dalszego przetwarzania

[234] Zob. J. Byrski, H. Hoser, *Ocena celowości przetwarzania danych osobowych*, „ABI Expert" 2020, nr 3, s. 22 i n.

danych, które nie pozwalają albo przestały pozwalać na zidentyfikowanie osoby, której dane dotyczą, cele należy realizować w ten sposób[235]. Poza wskazanymi wyżej rozwiązaniami należy wziąć pod uwagę także te przyjęte na gruncie art. 6 ust. 4 RODO. Przewidują one bowiem możliwość przetwarzania danych w celu innym niż cel, w którym dane osobowe zostały zebrane, pod warunkiem że odbywa się ono na podstawie zgody osoby, której dane dotyczą, albo prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1 RODO.

5.3. Zasada minimalizacji danych

Zasadę minimalizacji danych wyraża treść art. 5 ust. 1 lit. c). W myśl tego przepisu dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"). Jak wynika z treści tego przepisu, wyrażona w nim zasada wprowadza kryteria limitacyjne, które ograniczają zbieranie i dalsze przetwarzanie danych osobowych[236]. W konsekwencji oznacza to, że dane osobowe powinny być przetwarzane przez administratora tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami[237]. Wspomniane wyżej kryteria limitacyjne to **adekwatność, stosowność i niezbędność**. W orzecznictwie sądów administracyjnych określenie „«adekwatne» oznacza odpowiednie, zgodne, proporcjonalne, nienadmierne i może być traktowane jako synonim słowa «stosowne». **Adekwatność i stosowność**

[235] Art. 89 ust. 1 RODO.
[236] Wyrok WSA w Warszawie z dnia 19 kwietnia 2022 r., II SA/Wa 2259/21.
[237] Motyw 39 RODO.

rozumieć można jako konieczność zachowania odpowiednich proporcji zakresu danych do celów przetwarzania i przetwarzanie tylko takich danych, które są potrzebne dla realizacji określonych celów"[238]. Z kolei „**wymóg niezbędności** należy odczytywać łącznie z wymogiem adekwatności i stosowności, co powinno pozwolić na uwzględnienie okoliczności i dopuszczenie przetwarzania danych, które w istotny sposób mogą pomóc osiągnąć cele przetwarzania"[239]. W prezentowanym ujęciu nie mamy więc do czynienia z przyznaniem prymatu minimalizacji kosztem adekwatności. Wskazane wyżej wymogi poddawane są bowiem łącznej ocenie, co – jak podkreśla się w literaturze i orzecznictwie – pozwala na przetwarzanie danych osobowych „w nieco szerszym zakresie, niż tylko […] konieczne minimum, pod warunkiem że przetwarzane dane mają ścisły związek z realizację celu (np. ułatwiają jego osiągnięcie)"[240]. W praktyce zastosowanie tej zasady wymaga podjęcia przez administratora odpowiednich działań zarówno w fazie projektowania (*privacy by design*), jak i domyślnej ochrony danych osobowych (*privacy by default*)[241]. Nie zawsze jednak wdrożenie przez administratora pewnych rozwiązań – w tym przypadku – w kontekście zasady minimalizacji danych będzie akceptowane przez PUODO. Przykładem takiego stanu jest sprawa, w której WSA w Warszawie nie podzielił stanowiska organu nadzorczego, że przetwarzanie przez szkołę podstawową danych biometrycz-

---

[238] Wyrok WSA w Warszawie z dnia 19 kwietnia 2022 r., II SA/Wa 2259/21.

[239] *Ibidem*.

[240] *Ibidem*. Zob. P. Fajgielski, *Komentarz do art. 5*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa 2022, Lex; P. Barta, M. Kawecki, P. Litwiński, *Komentarz do art. 5…*

[241] Zob. na ten temat: M. Jabłoński, J. Węgrzyn, *Zmiana modelu ochrony danych osobowych – podejście oparte na ryzyku, privacy by design i privacy by default*, [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *op. cit.*, s. 75 i n.; T. Ochocki, *Mechanizmy domyślnej ochrony danych w fazie projektowania*, „ABI Expert" 2020, nr 3, s. 30 i n.

nych uczniów (tj. odcisków palców dzieci w celu ich identyfikacji podczas korzystania przez nie z usług stołówki szkolnej) jest niezgodne z zasadą minimalizacji danych. W konsekwencji Sąd uchylił decyzję PUODO nakładającą na szkołę karę pieniężną w wysokości 20 000 złotych[242]. Stanowisko WSA w Warszawie zostało podtrzymane przez NSA, który w nawiązaniu do motywu 39 RODO podkreślił, że „realizacja przedmiotowej zasady wymaga «w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu». Z powyższego fragmentu motywu 39 RODO wynika kilka wniosków. Po pierwsze, zasada minimalizacji danych limituje okres przetwarzania danych wyłącznie do czasu, w którym jest to niezbędne dla celu tego przetwarzania. Po drugie, rozstrzyga o dopuszczalności przetwarzania danych osobowych wyłącznie w takich układach, w których nie da się podać innych rozsądnych sposobów osiągnięcia celu tego przetwarzania. Prawodawca unijny nie dookreślił, co należy rozumieć przez inną niż przetwarzanie danych osobowych rozsądną alternatywę osiągnięcia celu przetwarzania. W ocenie Naczelnego Sądu Administracyjnego chodzi tu o wskazanie takich działań, które bez konieczności przetwarzania danych osobowych pozwolą osiągnąć określony cel, a jednocześnie nie generują zasadniczo wyższych «kosztów» materiałowych, finansowych, czasowych i osobowych od tych, jakie należałoby ponieść,

[242] Wyrok WSA w Warszawie z dnia 7 sierpnia 2020 r., II SA/Wa 809/20. Odnośnie do zasady minimalizacji danych zob. także wyrok NSA z dnia 11 stycznia 2023 r., III OSK 6317/21; wyrok WSA w Warszawie z dnia 2 sierpnia 2022 r., II SA/Wa 3687/21.

gdyby do realizacji tego celu doszło poprzez przetwarzanie danych osobowych. W istocie chodzi więc o skonfrontowanie wielkości szeroko ujętych kosztów dwóch trybów osiągnięcia tego samego celu: trybu uwzględniającego przetwarzanie danych osobowych i trybu, który takiego przetwarzania nie uwzględnia. W tej pespektywie zasada minimalizacji danych zobowiązuje zatem do tego, aby nie dochodziło do przetwarzania danych osobowych w tych skonfigurowaniach, w których cel, dla którego to przetwarzanie miało być prowadzone, z wykorzystaniem porównywalnych zasobów, można osiągnąć bez przetwarzania danych osobowych. Po trzecie, zasadę minimalizacji danych należy rozumieć również w ten sposób, że jeżeli nie można osiągnąć założonego celu bez przetwarzania danych osobowych, to dane, które podlegają przetwarzaniu muszą być do tego celu adekwatne, stosowne i ograniczone. W tym ujęciu zasada minimalizacji danych wprowadza swego rodzaju rygor proporcjonalności przetwarzania danych. Chodzi więc o to: 1) aby administrator pozyskał wyłącznie taki rodzaj danych osobowych, których przetworzenie jest niezbędne do osiągnięcia celu przetwarzania; 2) aby administrator pozyskał dane osobowe w minimalnej wystarczającej ilości dla osiągnięcia celu przetwarzania; 3) aby administrator przetwarzał je wyłącznie w taki sposób, który jest niezbędny do osiągnięcia celu przetwarzania; 4) aby administrator przetwarzał dane osobowe wyłącznie przez czas niezbędny do osiągnięcia celu przetwarzania.

Uwzględnienie przyjętych założeń uzasadnia wniosek, że zasada minimalizacji danych dopuszcza przetwarzanie danych osobowych wyłącznie wtedy, gdy jest to niezbędne do osiągnięcia celu przetwarzania i wyłącznie w zakresie, w ilości, w sposób i przez czas, jakie są niezbędne do osiągnięcia celu przetwarzania”[243].

[243] Wyrok NSA z dnia 10 października 2024 r., II OSK 4804/21.

5.4. Zasada prawidłowości

Zasadę prawidłowości, nazywaną także zasadą merytorycznej poprawności[244], reguluje art. 5 ust. 1 lit. d) RODO. Zgodnie z treścią tego przepisu dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość"). Prawidłowa realizacja tej zasady wymaga więc od administratora podjęcia czynności usunięcia lub sprostowania danych w sytuacji, gdy osoba, której dane dotyczą, wystąpi ze skutecznym żądaniem lub administrator będzie w posiadaniu prawdziwych informacji, które samodzielnie pozyskał (np. z zewnętrznych źródeł)[245]. Innymi słowy, **„merytorycznie poprawne przetwarzanie danych osobowych to [...] takie, które pozostaje w zgodzie z rzeczywistością i jest treściowo właściwe"**[246]. Aby jednak możliwe było przypisanie administratorowi faktu nierzetelnego przetwarzania danych osobowych, konieczne jest ustalenie w wyczerpujący sposób stanu faktycznego danej sprawy, a mianowicie tego:

- czy administrator „przetwarza konkretne dane osobowe (czy jest w ich posiadaniu);
- czy dane osobowe są przetwarzane prawidłowo (m.in. czy są aktualne);
- czy zaistniała potrzeba uaktualnienia danych, a administrator danych zignorował tę potrzebę.

Dopiero łączne spełnienie wszystkich powyższych przesłanek umożliwi organowi uznanie, że administrator danych osobowych

---

[244] P. Drobek, *Komentarz do art. 5*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 339.

[245] A. Nerka, *Komentarz do art. 5*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 146.

[246] Wyrok NSA z dnia 7 sierpnia 2008 r., I OSK 1218/07.

nie podołał obowiązkowi”[247] przestrzegania zasady prawidłowości. Do wniosku takiego doszedł WSA w Warszawie, rozpatrując skargę kancelarii od decyzji PUODO na naruszenie m.in. art. 5 ust. 1 lit. d) RODO „poprzez jego błędną wykładnię wyrażającą się w uznaniu naruszenia zasady prawidłowości danych w związku z posiadaniem przez kancelarię […] nieaktualnych danych, podczas gdy treść i prawidłowa wykładnia ww. przepisu nie zakłada bezwzględnego posiadania prawidłowych danych, a nakazuje podejmowanie czynności «w miarę potrzeby» i poprawianie danych”[248]. Odnosząc się do

[247] Wyrok WSA w Warszawie z dnia 16 listopada 2021 r., II SA/Wa 1489/21.

[248] *Ibidem*. W niniejszej sprawie chodziło o przesłanie przez kancelarię formularza PIT-11 na niewłaściwy adres. W ocenie WSA w Warszawie Prezes Urzędu Ochrony Danych Osobowych nie przedstawił dowodów na spełnienie wskazanych wyżej przesłanek. „Przede wszystkim z uzasadnienia skarżonej decyzji nie wynika to, czy skarżący posiadał w ogóle adres korespondencyjny osoby inicjującej przedmiotowe postępowanie – przed wysłaniem spornego dokumentu PIT-11. W tym zakresie organ przywołał jedynie oświadczenie spółki, że z uwagi na brak kontaktu z A. T., uzyskano jej adres z systemu teleinformatycznego. Przywołał też oświadczenie samej A. T. o tym, że adresu na który wysłano pierwotnie PIT-11 nigdy nie podawała stronie i nigdy pod nim nie mieszkała. Należy zauważyć, że takie stwierdzenia jak wyżej, nie zawierają jednoznacznej informacji. Może bowiem sugerować, iż spółka weszła w posiadanie adresu A. T. dopiero z chwilą ich ustalenia w owym systemie. Mimo tego organ nie dochowując należytej staranności nie ustalił tego, czy spółka dysponowała spornym adresem jeszcze przed sięgnięciem do systemu teleinformatycznego. Nadto, co również wielce istotne, organ nie ustalił tego o jakim systemie teleinformatyczny jest mowa (czy był to wewnętrzny system spółki czy np., system PESEL lub jeszcze inny). Zwrócić należało także organowi uwagę na to, iż w sposób nieuprawniony zdaje się zrównywać pojęcie «nieprawidłowego adresu» i «adresu nieaktualnego» pomijając fakt, że oba w/w pojęcia nie tworzą jednakowych zbiorów znaczeniowych. Adres nieprawidłowy, może być bowiem nie tylko adresem nieaktualnym, ale także adresem nie wynikającym z żadnych dokumentów (np. wymyślonym przez pracownika administratora danych). W realiach niniejszej sprawy powyższe rozróżnienie ma bardzo istotne znaczenie w sytuacji gdy organ nie ustalił tego, czy spółka dysponowała spornym adresem przed wysłaniem na niego dokumentu PIT-11 i czy w chwili dokonania kwestionowanej wysyłki adres ten był już nieaktualny czy nieistniejący w dokumentacji. Brak szczegółowych ustaleń powyższych faktów sprawia, że jako przedwczesne jawią się wnioski organu o przetwarzaniu przez spółkę danych osobowych A. T. z naruszeniem omawianych przepisów RODO. Nadto brak wskazanych ustaleń powoduje, że w chwili obecnej

zasady prawidłowości, warto zwrócić także uwagę na decyzję PUODO z dnia 9 grudnia 2020 r., DKN.5131.5.2020, nakładającą na TUiR WARTA S.A. karę pieniężną w wysokości 85 588 złotych. W niniejszej sprawie naruszenie polegało na wysłaniu przez agenta ubezpieczeniowego na wskazany przez klienta nieprawidłowy adres e-mail polisy zawierającej dane osobowe do nieuprawnionego adresata. Jak podkreślił PUODO, „administrator danych dopuszczający możliwość wykorzystania do komunikacji z klientem pocztę elektroniczną powinien mieć świadomość ryzyk związanych np. z nieprawidłowym podaniem przez klienta adresu poczty elektronicznej i w celu ich minimalizacji przedsięwziąć odpowiednie środki organizacyjne i techniczne, jak np. weryfikacja podanego adresu, czy też szyfrowanie przesyłanych w ten sposób dokumentów”[249].

5.5. Zasada ograniczonego czasu przechowywania

Zasada, o której mowa, wyrażona została w art. 5 ust. 1 lit. e) RODO, który stanowi, że 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolno-

nie sposób rzetelnie ocenić tego, czy po stronie spółki – przed wysłaniem dokumentu PIT-11 na kwestionowany adres – zaistniała uzasadniona potrzeba uaktualnienia tego adresu”. W związku z powyższym Sąd uchylił pkt 1 zaskarżonej decyzji.

[249] Decyzja PUODO z dnia 9 grudnia 2020 r., DKN.5131.5.2020. Decyzja dostępna na stronie: https://uodo.gov.pl/decyzje/DKN.5131.5.2020 [dostęp: 24.06.2025].

ści osób, których dane dotyczą („ograniczenie przechowywania"). Jak wynika z treści tego przepisu, **czas przechowywania danych osobowych uwarunkowany jest celem przetwarzania**. Aby więc „zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu"[250]. Terminy te administrator określa na podstawie przepisów prawa lub w przypadku ich braku według własnej oceny. I tak na przykład, art. 5c ustawy o radcach prawnych[251] statuuje okres przechowywania danych osobowych przez radców prawnych w ramach wykonywania zawodu. Okres ten wynosi odpowiednio 5, 10 lub 15 lat[252]. Po jego upływie dane osobowe ulegają usunięciu. W przy-

---

[250] Motyw 39 RODO.

[251] Ustawa z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz. U. z 2024 r. poz. 499).

[252] Art. 5c ustawy o radcach prawnych stanowi:

„Ust. 1. Okres przechowywania danych osobowych wynosi:

1) 5 lat od końca roku, w którym zakończyło się postępowanie, w którym dane osobowe zostały zgromadzone – w przypadku danych osobowych przetwarzanych przez organy samorządu radców prawnych w zakresie niezbędnym do prawidłowej realizacji zadań publicznych określonych w ustawie oraz danych osobowych przetwarzanych w ramach nadzoru nad działalnością samorządu radców prawnych;

2) 10 lat od końca roku, w którym zakończyło się postępowanie, w którym dane osobowe zostały zgromadzone – w przypadku danych osobowych przetwarzanych:

a) w toku prowadzonych przez organy samorządu radców prawnych postępowań:

– administracyjnych,

– w zakresie skarg i wniosków,

– innych przewidzianych przez ustawę lub wydane na podstawie ustawy akty prawne organów samorządu radców prawnych dotyczących radców prawnych, aplikantów radcowskich lub osób ubiegających się o wpis na listę radców prawnych lub listę aplikantów radcowskich, a także osób przystępujących do egzaminu wstępnego na aplikację radcowską i egzaminu radcowskiego,

b) w ramach nadzoru nad tymi postępowaniami, o których mowa w lit. a,

c) przez radców prawnych w ramach wykonywania zawodu;

3) 15 lat od końca roku, w którym zakończyło się postępowanie, w którym dane osobowe zostały zgromadzone – w przypadku danych osobowych przetwarzanych w toku prowadzonych przez organy samorządu radców prawnych postępowań dyscyplinarnych wobec radców prawnych i aplikantów radcowskich oraz podczas

padku zaś danych przekazanych administratorowi (np. potencjalnemu pracodawcy) na potrzeby przyszłych procesów rekrutacji okres przechowywania danych osoby ubiegającej się o zatrudnienie poza procesem rekrutacji zależy od oceny administratora. Może on być np. nie dłuższy niż 12 miesięcy. **Od zasady czasowości (ograniczenia przechowywania) prawodawca unijny dopuścił wyjątki, co potwierdza treść wskazanego wyżej art. 5 ust. 1 lit. e)**. Mianowicie administrator może przechowywać dane osobowe przez dłuższy okres, jeżeli będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. A ponadto wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO. Jednym z takich środków może być pseudonimizacja, tzn. przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej[253]. Odnosząc się do zasady czasowości, należy także podkreślić, że ma ona ścisły związek z obowiązkiem informacyjnym (art. 13 i 14 RODO) oraz obowiązkiem prowadzenia czynności przetwarzania danych osobowych (art. 30 ust. 1 lit. f) RODO). W praktyce konsekwencją naruszenia tej zasady może być nałożenie przez PUODO administracyjnej kary pieniężnej. Tak było w rozpatrywanej przez

wykonywania przewidzianych przez ustawę kompetencji nadzorczych nad postępowaniami dyscyplinarnymi w sprawach radców prawnych i aplikantów radcowskich.

Ust. 2. Po upływie okresów, o których mowa w ust. 1, w przypadku danych osobowych przetwarzanych przez radców prawnych w ramach wykonywania zawodu, dane osobowe ulegają usunięciu".

[253] Art. 4 pkt 5 RODO. Na temat pseudonimizacji zob. M. Kołodziej, *Pseudonimizacja w RODO – kiedy i jak stosować?*, „ABI Expert" 2018, nr 2, s. 44 i n. M. Kogut-Czarkowska, *Pseudonimizacja i anonimizacja danych osobowych w badaniach naukowych – wybrane zagadnienia*, „Prawo Nowych Technologii" 2021, nr 1, s. 10 i n.

WSA w Warszawie sprawy ze skargi uczelni na decyzję PUODO nakładającą na ten podmiot karę pieniężną w wysokości 50 000 złotych za naruszenie m.in. art. 5 ust. 1 lit. e-f) i art. 5 ust. 2 RODO[254]. W niniejszej sprawie naruszenie ochrony danych kandydatów na studia związane było z kradzieżą przenośnego prywatnego komputera pracownika. Skradziony laptop używany było zarówno do celów prywatnych, jak i służbowych, w tym również do przetwarzania danych osobowych kandydatów na studia na potrzeby czynności rekrutacyjnych w ramach pełnionej przez tego pracownika funkcji sekretarza Uczelnianej Komisji Rekrutacyjnej. Zgromadzony w sprawie materiał dowodowy wskazał, że uczelnia nie dokonała oceny ryzyka w zakresie możliwości naruszenia zasady poufności danych osobowych (art. 5 ust. 1 lit. f) RODO) czy zasady ograniczenia przechowywana danych (art. 5 ust. 1 lit. e) RODO), wynikającego z zagrożenia, jakim jest możliwość eksponowania z systemu SOK (System Obsługi Kandydatów) szerokiego zakresu kategorii danych na nośnik zewnętrzny. Odnośnie do czasu trwania naruszeń wskazano, że sekretarz Uczelnianej Komisji Rekrutacyjnej przechowywał dane osobowe kandydatów na studia przez okres dłuższy, aniżeli było to konieczne. Dane pochodziły bowiem z okresu ostatnich 5 lat rekrutacji, co było niezgodne z wyznaczonym okresem przechowywania tych danych osobowych, który został określony na 3 miesiące od zakończenia rekrutacji. Mając powyższe na względzie, WSA w Warszawie podzielił stanowisko PUODO.

5.6. Zasada integralności i poufności

Zasada integralności i poufności została wyrażona w art. 5 ust. 1 lit. f) RODO, który stanowi: dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych

[254] Wyrok WSA w Warszawie z dnia 13 maja 2021 r., II SA/Wa 2129/20.

osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność"). Jak wynika z treści zacytowanego przepisu, prawodawca unijny odniósł się w nim do dwóch kluczowych cech bezpieczeństwa informacji, tj. integralności i poufności. **Integralność danych** to cecha, która przejawia się w zagwarantowaniu tego, że przetwarzane dane będą prawdziwe i zabezpieczone przed ich nieupoważnionym przekształceniem, usunięciem lub dodaniem. Z kolei **poufność** to cecha zapewniająca, że dostęp do przetwarzanych danych mają wyłącznie osoby uprawnione. W praktyce realizacja tej zasady nakłada na administratora obowiązek uwzględnienia stanu wiedzy technicznej, kosztów wdrożenia oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, w celu wdrożenia odpowiednich środków technicznych i organizacyjnych, które są konieczne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku[255], w tym m.in. w stosownym przypadku:

[255] „RODO wprowadziło podejście, w którym zarządzanie ryzykiem jest fundamentem działań związanych z ochroną danych osobowych i ma charakter ciągłego procesu. Podmioty przetwarzające dane osobowe zobligowane są nie tylko do zapewnienia zgodności z wytycznymi ww. rozporządzenia poprzez jednorazowe wdrożenie organizacyjnych i technicznych środków bezpieczeństwa, ale również do zapewnienia ciągłości monitorowania poziomu zagrożeń oraz zapewnienia rozliczalności w zakresie poziomu oraz adekwatności wprowadzonych zabezpieczeń. Oznacza to, że koniecznością staje się możliwość udowodnienia przed organem nadzorczym, że wprowadzone rozwiązania, mające na celu zapewnienie bezpieczeństwa danych osobowych, są adekwatne do poziomu ryzyka, jak również uwzględniają charakter danej organizacji oraz wykorzystywanych mechanizmów przetwarzania danych osobowych. Konsekwencją takiej orientacji jest rezygnacja z list wymagań, w zakresie bezpieczeństwa narzuconych przez prawodawcę, na rzecz samodzielnego doboru zabezpieczeń w oparciu o analizę zagrożeń. Administratorom nie wskazuje się konkretnych środków i procedur w zakresie bezpieczeństwa. Administrator samodzielnie ma przeprowadzić szczegółową analizę

a) pseudonimizację i szyfrowanie danych osobowych;
b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania[256].

Należy przy tym podkreślić, że administrator, dokonując oceny, czy stopień bezpieczeństwa jest odpowiedni, musi uwzględnić w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych[257]. Praktyka pokazuje, że również i art. 5 ust. 1 lit. f) RODO jest przedmiotem analizy spraw rozpatrywanych przez PUODO oraz sądy administracyjne. Przykładem jest decyzja PUODO nakładająca na Burmistrza Aleksandrowa Kujawskiego karę pieniężną w wysokości 40 000 złotych za naruszenie m.in.:

– art. 5 ust. 1 lit. f) w związku z art. 5 ust. 2 RODO, tj. zasady integralności i poufności, zasady prawidłowości oraz art. 24 RODO poprzez nieprzeprowadzenie analizy ryzyka związanego z korzystaniem przez burmistrza z kanału YouTube w celu transmisji nagrań z obrad Rady Miasta Aleksandrowa Kujawskiego;

---

prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka" (wyrok WSA w Warszawie z dnia 3 września 2020 r., II SA/Wa 2559/19).

[256] Art. 35 ust. 1 RODO.

[257] Art. 35 ust. 2 RODO.

– art. 5 ust. 1 lit. f) w związku z art. 5 ust. 2 RODO, tj. zasady integralności i poufności oraz art. 32 RODO poprzez **niewdrożenie odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie danych osób fizycznych w związku z przechowywaniem nagrań sesji Rady Miasta Aleksandrowa Kujawskiego wyłącznie na serwerach YouTube, bez wykonywania i przechowywania kopii zapasowych tych nagrań w zasobach własnych Urzędu Miejskiego w Aleksandrowie Kujawskim**[258].

5.7. Zasada rozliczalności

Zgodnie z treścią art. 5 ust. 2 RODO administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność"). W praktyce realizacja tej zasady wymaga od administratora:

1) „wdrożenia środków (w tym wewnętrznych procedur) gwarantujących przestrzeganie przepisów o ochronie danych osobowych w związku z operacjami ich przetwarzania;
2) […] sporządzenia dokumentacji, która wskazuje osobom, których dane dotyczą oraz organom nadzorczym, jakie środki podjęto, aby zapewnić przestrzeganie przepisów o ochronie danych osobowych"[259].

Dokumentacja, o której mowa, obejmuje wdrożoną w danej organizacji procedurę ochrony danych osobowych, na którą składają się przyjęte np. polityki, regulaminy, instrukcje, dotyczące m.in.:

---

[258] Decyzja PUODO z dnia 18 października 2019 r., ZSPU.421.3.2019, https://uodo.gov.pl/decyzje/ZSPU.421.3.2019 [dostęp: 24.06.2025].

[259] P. Barta, M. Kawecki, P. Litwiński, *Komentarz do art. 5*… Zob. także P. Siemieniak, *Wymagania dokumentacyjne przetwarzania danych*, „ABI Expert" 2017, nr 2, s. 29 i n.

- realizacji praw osób, których dane dotyczą;
- prowadzonego w sposób prawidłowy i rzetelny rejestru czynności przetwarzania danych[260];
- przeprowadzonej analizy ryzyka[261];
- przeprowadzonej oceny skutków dla ochrony danych[262];
- wyznaczenia inspektora ochrony danych;
- odbytych szkoleń z zakresu ochrony danych osobowych;
- przeprowadzonych audytów ochrony danych osobowych.

Odnosząc się do zasady rozliczalności, należy podkreślić, że była ona przedmiotem zainteresowania zarówno PUODO[263], jak i sądów administracyjnych. W rozpatrywanej przez WSA w Warszawie sprawie ze skargi C. sp. z o.o. na decyzję PUODO nakładającą na ten

---

[260] Zob. na ten temat M. Więckowska, *RODOwskaz prowadzenia rejestru czynności przetwarzania*, „ABI Expert" 2017, nr 3, s. 48.

[261] Zob. na ten temat A. Kaczmarek, A. Łapińska, A. Miłocha, M. Młotkiewicz, *Nowa optyka w ocenie ryzyka*, „ABI Expert" 2017, nr 4, s. 24.

[262] Zob. na ten temat M. Więckowska, *Przewodnik po ocenie skutków dla ochrony danych*, „ABI Expert" 2017, nr 1, s. 48.

[263] Na przykład wskazana już wcześniej decyzja PUODO nakładająca na Burmistrza Aleksandrowa Kujawskiego karę pieniężną w wysokości 40. 000 złotych za naruszenie m.in.:

– „art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych, tj. zasady rozliczalności, oraz art. 30 ust. 1 lit. d) oraz f) ogólnego rozporządzenia o ochronie danych poprzez niewskazanie w rejestrze czynności przetwarzania danych osobowych, dla czynności związanych z publikacją informacji na stronie Biuletynu Informacji Publicznej Urzędu Miasta w Aleksandrowie Kujawskim, wszystkich odbiorców danych oraz niewskazanie dla tych czynności przetwarzania planowanego terminu usunięcia danych w sposób zapewniający przetwarzanie danych zgodnie z zasadą ograniczonego przechowywania", decyzja PUODO z dnia 18 października 2019 r., ZSPU.421.3.2019.

Na zasadę rozliczalności, tyle że w kontekście realizacji obowiązku informacyjnego wynikającego z art. 14 RODO, zwrócił uwagę PUODO w decyzji z dnia 15 marca 2019 r., ZSPR.421.3.2018, wskazując, że z „przepisu tego nie wynika, żeby prawodawca nałożył na administratora obowiązek wysyłania takiej informacji np. przesyłką poleconą, byleby tylko administrator mógł stosownymi dowodami wykazać, że ów obowiązek informacyjny został przez niego spełniony wobec podmiotów, których dane osobowe przetwarza". Zob. także decyzję PUODO z dnia 23 czerwca 2022 r., DKN.5131.11.2022.

podmiot karę pieniężną w wysokości 201 559,50 złotych za naruszenie przepisów RODO – w tym zasad ochrony danych osobowych wyrażonych w art. 5 – sąd ten podkreślił, że „podstawową zasadą przetwarzania danych osobowych jest zasada rozliczalności określona w art. 5 ust. 2 rozporządzenia. […]. Zasada rozliczalności bazuje […] na prawnej odpowiedzialności administratora za właściwe wypełnianie obowiązków i nakłada na niego obowiązek wykazania zarówno przed organem nadzorczym, jak i przed podmiotem danych, dowodów na przestrzeganie wszystkich zasad przetwarzania danych”[264]. Dlatego też realizacja zasady rozliczalności, np. w kontekście pierwszej z wymienionych wyżej zasad, tj. zasady legalności, rzetelności i przejrzystości przetwarzania, sprowadzać się będzie do wykazania zgody osoby, której dane dotyczą (o ile podstawą przetwarzania jest przesłanka zgody), wyrażonej w formie pisemnej lub elektronicznej. „Rozliczalność zasady rzetelności zrealizować można poprzez pieczołowite i powtarzalne zbieranie dowodów, z których wynika, że zasada rzetelności jest realizowana. Jeśli obowiązek informacyjny realizowany jest na stronie WWW widocznej po zalogowaniu, to można wprowadzić np. przycisk ekranowy o treści „przeczytałem…” lub podobnej i fakt użycia tego przycisku odnotować w bazie danych. Można zbierać pokwitowania, zwłaszcza jeśli i tak się jakieś oświadczenia pisemne odbiera, wreszcie należy odnotować w polityce ochrony danych sposób realizacji zasady rzetelności. Należy również odnotowywać odpowiedzi na pytania zadawane w zakresie uprawnień kontrolnych z art. 15”[265] RODO. W ten sam

[264] Wyrok WSA w Warszawie z dnia 10 lutego 2021 r., II SA/Wa 2378/20. Zob. także wyrok WSA w Warszawie z dnia 26 sierpnia 2020 r., II SA/Wa 2826/19.

[265] J. Rzymowski, *Zasada rozliczalności w RODO*, „ABI Expert” 2018, nr 1, s. 39. Zob. także S. Stefaniak, H. Suszek-Borowska, *Rozliczalność przetwarzania danych a systemy informatyczne*, „ABI Expert” 2018, nr 2, s. 22 i n. W praktyce wskazuje się, że „w kontekście zapewnienia rozliczalności pewnym standardem powinny się stać odpowiednie narzędzia, które zapewniają m.in.:

– kontrolę w zakresie utrzymania wiarygodnego rejestru czynności przetwa-

sposób realizowana jest także rozliczalność zasady przejrzystości. Ważne zatem w tym przypadku jest, aby administrator był w stanie wykazać transparentność informacji i komunikatów kierowanych do osoby, której dane dotyczą. Rozliczalność zaś pozostałych zasad ochrony danych realizowana jest przez właściwe i rzetelne wypełnianie rejestru czynności przetwarzania danych i/lub prowadzenie uzupełniającej dokumentacji, takiej jak np. dokumentacja dotycząca realizacji praw osób, których dane dotyczą, dokumentacja dotycząca nadanych upoważnień do przetwarzania danych (w przypadku zasady integralności)[266].

rzania, przeprowadzonych analiz i podjętych decyzji oraz ich historycznych wersji;

– zarządzanie dostępem do analiz i dokumentacji;

– zachowanie spójności dokumentacji;

– zarządzanie relacjami z podmiotami zewnętrznymi, którym przekazywane są dane, oraz procesem realizacji praw podmiotów danych;

– zastosowanie metodyk, które zapewnią powtarzalność i automatyzację procesu oceny skutków dla ochrony danych i reakcji na incydenty" (Sz. Grabski, *Rozliczalność, czyli dlaczego nie można zapomnieć o RODO*, „ABI Expert" 2020, nr 1, s. 28).

[266] J. Rzymowski, *op. cit.*, s. 40 i n.

Rozdział VI

Obowiązki administratora i podmiotu przetwarzającego

6.1. Podstawowe obowiązki administratora

RODO w znaczny sposób zmieniło podejście do ochrony danych osobowych – z ochrony reaktywnej na ochronę aktywną, wprowadzając model, w którym na administratorze danych leży szereg obowiązków, w tym przede wszystkim ocena ryzyka związanego z przetwarzaniem i wdrożenie regulacji zapewniających zgodność przetwarzania z przepisami o ochronie danych[267]. Obowiązki administratora na gruncie RODO bezpośrednio korelują z uprawnieniami osób, których dane dotyczą. Część z kluczowych obowiązków ADO została już omówiona w rozdziale dotyczącym zasad ochrony danych osobowych, inne z kolei będą w sposób bardziej szczegółowy omówione w rozdziałach dotyczących systemowego zarządzania bezpieczeństwem informacji i realizacji praw podmiotów danych. Niemniej spośród najważniejszych obowiązków administratora można wymienić:

– zapewnienie tego, że przetwarzanie jest zgodne z prawem (posiadanie podstaw prawnych do przetwarzania danych osobowych) – art. 6 i 9 RODO, szerzej omówione w rozdziale piątym;

---

[267] M. Ganczar, A. Sytek, *Jednostki samorządu terytorialnego wobec ogólnego rozporządzenia o ochronie danych (RODO)*, [w:] B. Dolnicki (red.), *Źródła prawa w samorządzie terytorialnym*, Warszawa 2018, s. 262.

- wykonanie obowiązku informacyjnego wobec osób, których dane dotyczą – art. 13, 14 RODO, szerzej omówione w rozdziale ósmym;
- rozpatrywanie żądań osób, których dane dotyczą, wykonanie przysługujących im praw (dostępu, usunięcia, sprzeciw itp.) – art. 15–23 RODO, szerzej omówione w rozdziale ósmym;
- wyznaczenie przedstawiciela w Unii Europejskiej (dla podmiotów mających siedzibę poza Unią Europejską) – art. 27; dotyczy to w sytuacji, kiedy RODO ma zastosowanie do podmiotu mającego swoją siedzibę poza terytorium Unii Europejskiej i nakłada na takiego administratora obowiązek wyznaczenia swojego przedstawiciela w jednym z krajów UE (za wyjątkiem sytuacji, w której przetwarzanie ma charakter sporadyczny, nie dotyczy szczególnych kategorii danych osobowych lub danych dotyczących wyroków skazujących i jest mało prawdopodobne, że dojdzie do naruszenia praw i wolności);
- weryfikacja środków bezpieczeństwa stosowanych przez procesora oraz zawarcie z nim umowy powierzenia – art. 28 RODO, szerzej omówiony w rozdziale VI pkt 6.2;
- nadawanie upoważnień do przetwarzania danych osobowych – art. 29 RODO, który wskazuje, że podmiot przetwarzający i osoby biorące udział w procesie przetwarzania danych działają jedynie na podstawie upoważnienia i przetwarzają dane wyłącznie na jego polecenie (chyba że obowiązek przetwarzania danych wynika z prawa krajowego lub prawa unijnego);
- prowadzenie rejestru czynności przetwarzania – obowiązek ten wiąże się bezpośrednio z zasadą rozliczalności i zobowiązuje administratora do prowadzenia dokładnego, rzetelnego rejestru czynności podejmowanych w ramach procesu przetwarzania. Zakres informacji, które powinny znaleźć się w rejestrze, został szczegółowo określony przez unijnego prawodawcę w art. 30 RODO;

- przeprowadzenie ogólnej analizy ryzyka – art. 32 RODO, szerzej omówione w rozdziale siódmym;
- zgłoszenie naruszenia organowi nadzorczemu i poinformowanie osób, których dane dotyczą, o naruszeniu, jeżeli spełnione są warunki określone w RODO – art. 33 i 34 RODO;
- przeprowadzenie oceny skutków dla ochrony danych (DPIA) w zakresie procesów, które tego wymagają – art. 35 RODO;
- wyznaczenie Inspektora Ochrony Danych – art. 37 RODO, szerzej opisane w rozdziale dziewiątym.

Brak realizacji jednego z obowiązków nałożonych na administratora (lub podmiot przetwarzający) może się wiązać ze wszczęciem postępowania przed organem nadzorczym (w Polsce – Prezesem Urzędu Ochrony Danych Osobowych). Jeśli w trakcie postępowania organ stwierdzi naruszenie, może nałożyć administracyjną karę pieniężną. Jej wysokość jest zależna z jednej strony od rodzaju naruszonego obowiązku, z drugiej – organ nadzorczy ma obowiązek wziąć pod uwagę szereg elementów (np. czas trwania naruszenia, liczbę podmiotów danych nim dotkniętych, powagę naruszenia, umyślność lub nieumyślność naruszenia oraz inne wskazane w art. 83 ust. 2).

W zakresie naruszenia obowiązków wskazanych w art. 8, 11, 25–39 oraz 42 i 43 RODO maksymalna kara, która może być nałożona na administratora, to 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. W przypadku naruszenia w zakresie: podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9 RODO; praw osób, których dane dotyczą, o których mowa w art. 12–22 RODO; przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 44–49 RODO, oraz wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX RODO mak-

symalna kara to 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

W przypadku administratorów danych – podmiotów publicznych określonych w ustawie o ochronie danych osobowych, tj. jednostek sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, instytutów badawczych oraz Narodowego Banku Polskiego, Prezes Urzędu Ochrony Danych Osobowych może nałożyć karę w maksymalnej wysokości 100 000 złotych. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, tzn. państwowe i samorządowe instytucje kultury.

6.2. Powierzenie przetwarzania

Prawodawca unijny nie zdecydował się na zdefiniowanie terminu „powierzenie przetwarzania", a jedynie w art. 28 zawarł gwarancje jego skuteczności. Obowiązkiem administratora, który decyduje się powierzyć przetwarzanie podmiotowi trzeciemu, jest wybór takiego procesora, który da odpowiednie gwarancje ochrony danych osobowych. Pomocna w definiowaniu pojęcia „powierzenia przetwarzania" jest definicja czynności „przetwarzania" zawarta w RODO. Przetwarzanie na gruncie RODO oznacza operację 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.

Analogicznie należałoby uznać, że powierzenie przetwarzania to zlecenie podmiotowi zewnętrznemu w stosunku do administratora wykonywania czynności mieszczących się w kategorii pojęcia „przetwarzanie" w ramach szeroko rozumianej współpracy pomiędzy administratorem i podmiotem przetwarzającym. Sprowadza się to do przetwarzania danych osobowych przez podmiot przetwarzający w imieniu administratora. Europejska Rada Ochrony Danych wskazuje, że powierzenie przetwarzania to działanie w czyimś imieniu, oznacza to służenie czyjemuś interesowi i jest zbliżone do delegacji[268].

Warto zwrócić uwagę, że powierzenie przetwarzania jest sytuacją faktyczną – dopełnienie warunków formalnych (związanych np. z zawarciem umowy) nie ma charakteru kreującego, nie tworzy sytuacji powierzenia przetwarzania, a jedynie ją potwierdza i legalizuje. Inaczej dzieje się w przypadku, gdy powierzenie przetwarzania następuje na podstawie ustawy lub innego instrumentu prawnego o podobnym charakterze (np. poprzez akt prawa miejscowego). W takiej sytuacji to właśnie odpowiednia norma prawna kreuje relacje pomiędzy administratorem a podmiotem przetwarzającym. Odwrotnie niż w przypadku umowy powierzenia przetwarzania, w sytuacji gdy przetwarzanie oparte jest na instrumencie prawnym, relacja administrator–podmiot przetwarzający nie zaistnieje, dopóki dany instrument nie zacznie obowiązywać w stosunkach prawnych. Konieczne jest jednak, aby zgodnie z art. 28 RODO administrator i podmiot przetwarzający zawarli umowę powierzenia przetwarzania bądź aby przetwarzanie odbywało się na podstawie innego in-

[268] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, wersja 1.0, z 2.9.2020 r., s. 24, https://www.edpb.europa.eu/system/files_en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf [dostęp: 24.06.2025].

strumentu prawnego, który podlega prawu Unii lub prawu państwa członkowskiego i wiąże podmiot przetwarzający i administratora, określając przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Artykuł 28 RODO wskazuje na obowiązkowe elementy umowy powierzenia przetwarzania danych. Nie znaczy to jednak, że obok nich nie mogą pojawić się inne, uzgodnione przez strony elementy. Umowa powierzenia przetwarzania może być zarówno jedyną umową łączącą strony, jak i mieć charakter akcesoryjny (dodatkowy) do umowy głównej, np. o świadczenie innych usług. Zgodnie z art. 28 RODO umowa powierzenia przetwarzania danych powinna określać przede wszystkim cel i przedmiot przetwarzania danych osobowych (rodzaj danych osobowych oraz kategorie danych osób, których dane dotyczą, obowiązki i prawa administratora). Cel powierzenia powinien być bardzo blisko związany z celem przetwarzania danych określonym przez administratora, ale nie musi być tożsamy[269]. W przypadku, gdyby administrator zlecił podmiotowi przetwarzającemu przetwarzanie danych w celu zupełnie niepowiązanym z celem pierwotnym, dochodziłoby do naruszenia zasady celowości i minimalizacji danych. Cel i charakter przetwarzanych danych może być na bieżąco dookreślany przez administratora w formie instrukcji i poleceń, do których przestrzegania zobowiązany jest podmiot przetwarzający.

Zgodnie z art. 28 ust. 3 RODO umowa powierzenia przetwarzania powinna wskazywać, że podmiot przetwarzający:

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania

[269] M. Czech, *Umowa powierzenia przetwarzania danych osobowych jako instrument ich ochrony*, rozprawa doktorska napisana pod kierunkiem prof. dr hab. Teresy Mróz, Białystok 2019, s. 218; zob. również Ł. Głębocki, *Umowa powierzania przetwarzania danych osobowych zgodnie z RODO*, „Informacja w Administracji Publicznej" 2018, nr 1, s. 30–35.

danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w RODO;
e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą;
f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;
g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Umowa powierzenia przetwarzania ze swej natury nakłada większość obowiązków na podmiot przetwarzający. Jednocześnie, jeśli strony tak postanowią, może ona również nakładać określone obowiązki na administratora. Nie jest to jednak powszechna praktyka.

Umowa powierzenia przetwarzania powinna również określić zakres terytorialny przetwarzania. Takie stanowisko wydaje się być uzasadnione, biorąc pod uwagę również ograniczenia przewidziane w RODO odnoszące się do generalnego zakazu przekazywania danych osobowych do państw trzecich.

6.3. Podstawowe obowiązki w zakresie transferu danych poza EOG

Co do zasady RODO wprowadza zakaz przekazywania danych osobowych do państw trzecich za wyjątkiem sytuacji, w których przekazanie (transfer) danych odbywa się na podstawie decyzji Komisji Europejskiej stwierdzającej adekwatny poziom ochrony danych osobowych lub na podstawie jednego ze wskazanych w art. 46 RODO mechanizmów transferu.

RODO dopuszcza również sytuację, w której transfer danych odbywa się przy braku decyzji o adekwatności ochrony i braku mechanizmu transferu. Zgodnie z art. 49 RODO w takich sytuacjach jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie pod warunkiem, że:

1) osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę;

2) przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą;
3) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną;
4) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego;
5) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń;
6) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; lub
7) przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

Biorąc pod uwagę, że wyjątki określone w art. 47 RODO powinny być interpretowane w bardzo ścisły sposób (ponieważ transfer bez odpowiednich zabezpieczeń lub decyzji o adekwatności zwiększa ryzyko dla podmiotów danych) w praktyce mają one marginalny charakter i co do zasady nie są wykorzystywane przez znaczną część administratorów. Należy zatem poprzestać jedynie na powyższym ich wspomnieniu.

Podstawowym środkiem, który zezwala na przekazanie danych do państwa lub organizacji znajdujących się poza Europejskim Obszarem Gospodarczym, jest decyzja Komisji Europejskiej stwier-

dzająca adekwatny stopień ochrony danych osobowych. Sposób jej przyjęcia został określony w art. 45 RODO oraz w bardzo szeroki sposób omówiony w doktrynie. Warto zauważyć, że obecnie (maj 2025) obowiązuje 16 decyzji stwierdzających odpowiedni poziom ochrony, dotyczą one: Andory, Argentyny, Kanady (organizacje komercyjne), Wysp Owczych, Guernsey, Izraela, Wyspy Man, Japonii, Jersey, Nowej Zelandii, Republiki Korei, Szwajcarii, Zjednoczonego Królestwa (w ramach RODO i LED), Stanów Zjednoczonych (dla firm certyfikowanych w ramach Europejskiego Programu Ochrony Danych Osobowych) oraz Urugwaju. Decyzje o uznaniu adekwatności ochrony są samodzielnym mechanizmem transferu, niewymagającym od administratora zawierania dodatkowych porozumień. Jednocześnie decyzje te nie zwalniają administratora z obowiązku przeprowadzenia analizy ryzyka dla transferu danych.

Chociaż co do zasady decyzje o uznaniu adekwatności ochrony miały być najbardziej stabilnym mechanizmem pozwalającym na transfer danych, w praktyce dwukrotnie zostały już one unieważnione. Dotyczyły one porozumień pomiędzy Komisją Europejską i Stanami Zjednoczonymi w ramach programów Safe Harbour i Privacy Shield. Należy również zwrócić uwagę, że obie decyzje miały charakter „ograniczonej decyzji o adekwatności”[270]. Oznacza to, że jedynie podmioty, które skorzystały z mechanizmów samocertyfikacji określonych w Safe Harbour[271] i Privacy Shield[272], mogły być odbiorcami danych osobowych zgodnie z regułami określonymi w art. 45 RODO. Pokazuje

[270] Zob. M. Corrales Compagnucci, T. Minssen, C. Seitz, M. Aboy, *Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Transfers in the Pharmaceutical Sector After Schrems II Invalidation of the EU-US Privacy Shield*, „European Data Protection Law Review” 2020, nr 3, s. 154.

[271] Wyrok TSUE z dnia 6 października 2015 r. *Maximillian Schrems przeciwko Data Protection Commissioner*, C-362/14.

[272] Wyrok Trybunału (wielka izba) z dnia 16 lipca 2020 r. *Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi*, C-311/18.

to, że w obecnej sytuacji geopolitycznej decyzje o uznaniu adekwatności ochrony wydawane przez Komisję Europejską nie zawsze mogą być uznane za wiarygodną i stabilną podstawę transferu danych.

W przypadku braku decyzji o uznaniu adekwatności ochrony administrator lub podmiot przetwarzający decydujący się na przekazanie danych do państwa lub organizacji znajdujących się poza Europejskim Obszarem Gospodarczym powinien oprzeć przekazanie na jednym z mechanizmów określonych w art. 46 RODO, tj.:

1) prawnie wiążącym i egzekwowalnym instrumencie między organami lub podmiotami publicznymi;
2) wiążących reguł korporacyjnych zgodnie z art. 47;
3) standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;
4) standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;
5) zatwierdzonym kodeksie postępowania zgodnie z art. 40 RODO wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą; lub
6) zatwierdzonym mechanizmie certyfikacji zgodnie z art. 42 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

Metody te nie wymagają dodatkowej zgody od lokalnego organu nadzorczego. Jednocześnie istnieją jeszcze dwa mechanizmy, które takiej zgody wymagają. Należą do nich:

1) klauzule umowne między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarza-

jącym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej; i

2) postanowienia uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

W praktyce zasadniczą rolę w przekazywaniu danych do państw lub organizacji znajdujących się poza Europejskim Obszarem Gospodarczym odgrywają standardowe klauzule umowne oraz wiążące reguły korporacyjne. Treść standardowych klauzul umownych jest przyjmowana przez Komisję Europejską, a administratorzy i podmioty przetwarzające, które z nich korzystają, nie mają swobody w dowolnym ich kształtowaniu. Jednocześnie wymagają one przeprowadzenia analizy ryzyka dla transferu danych. Wiążące reguły korporacyjne są z kolei środkiem wykorzystywanym przez międzynarodowe grupy powiązane osobowo i kapitałowo – ich przyjęcie jest procesem sformalizowanym i długotrwałym, wymagającym ścisłej współpracy z organem nadzorczym. Stąd też stosunkowo niewielu administratorów decyduje się na ich wdrożenie w organizacjach. Jednocześnie wiążące reguły korporacyjne, jeśli wdrożone są w sposób kompleksowy, pomagają utrzymać jednolity poziom ochrony danych w całej organizacji i stanowią środek, który może w znacznym stopniu przyczynić się do zapewnienia systemowego bezpieczeństwa informacji.

Rozdział VII

Systemowe zarządzanie bezpieczeństwem informacji

7.1. Zarządzanie bezpieczeństwem informacji

Systemowe zarządzanie bezpieczeństwem informacji (ang. Information Security Management System, ISMS, SZBI) to **zestaw procesów, procedur, polityk i zasobów wdrażanych w organizacji w celu ochrony informacji przed zagrożeniami**. SZBI jest oparty na podejściu systemowym, co oznacza, że **obejmuje nie tylko technologię, ale również ludzi, procesy i kulturę organizacyjną**. Podstawą SZBI są normy, takie jak ISO/IEC 27001, które definiują wymagania i najlepsze praktyki dla skutecznego zarządzania bezpieczeństwem informacji.

Celem systemowego zarządzania bezpieczeństwem informacji jest **zapewnienie bezpieczeństwa informacji, rozumianego jako stopień zaufania, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego ujawnienia, modyfikacji, zniszczenia, uniemożliwienia przetwarzania informacji przechowywanej i przetwarzanej w określonym systemie obiegu informacji**[273]. Pojęcie bezpieczeństwa informacji ma szersze znaczenie niż pojęcie bezpieczeństwa teleinformatycznego, które odnosi się jedynie do sys-

[273] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008, s. 12.

temów teleinformatycznych[274]. Biorąc pod uwagę skalę i zakres działalności współczesnych cyberprzestępców, można pokusić się o stwierdzenie, że obecnie, w przypadku sektora prywatnego, niemożliwe jest wdrożenie takiego systemu, który zapewni całkowitą odporność, a stopień ryzyka, jaki organizacja jest w stanie zaakceptować, zależy od decyzji zarządczych. W przypadku sektora publicznego również trudno o wskazanie państw czy organizacji, które mogą poszczycić się pełną odpornością na ataki zewnętrzne i wewnętrzne, jednak szczególnie w sektorach wyjątkowo istotnych dla funkcjonowania państwa poziom zabezpieczeń w niektórych krajach jest niezwykle wysoki.

Spośród pozostałych celów SZBI można wymienić: zapewnienie integralności, zagwarantowanie dostępności, zarządzanie ryzykiem, budowanie zaufania i zapewnienie zgodności z regulacjami (*compliance*). Poza osiągnięciem powyższych celów wdrożenie sprawnego i efektywnego SZBI ma szereg korzyści, zarówno wewnętrznych jak i zewnętrznych. Spośród tych pierwszych można wyróżnić:

- uniknięcie kar za naruszenie przepisów związanych z bezpieczeństwem informacji;
- ochronę informacji będących w organizacji;
- zabezpieczenie informacji w razie wystąpienia katastrofy czy awarii;
- wzrost świadomości pracowników, podwyższenie sprawności kadry, rozwój personelu;
- wiedzę i większą kontrolę nad tym, co dzieje się w organizacji;
- zwiększenie zaufania do własnej organizacji;
- usystematyzowanie procesów i dokumentów;
- usprawnienie przepływów informacji przy jednoczesnym wzroście elastyczności przyjętych rozwiązań;
- ograniczenie ryzyk związanych z bezpieczeństwem informacji[275].

---

[274] *Ibidem*.

[275] J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2010, s. 50–51.

Do korzyści zewnętrznych można zaliczyć:
- zwiększenie zaufania do firmy;
- wzrost konkurencyjności na rynku;
- potwierdzenie wysokiego poziomu kultury organizacji;
- prestiż wynikający z posiadanych certyfikatów;
- spełnienie wymagań przetargowych oraz warunków stawianych przez największych globalnych klientów w zakresie certyfikacji;
- ochronę marki i jej dobrego imienia wraz z poprawą wizerunku;
- podniesienie wiarygodności przedsiębiorstwa[276].

Systemowe zarządzanie bezpieczeństwem informacji zakłada **kompleksowe podejście do kwestii zarządzania ryzykiem w danej organizacji**. Proces ten powinien być w pełni przemyślany, odzwierciedlający nie tylko ryzyka (szerzej opisane w puncie 7.3), ale również możliwości jednostki organizacyjnej. Biorąc pod uwagę ustawę o ochronie informacji niejawnych, warto zwrócić uwagę, że **zarządzanie ryzykiem opiera się na czterech zasadniczych elementach: szacowania ryzyka, postępowania z ryzykiem, akceptacji ryzyka, przeglądu i monitorowania ryzyk**[277]. Zgodnie z § 19 rozporządzenia o bezpieczeństwie systemów teleinformatycznych proces zarządzania ryzykiem w systemie teleinformatycznym prowadzi się w celu zapewnienia i utrzymania na poziomie akceptowanym przez kierownika danej jednostki organizacyjnej bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie. Chociaż unijny prawodawca w RODO nie zawarł wprost takich rozwiązań, są one powszechnie praktykowane również w zakresie zarządzania bezpieczeństwem przetwarzania danych osobowych. Jednocześnie, w przypadku zarządzania ryzykiem w przetwarzaniu danych osobowych, celem nadrzędnym jest właśnie zapewnienie bezpieczeństwa

[276] *Ibidem*, s. 52.
[277] M. Jabłoński, T. Radziszewski, *op. cit.*, s. 93.

zarówno w warstwie materialnej (danych osobowych), jak i proceduralnej (proces przetwarzania).

Zdefiniowanie uwarunkowań organizacji można zacząć od przeprowadzenia analizy SWOT, która umożliwi zestawienie obrazujące: silne strony podmiotu, słabe strony podmiotu, szanse istniejące lub mogące się pojawić, zagrożenia istniejące lub mogące się pojawić[278]. O ile analizę SWOT można przeprowadzać dla różnorakich organizacji na każdym etapie ich funkcjonowania, a jej zakres szczegółowości może być różny, to w przypadku procesów związanych z bezpieczeństwem informacji kompleksowe opracowanie procedur zarządczych wymaga zmapowania procesów zachodzących w zakresie przetwarzania danych. Do podstawowych kwestii, jakie powinny być określone, należą m.in.:

- zakres i charakter informacji, jakie są przetwarzane;
- katalog podmiotów, których dotyczą dane informacje;
- cel(e), dla których informacje są przetwarzane;
- podstawy prawne umożliwiające przetwarzanie informacji;
- sposób przepływu informacji w organizacji (zarówno w kontekście personalnym, jak i sposobów wykorzystywanych do przekazywania informacji);
- zakres i sposób zaangażowania podmiotów trzecich w procesy związane z przetwarzaniem informacji;
- osoby decyzyjne w procesach przetwarzania informacji.

Powyższy katalog nie jest zamknięty, a ilość zmiennych, które należy ustalić, zależy nie tylko od wielkości organizacji, ale również branży, w której działa, jej struktury organizacyjnej, powiązania z podmiotami trzecimi, schematu grupy kapitałowej, do której należy, czy np. podlega w jakikolwiek sposób innym organom administracyjnym. Niemniej powyższe wyliczenie można potraktować

[278] W. Sokołowicz, A. Srzednicki, *ISO. System zarządzania jakością oraz inne systemy oparte na* normach, Warszawa 2006, s. 75.

jako punkt wyjścia i od niego zacząć analizę procedur przetwarzania informacji.

Analiza procesów przetwarzania wraz z analizą SWOT może okazać się niezbędna dla dalszego określenia procesów zarządczych. Powinny one rozpoczynać się od ciągłego pytania, co należy i można zrobić, a zarządzanie (w tym również procesami bezpieczeństwa informacji) polega na znajdowaniu trafnych odpowiedzi przez osoby decyzyjne różnych szczebli na te pytania[279].

Istotną cechą systemu zarządzania bezpieczeństwem informacji jest jego **optymalizacja przy jednoczesnym dążeniu do jego doskonałości** (idealności). Za M. Jabłońskim i T. Radziszewskim można uznać, że system idealny jest optymalny organizacyjnie i kosztowo, dokładnie powtarzalny w zakresie jakości efektu działania, skuteczny, bezpieczny, nieprzerwany[280]. Koniecznie jednak trzeba podkreślić, że system idealny nie jest systemem raz wdrożonym, do którego następnie nie zaglądamy przez lata. Biorąc pod uwagę rozwój zagrożeń dla bezpieczeństwa informacji, konieczny jest stały przegląd i udoskonalanie procedur, również biorąc pod uwagę zmieniające się potrzeby i możliwości danej organizacji. Konieczne jest takie zaprojektowanie systemów, które nie tylko umożliwiają, ale wręcz zmuszają kadrę zarządzającą lub inne osoby odpowiedzialne do przeprowadzania okresowych przeglądów i reagowania na zmiany w odpowiednim czasie.

Systemowe zarządzanie bezpieczeństwem informacji nie będzie jednolite w każdej z organizacji. **Musi ono być dostosowane do warunków i potrzeb określonego podmiotu**. Jednocześnie kompletny SZBI ma pewne elementy wspólne. Należą do nich: polityki bezpieczeństwa, szkolenia i świadomość, kontrole i audyty, ciągłe doskonalenie, wdrożone procedury oraz proces zarządzania ryzykiem.

---

[279] *Ibidem*.

[280] M. Jabłoński, T. Radziszewski, *op. cit.*, s. 89.

7.2. Normy ISO

Opracowywanie standardów w systemach zarządzania bezpieczeństwem informacji zaczęło się już w latach 80. XX w. To wtedy w Wielkiej Brytanii powołano Commercial Computer Security Centre, który miał opracować międzynarodowe zestawy kryteriów oceny rozwiązań IT oraz powiązanych z nimi schematów ocen i certyfikacji[281]. Jednocześnie pierwsza norma o charakterze międzynarodowym w zakresie bezpieczeństwa informacji została przyjęta dopiero w 2000 r. i była to ISO/EIC 27002 *Information Technology – Code of practice for information security management*[282]. Zawierała ona opisy i zalecenia w zakresie bezpieczeństwa informacji oraz szeroki zakres proponowanych zabezpieczeń[283]. I chociaż standardów w ostatnich latach wykształciło się wiele (np. COBBIT, ITIL czy nawet standardy opracowane przez polski PKN), to największe znaczenie ma opublikowana w październiku 2005 r. norma ISO/IEC 27001.

Norma ISO/IEC 27001 za zasadniczy cel uznaje **zapewnienie odpowiedniej ochrony informacji przed zagrożeniami, które mogą prowadzić do strat finansowych, utraty reputacji czy naruszenia przepisów**. Norma ta cechuje się proaktywnym podejściem, które zakłada, że identyfikacja i ocena ryzyk pozwala organizacji podejmować środki zapobiegawcze, zamiast reagować dopiero po wystąpieniu incydentu. Wdrożenie normy ISO/IEC 27001 pozwala również na skuteczniejszą alokację zasobów – zarządzanie ryzykiem pomaga organizacjom zidentyfikować obszary wymagające największej ochrony, co umożliwia bardziej efektywne inwestowanie w zabezpieczenia. Co więcej, **standardy przyjęte w tej normie**

---

[281] J. Łuczak, M. Tyburski, *op. cit.*, s. 55.
[282] *Ibidem*.
[283] *Ibidem*.

są zbieżne z wymaganiami prawnymi związanymi z bezpieczeństwem informacji, np. RODO, co pozwala przyjąć, że jej wdrożenie zbliży organizację do zapewnienia zgodności działania z aktualnie obowiązującymi przepisami.

Norma ISO-IEC 27001 opiera się na **cyklu Deminga** jako sekwencji działań, których celem jest doskonalenie problemów jakościowych i wdrażanie nowych rozwiązań[284]. Nazywany często modelem PDCA (z ang. Plan-Do-Check-Act), stosowany jest w każdego rodzaju działalności. Cykl Deminga zakłada następujące kroki:

1) planuj – związany jest z analizą i możliwością rozpoznania niezbędnych zmian, z doskonaleniem i zaplanowaniem ich poprzez wyznaczenie celu i zaprojektowanie planu działania;
2) wykonaj – zakłada wykonanie opracowanego planu w celu wdrożenia zmian w procesie przy wsparciu i zrozumieniu kierownictwa;
3) sprawdzaj – polega na przetestowaniu, czy nowe rozwiązania przyniosły odpowiednie rezultaty; jeśli tak się stało, następuje przejście do kolejnego kroku;
4) działaj – krok ten związany jest ze stosowaniem wdrożonych rozwiązań[285].

Norma ISO/IEC 27001 nie funkcjonuje w próżni – jest częścią większej rodziny norm ISO, do której można zaliczyć:

- ISO 27002 – jest zbiorem najlepszych praktyk i wytycznych dotyczących zabezpieczeń technicznych i organizacyjnych;
- ISO 27005 – standard ten szczegółowo opisuje proces zarządzania ryzykiem w kontekście bezpieczeństwa informacji;
- ISO 27701 – rozszerza ISO/IEC 27001 o wymagania dotyczące ochrony prywatności (szczególnie w kontekście RODO).

---

[284] W. Fehler (red.), *Leksykon bezpieczeństwa informacyjnego*, Siedlce 2023, s. 83.

[285] Opracowano na podstawie: *ibidem*, s. 83–84.

W zakresie zarządzania bezpieczeństwem informacji norma ISO/IEC 227001 jest z pewnością najważniejszą. Jej wdrożenie w znacznym zakresie ułatwia zapewnienie zgodności z prawem procesów przetwarzania danych osobowych i informacji niejawnych.

7.3. Proces szacowania ryzyka bezpieczeństwa informacji

Proces szacowania ryzyka (analiza ryzyka) jest jednym z elementów zarządzania ryzykiem w organizacji. W przypadku ochrony informacji niejawnych ustawodawca posługuje się pojęciem „szacowania ryzyka dla bezpieczeństwa informacji niejawnych" (§ 19 pkt 2 rozporządzenia o bezpieczeństwie systemów teleinformatycznych), a w przypadku RODO wprowadzone zostało pojęcie „analizy ryzyka". Biorąc pod uwagę zbieżny cel obu procesów i jedynie drobne różnice semantyczne, w dalszej części opracowania pojęcia te będą używane zamiennie, zaznaczając ewentualne różnice między dwoma modelami ochrony. Na marginesie należy dodać, że w przypadku przetwarzania danych osobowych szacowanie ryzyka następuje nie tylko w wobec konieczności wyboru odpowiednich środków organizacyjnych i technicznych zapewniających bezpieczeństwo przetwarzania i bezpieczeństwo danych osobowych, ale również w przypadkach incydentów i naruszeń.

Zgodnie z § 19 pkt 3 rozporządzenia o bezpieczeństwie systemów teleinformatycznych[286] przed przeprowadzeniem procesu szacowania ryzyka ustala się granice i zakres analizy ryzyka, strukturę organizacyjną odpowiedzialną za zarządzanie ryzykiem w systemie teleinformatycznym oraz dokonuje się wyboru metody analizy ryzyka. Chociaż RODO wprost nie zawiera takiego rozwiązania (pozostawiając w tym

[286] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r. Nr 159, poz. 948).

zakresie swobodę administratorom danych), to konieczność poprzedzenia analizy ryzyka zdefiniowaniem powyżej wskazanych obszarów wynika z praktyki zapewniania zgodności procesów przetwarzania z RODO. Trudno też byłoby sobie wyobrazić proces analizy ryzyka bez określenia jego metodologii czy granic dokonywanej analizy. RODO nie wymaga również tworzenia nowych struktur w organizacji (poza ewentualnym powołaniem inspektora ochrony danych w określonych przypadkach – szerzej na ten temat w rozdziale dziewiątym), zatem zasadne byłoby przed wykonaniem analizy ocenić osoby decyzyjne bądź zajmujące się bezpieczeństwem systemów teleinformatycznych i danych osobowych w organizacji. Może to być również elementem analizy SWOT opisanej w rozdziale 7.1.

Analiza ryzyka wymaga **zdefiniowania kluczowych procesów biznesowych**, czyli takich, które mają zasadnicze znaczenie dla podstawowej działalności biznesowej podmiotów, a ich zakłócenie może być przyczyną znacznych strat nie tylko przez firmę, ale również usługobiorców czy środowisko, w którym te procesy przebiegają[287]. Kluczowymi procesami biznesowymi nie zawsze będą procesy końcowe, często za takie można uznać te niezauważalne przez ostatecznego odbiorcę produktu. W przypadku administracji publicznej trudno mówić o procesach biznesowych. Dla podmiotów publicznych konieczne jest **zdefiniowanie kluczowych zadań publicznych**, jakie one wykonują, oraz określenie ich wpływu nie tylko na daną jednostkę organizacyjną, ale szerzej: na społeczeństwo (lub jego fragment) i sfery działalności państwa, na które wykonywane zadania publiczne oddziaływa.

Gdy zostaną już określone procesy kluczowe, konieczne jest sprawdzenie, jakie są dopuszczalne czasy przestojów, oraz to, jak są wrażliwe na zakłócenia we wspierających je procesach przetwarzania informacji[288]. Można domniemywać, że dwugodzinna przerwa

[287] K. Liderman, *op. cit.*, s. 26.
[288] *Ibidem*.

w dostawie prądu w urzędzie miasta będzie stanowiła niedogodność dla pracowników i petentów, ale po przywróceniu łączności urząd szybko podejmie wykonywanie dalszej pracy. Jeśli jednak okaże się, że awaria potrwa dłużej, na przykład 7 dni, to jest to już istotne ryzyko dla funkcjonowania infrastruktury całego miasta. W przypadku podmiotów prywatnych łatwo można sobie wyobrazić sytuację (i w rzeczywistości zdarzenia takie miały już miejsce), że awarii ulega dostawca chmur obliczeniowych, z którego usług korzysta znaczna część populacji. Nawet 2–3-godzinny przestój może doprowadzić do chaosu oraz w konsekwencji narazić znaczną część użytkowników na straty. W konsekwencji być może będzie to wiązało się z koniecznością wypłacenia odszkodowań (chociaż trzeba przyznać, że większość dostawców usług chmurowych zastrzega sobie dosyć silne gwarancje umowne chroniące ich przed ewentualną wypłatą odszkodowań). Przykładowo w lipcu 2024 r. globalna awaria chmury Microsoftu doprowadziła do uziemienia samolotów na całym świecie[289].

Powyższa analiza pozwoli organizacjom na zdefiniowanie procesów krytycznych, to znaczy tych, których czas dopuszczalnego przestoju jest najkrótszy, a wrażliwość na utratę tajności, integralności lub dostępności informacji wykorzystywanej w procesie najbardziej kluczowa[290]. Zidentyfikowanie procesów wspierających procesy krytyczne pozwoli na określenie punktu lub punktów najbardziej newralgicznych dla organizacji.

Warto zauważyć w tym kontekście, że analiza ryzyka dla bezpieczeństwa informacji łączy się tutaj z kwestiami związanymi z zarządzaniem ciągłością działania. Chociaż w polskim prawie wymóg ten dotyczy jedynie niektórych branż i gałęzi gospodarki (np. banków, ope-

[289] J. Żabnicka, *Microsoft usuwa awarię chmury, która spowodowała, że niektóre amerykańskie linie lotnicze wstrzymały loty*, ITReseller, 19.02.2024, https://itreseller.pl/microsoft-usuwa-awarie-chmury-ktora-spowodowala-ze-niektore-amerykanskie-linie-lotnicze-wstrzymaly-loty/ [dostęp: 24.06.2025].

[290] K. Liderman, *op. cit.*, s. 27.

ratorów telekomunikacyjnych), to w praktyce większość dużych przedsiębiorców ma opracowane procedury, które mają zapewnić możliwie jak najszybsze przywrócenie firmy do działania w przypadku awarii.

Analiza ryzyka powinna brać pod uwagę zarówno zagrożenia, jak i podatność. Zagrożeniami są potencjalne działania człowieka (lub zaniechanie takich działań) albo sił wyższych, które dotyczą bezpośrednio organizacji procesu przetwarzania informacji i mogą spowodować straty proporcjonalne do wagi procesu krytycznego, wspieranego przez ten proces i wykorzystywane w nim zasoby[291]. Z kolei podatność to wada lub luka w strukturze fizycznej, organizacyjnej, procedurach czy personelu, która może być wykorzystana do spowodowania szkód w systemie teleinformatycznym lub działalności użytkownika[292].

Zagrożenia w bezpieczeństwie informacji tradycyjnie ujmowane są w wielorakich klasyfikacjach. Można zatem wyróżnić zagrożenia bierne (nieuprawnione ujawnienie informacji bez oddziaływania na system informatyczny) i czynne (związane z aktywnym oddziaływaniem na system); wewnętrzne (dokonywane ze strony legalnych użytkowników systemu) i zewnętrzne (dokonywane przez podmioty trzecie); przypadkowe i celowe; sprzętowe lub programowe[293].

Dla cyberprzestępców można wyróżnić pewne typowe formy działania, takie jak celowe powodowanie awarii w momentach krytycznych, wywoływanie fałszywych alarmów, techniki typu *sniffing* i *spoofing*, *phishing*, szyfrowanie plików, przeszukiwanie śmietników, wyłudzanie informacji w trakcie spotkań towarzyskich, podszywanie się pod kontrole i audyty, penetracja systemu przez pocztę elektroniczną, szantaż, korupcja czy wyłudzanie informacji[294]. Działania te mogą prowadzić do instalowania na urządzeniach organizacji bę-

[291] *Ibidem*, s. 41.
[292] *Ibidem*, s. 40.
[293] M. Molski, M. Łacheta, *Bezpieczeństwo i audyt systemów informatycznych*, Bydgoszcz 2009, s. 32–33.
[294] *Ibidem*, s. 38–39.

dącej celem ataku złośliwego oprogramowania, takiego jak wirusy, robaki, *spyware*, *adware*, konie trojańskie, aplikacje typu *keylogger*, *rootkit* czy *dialer*[295]. Wszystkie te działania mają na celu wyrządzenie krzywdy atakowanej organizacji i mogą prowadzić do nieuprawnionego ujawnienia, zniszczenia lub przetwarzania informacji.

Ocena skutków jest kwalifikowaną formą analizy ryzyka. Zgodnie z art. 35 RODO przeprowadza się ją, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ocenę skutków dla ochrony danych przeprowadza się przed rozpoczęciem przetwarzania. Powinna być wykonana tak szybko, jak to możliwe, nawet jeśli na etapie projektowania procesu niektóre z operacji przetwarzania nie są jeszcze znane[296]. Konieczne jest również, aby ocena skutków dla ochrony danych była aktualizowana przez cały czas trwania projektu[297]. Przepis art. 35 ust. 1 RODO zawiera szereg klauzul niedookreślonych („duże prawdopodobieństwo", „wysokie ryzyko", „podobne operacje przetwarzania"), stąd też jego interpretacja może budzić szereg wątpliwości.

Na gruncie RODO prawodawca nie zdecydował się na określenie, czym jest ocena skutków. Grupa Robocza Art. 29 definiuje ocenę skutków jako proces pozwalający opisać przetwarzanie oraz ocenić jego konieczność i proporcjonalność, a także mający wspomóc zarządzanie ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania danych osobowych[298]. W wytycznych

---

[295] *Ibidem*, s. 39–40.

[296] Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679*, przyjęte 4.04.2017 r., ostatnio zmienione i przyjęte 4.10.2017 r., WP 248, s. 11.

[297] *Ibidem*, s. 12.

[298] Grupa Robocza Art. 29, *Wytyczne dotyczące oceny…*, s. 4.

wskazano, że działania podejmowane w ramach oceny skutków są ważnym narzędziem zasady rozliczalności, „ponieważ ułatwiają administratorom nie tylko przestrzeganie wymogów określonych w RODO, ale także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO”[299]. Zdaniem Grupy Roboczej Art. 29 ocena skutków jest procesem budowania i wykazywania zgodności.

Ocena skutków dla ochrony danych jest obligatoryjna w następujących przypadkach:

1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO;
3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Przeprowadzenie oceny skutków dla ochrony danych osobowych będzie również obowiązkowe w przypadku, gdy organ nadzorczy uzna, że określone przez niego operacje przetwarzania danych wiążą się z obowiązkiem przeprowadzenia oceny. Bez wątpienia **ocena skutków jest przejawem technologicznej neutralności regulacji, podejścia opartego na ryzyku, ochrony proaktywnej i prewencyjnej**. Powinna być wykonywana z uwzględnieniem tych zasad. Podmiotem zobowiązanym do dokonania oceny skutków dla ochrony danych jest administrator, jednak podmiot przetwarzający powinien go w tym wspierać w ramach obowiązków określonych w omówionej już umowie powierzenia

[299] *Ibidem*.

przetwarzania danych osobowych. Jeśli w danym podmiocie został powołany inspektor ochrony danych, również on powinien być zaangażowany w prace nad oceną skutków dla ochrony danych.

Ocena skutków dla danych osobowych powinna zawierać co najmniej:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o której mowa w ust. 1; oraz
4) środki planowane w celu zarządzania ryzykiem, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Powyższy katalog jest katalogiem otwartym, określa minimalny zakres czynności, jakie powinny być uwzględnione w procesie oceny skutków[300]. Oznacza to, że ocena może obejmować również inne czynności niewskazane przez prawodawcę, a które administrator uzna za istotne z właściwego i zgodnego z zasadą rozliczalności przeprowadzenia procesu oceny. W praktyce, jak wskazuje Grupa Robocza Art. 29, ocena skutków może składać się z następujących etapów:

a) opis planowanych operacji przetwarzania;
b) ocena konieczności i proporcjonalności;
c) środki planowane w celu wykazania zgodności;

---

[300] N. Kalinowska, P. Litwiński, *Ocena skutków dla ochrony danych i uprzednie konsultacje – nowe obowiązki podmiotów przetwarzających dane osobowe*, „Monitor Prawniczy" 2017, nr 13, s. 697.

d) ocena ryzyka naruszenia praw i wolności;
e) środki planowane w celu wyeliminowania ryzyka;
f) dokumentacja;
g) monitorowanie i przegląd[301].

W przypadku gdy po dokonaniu analizy ryzyka okaże się, że administrator nie jest w stanie wskazać i zastosować rozsądnych środków organizacyjnych i technicznych, które mają zminimalizować występujące ryzyko, powinien on skonsultować się z organem nadzorczym przed rozpoczęciem przetwarzania[302].

RODO dopuszcza możliwość przeprowadzenia jednej oceny skutków dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem. W motywie 92 regulacji wskazano nawet, że „w niektórych okolicznościach rozsądnie i korzystnie byłoby nie ograniczać oceny skutków dla ochrony danych do pojedynczego projektu, na przykład w przypadkach, gdy organy lub podmioty publiczne zamierzają ustanowić wspólną aplikację lub platformę przetwarzania lub gdy kilku administratorów planuje wprowadzić wspólną aplikację lub środowisko przetwarzania obejmujące sektor lub segment gospodarki lub szeroko rozpowszechnioną działalność horyzontalną". Kwestia ta wydaje się szczególnie istotna w przypadku jednostek samorządu gminnego, które decydują się na skorzystanie z rozwiązań chmurowych. Przeprowadzenie przez nie jednej analizy ryzyka dla wielu procesów przetwarzania pozwala nie tylko obniżyć koszty takiego działania, ale również zastosować bardziej kompleksowe i całościowe podejście. Grupa Robocza Art. 29 odwołuje się nawet do przykładu, w którym grupa władz miejskich instaluje podobny system monitorowania, i wskazuje, że w takiej sytuacji można przeprowadzić jedną ocenę skutków dla ochrony danych obejmującą przetwarzanie danych przez oddzielnych administratorów.

---

[301] Grupa Robocza Art. 29, *Wytyczne dotyczące oceny…*, s. 20.
[302] Zob. M. Jabłoński, J. Węgrzyn, *Zmiana modelu…*, s. 80.

Unijny prawodawca nie zdecydował się również na zdefiniowanie w RODO pojęcia „wysokiego ryzyka", od którego zależy powstanie obowiązku do przeprowadzenia oceny skutków. Dla interpretacji tego pojęcia kluczowy jest motyw 76, w którym wskazano, że „prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko". Na tym tle można, za A. Mednisem, stwierdzić, że ryzyko to prawdopodobieństwo naruszenia praw lub wolności osoby, której dane dotyczą[303]. Ryzyko to może być związane z dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową itp.[304]

Prawdopodobieństwo wystąpienia określonego zdarzenia można szacować, biorąc pod uwagę przede wszystkim dwa elementy. Pierwszy z nich to **analiza ekspozycji na zagrożenia**, wskazanie, czy występuje ona często, czasami, rzadko, czy w innym przedziale czasowym. Szacując wystąpienie drugiego z czynników, należy odpowiedzieć na pytanie, czy i **w jakiej częstotliwości konkretne zagrożenie występowało w przeszłości**[305].

Decyzja, czy ocena skutków powinna zostać przeprowadzona, musi być podjęta przy współpracy z ekspertami IT, zarządzania, ryzyka, bezpieczeństwa, prawa i prywatności oraz właścicielami biz-

---

[303] A. Mednis, *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych osobowych*, „Monitor Prawniczy" 2016, nr 20, s. 29.

[304] M. Jabłoński, J. Węgrzyn, *Zmiana modelu…* , s. 78.

[305] Zob. T. Izydorczyk, *Ocena ryzyka naruszenia praw lub wolności osób i ocena skutków dla ochrony danych*, [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *op. cit.*, s. 96.

nesowymi danej zmiany[306]. Przesłanką, która powinna być wzięta pod uwagę przy podejmowaniu decyzji o przeprowadzaniu oceny skutków dla ochrony danych, jest również przetwarzanie danych na dużą skalę. Grupa Robocza Art. 29 zaleca, aby przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, wziąć pod uwagę w szczególności następujące czynniki:

1) liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;
2) ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;
3) czas trwania lub trwałość czynności przetwarzania danych;
4) zakres geograficzny czynności przetwarzania[307].

Zgodnie z art. 35 ust. 10 RODO ocena skutków dla ochrony danych nie będzie wymagana, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych. Jak już zostało wcześniej wielokrotnie wspomniane, jednostki samorządu gminnego w znacznym stopniu przetwarzają dane osobowe w oparciu o art. 6 ust. 1 lit. e. Jednocześnie w polskich warunkach w większości przypadków nie została spełniona druga przesłanka zwalniająca administratora z obowiązku przeprowadzania oceny skutków dla ochrony danych. Dotychczasowa praktyka ustawodawcy w Polsce jedynie w nielicznych przypadkach przewiduje

---

[306] Por. M. Więckowska, *Analiza ryzyka prywatności*, „ABI Expert" 2017, nr 2, s. 48.

[307] Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów ochrony danych ('DPO')*, przyjęte w dniu 13 grudnia 2016 r., s. 8–9.

bowiem sporządzenie oceny skutków dla ochrony danych w ramach oceny skutków regulacji. Jest to szczególnie problematyczne w sytuacjach, kiedy określone przepisy wskazywały na konieczność przetwarzania danych osobowych przez gminę w celu realizacji jej zadań własnych lub zleconych jeszcze przed wejściem w życie RODO.

7.4. Środki organizacyjne i techniczne

RODO miało być technologicznie neutralne i pozostawiać w rękach administratorów dużą swobodę co do wyborów metod i środków, co z kolei powinno sprzyjać elastyczności. Oznacza to, że **administrator, na podstawie wykonanej przez siebie analizy ryzyka, powinien sam wybrać środki, zarówno organizacyjne i techniczne, które powinny być wykorzystane w procesie ochrony danych osobowych**. RODO dokonało zmiany rozumienia pojęcia „zabezpieczenia danych osobowych". Należy je rozumieć w sposób możliwie szeroki, wykraczający poza zapewnienie poufności, integralności i dostępności danych osobowych, ale obejmujący również zagwarantowanie bezpieczeństwa także innych praw i wolności osoby, której dane dotyczą, w szczególności tych, które są określone w RODO, a także w prawie Unii i prawie państwa członkowskiego[308]. Co więcej – ochronie podlegają nie tylko dane osobowe, ale również procesy ich przetwarzania. Jednocześnie, w przypadku części informacji, szczególnie tych prawnie chronionych, niektóre ze środków mogą być narzucone przez konkretne przepisy.

W tworzeniu systemu ochrony informacji należy uwzględnić następujące elementy:

a) fizyczna i techniczna ochrona przed nieupoważnionym dostępem, ale również wypadkami takimi, jak zalania czy pożary;

---

[308] T. Izydorczyk, *Analiza oparta na ryzyku (risk-based approach)*, [w:] M. Kołodziej (red.), *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych*, Warszawa 2017, Legalis.

b) sprzęt i oprogramowanie obejmujące odpowiednią kontrolę dostępu, kryptografię oraz integralność informacji, monitorowanie przepływów i działań użytkowników, zapewnienie odpowiedniego poziomu dostępności, w tym również odpowiednio zbudowane systemy zasilania, zapewnienie odpowiedniego sprzętu do niszczenia informacji;
c) organizację i kadry, czyli właściwe dokumentowanie systemu ochrony informacji, klasyfikacje informacji i przyznawanie dostępu do niej, szkolenia, wyznaczenie osób odpowiedzialnych i decyzyjnych, nadzór i kontrolę oraz zasady reagowania na incydenty[309].

Dla zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych szczególne znaczenia mają koncepcje *privacy by design* i *privacy be default.* Pierwsze z tych pojęć w Polsce określa się jako „ochronę prywatności w fazie projektowania" i chociaż nie jest ono najwłaściwsze, to zdążyło już zyskać na popularności i staje się powszechnie wykorzystywane. Koncepcja *privacy by design* miała stanowić odpowiedź na zmiany systemowe związane z zastosowaniem technologii informacyjnych i komunikacyjnych oraz rozbudowanej infrastruktury telekomunikacyjnej[310]. Ochrona prywatności w fazie projektowania wymaga kompleksowego podejścia w organizacji i wdrożenia jej do wszystkich operacji podejmowanych w danym podmiocie, włączając w to technologię informacyjną, praktyki biznesowe, wdrożone procedury, projektowanie fizyczne i infrastrukturę sieciową. Aby koncepcja ta odniosła sukces, konieczne jest wdrożenie w organizacji całej filozofii związanej z ochroną danych osobowych wraz z odpowiednimi zabezpieczeniami technicznymi i organizacyjnymi, które będą odpowiadały zmieniającym się zagrożeniom. W tym

[309] K. Liderman, *op. cit.*, s. 14.

[310] W. Wiewiórski, *Privacy by design jako paradygmat ochrony prywatności*, [w:] G. Szpor, W. Wiewiórski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, Warszawa 2012, s. 13.

podejściu ochrona danych jest integralną częścią organizacji, zostaje uwzględniona w jej celach i priorytetach oraz wymaga osadzenia w każdym standardzie, protokole i procedurze związanej z życiem jednostki i podmiotu przetwarzającego dane osobowe[311].

Privacy by default jest pochodną powyżej omówionej zasady. Odzwierciedleniem tej koncepcji jest art. 25 ust. 2 RODO, zgodnie z którym administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne do osiągnięcia każdego konkretnego celu przetwarzania. Zasada ta wymaga systemowego podejścia do projektowania usług i systemów w sposób umożliwiający skonfigurowanie ustawień prywatności zgodnie z wolą i decyzją osoby, której dane dotyczą[312]. Rdzeniem takiego podejścia jest przyznanie, że jakiekolwiek ograniczenia prywatności jednostki powinny następować na wyraźne żądanie konkretnej osoby, oraz wykluczenie pozyskiwania danych osobowych w sposób domyślny[313]. *Privacy by default* oznacza również, że wykorzystywane w procesie przetwarzania środki organizacyjne i techniczne z założenia pierwotnie mają prowadzić do ochrony prywatności jednostki, bez konieczności wykonywania przez nią odrębnych czynności[314].

---

311 A. Cavoukian, *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*, https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf [dostęp: 24.06.2025].

312 M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, s. 208.

313 Warto zauważyć, iż dotychczasowa praktyka organów nadzorczych wskazuje, że zasada ta powinna być urzeczywistniona również w przypadku, gdy administrator pozyskuje dane osobowe w sposób tradycyjny (papierowy), zob. decyzja hiszpańskiego organu nadzorczego z 25 lutego 2020 r. w sprawie *HM Hospitales*, https://www.aepd.es/es/documento/ps-00187-2019.pdf [dostęp: 24.06.2025]; zob. również decyzja hiszpańskiego organu nadzorczego z 23 lipca 2020 r. w sprawie *Banco Bilbao Vizcaya Argentaria S.A.*, https://www.aepd.es/es/documento/ps-00134-2020.pdf [dostęp: 24.06.2025].

314 European Union Agency for Network and Information Security, *Privacy and Data Protection by Design – from policy to engineering*, 2014, s. 11.

Zgodnie z art. 32 RODO administrator i podmiot przetwarzający, wdrażając odpowiednie środki zabezpieczeń, biorą pod uwagę stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Brak jest precyzyjnie określonego katalogu środków i procedur, które należałoby wdrożyć, ponieważ zależą one od przeprowadzonej analizy ryzyka. Określono jednak przykładowe środki, które mogłyby zostać wdrożone przez administratora i podmiot przetwarzający. Należą do nich:

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

Praktyka stosowania RODO przez organy nadzorcze pokazuje jednak, że wymagają one niekiedy standardów bezpieczeństwa niemożliwych do wdrożenia. Dla przykładu można przywołać sprawę, w której Prezes Urzędu Ochrony Danych Osobowych, pomimo że przeprowadzony u administratora audyt nie wykazał nieprawidłowości, a zastosowane rozwiązania były adekwatne do zidentyfikowanych zagrożeń, nałożył karę administracyjną, wskazując na nieumyślny charakter naruszenia i niedochowanie należytej staranności[315].

W przypadku organów publicznych wydaje się, że rozsądne byłoby stosowanie zabezpieczeń określonych w rozporządzeniu o kra-

[315] ZSPR.421.2.2019.

jowych ramach interoperacyjności, które w wielu sytuacjach znajdują swoje odzwierciedlenie w RODO[316]. Przykłady takich obowiązków i ich odpowiedników w RODO przedstawia tabela 1.

Tabela 1. Analiza obowiązków wynikających z Rozporządzenia KRI i RODO

Obowiązek	Rozporządzenie KRI	RODO
obowiązek przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy	§ 20 ust. 2 pkt 2	art. 35
dbanie o nadawanie i aktualizację uprawnień personelu mającego dostęp do danych	§ 20 ust. 2 pkt 4 i 5	zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania (art. 32 ust. 1 pkt b RODO)
zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami	§ 20 ust. 2 pkt 7, 9 i 11 rozporządzenia KRI	
obowiązek zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych	§ 20 ust. 2 pkt 12 rozporządzenia KRI	zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego (art. 32 ust. 1 pkt b i c RODO)

[316] Zob. W. Dziomdziora, *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021, s. 89–90.

Obowiązek	Rozporządzenie KRI	RODO
obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji	(§ 20 ust. 2 pkt 14 rozporządzenia KRI)	obowiązek regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (art. 32 ust. 1 pkt d RODO)

Źródło: opracowanie własne.

Odrębny zakres obowiązków nałożony został w ramach dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii na tzw. operatorów kluczowych, tj. podmioty publiczne lub prywatne należące do następujących sektorów: energetyki, transportu, bankowości, infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną i jej dystrybucję, infrastruktury cyfrowej, które to podmioty świadczą usługę mającą kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, świadczenie tej usługi zależy od sieci i systemów informatycznych oraz incydent miałby istotny skutek zakłócający dla świadczenia tej usługi. Na podmiotach tych spoczywają różnorakie obowiązki w zakresie zapewnienia bezpieczeństwa cybernetycznego, takie jak:

1) konieczność wdrożenia systemu zarządzania bezpieczeństwem cybernetycznym,
2) przygotowanie do obsługi incydentu i jego obsługa;
3) zgłoszenie incydentu;
4) powołanie struktur wewnętrznych odpowiedzialnych za cyberbezpieczeństwo, przeprowadzanie regularnych audytów bezpieczeństwa systemu informacyjnego.

Dyrektywa NIS[317], zastąpiona obecnie przez dyrektywę NIS 2[318], została transponowana do polskiego porządku prawnego ustawą o krajowym systemie cyberbezpieczeństwa. Precyzuje i rozszerza ona obowiązki nałożone na kluczowych operatorów, wskazując na zobowiązanie ich do m.in. prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu i dostosowania do niego środków bezpieczeństwa, takich jak: bezpieczna eksploatacja systemu, bezpieczeństwo fizyczne systemu (w tym kontrola dostępu), bezpieczeństwo i ciągłość dostaw usług, które mają wpływ na świadczenie usługi kluczowej, utrzymanie planów działania umożliwiających ciągłość świadczenia usługi, ciągłe monitorowanie systemu zapewniającego świadczenie usługi. Zobowiązani są oni również do przeprowadzenia analizy ryzyka dotyczącej operatora sytuacji i oceny przygotowania go do poradzenia sobie z ryzykami[319].

7.5. Procedury służące zabezpieczeniu dokumentów zawierających informacje niejawne oraz objęte tajemnicą

Przyznanie informacjom charakteru niejawnego lub objęcie ich tajemnicą zawodową lub inną tajemnicą prawnie chronioną wiąże się z koniecznością zabezpieczenia dokumentów zawierających wskazanego rodzaju informacje przed nieuprawnionym ich ujaw-

[317] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. L 194 z 19.07.2016 r.).

[318] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. L 333 z 27.12.2022 r., s. 80–152).

[319] W. Dziomdziora, *op. cit.*, s. 28.

nieniem. Niezbędne do tego celu są specjalne procedury przewidziane w przepisach prawa powszechnie obowiązującego. **Kluczowe w tym kontekście znaczenie mają przepisy k.p.k., a mianowicie art. 225 i 226**.

Pierwszy ze wskazanych wyżej przepisów określa „zasady postępowania z zatrzymanymi lub znalezionymi w toku przeszukania dokumentami zawierającymi informacje niejawne lub wiadomości objęte tajemnicą zawodową lub inną tajemnicą prawnie chronioną albo o charakterze osobistym (art. 225 § 1 i 2 KPK), a także z dokumentami obejmującymi okoliczności związane z wykonywaniem funkcji obrońcy (art. 225 § 3 KPK)”[320]. Jak wynika z rozwiązań przyjętych na tle tego przepisu, w sytuacji, gdy kierownik instytucji państwowej lub samorządowej albo też osoba, u której dokonano zatrzymania rzeczy lub u której przeprowadza się przeszukanie, oświadczy, że wydane lub znalezione przy przeszukaniu pismo lub inny dokument zawiera informacje niejawne lub wiadomości objęte tajemnicą zawodową (np. tajemnica adwokacka, tajemnica radcowska, tajemnica notarialna, tajemnica lekarska, tajemnica doradcy podatkowego) lub inną tajemnicę prawnie chronioną, albo ma charakter osobisty, to organ przeprowadzający czynność (np. policja, ABW) przekazuje niezwłocznie pismo lub inny dokument bez jego odczytania prokuratorowi lub sądowi w opieczętowanym opakowaniu. Trybu, o którym mowa, nie stosuje się do pism lub innych dokumentów, które zawierają informacje niejawne o klauzuli „zastrzeżone” lub „poufne” albo dotyczą tajemnicy zawodowej lub innej tajemnicy prawnie chronionej, jeżeli ich posiadaczem jest osoba podejrzana o popełnienie przestępstwa, ani w stosunku do pism lub innych dokumentów o charakterze osobistym, których jest ona posiadaczem, autorem lub adresatem[321].

---

[320] J. Skorupka, *Komentarz do art. 225*, [w:] J. Skorupka (red.), *Kodeks postępowania karnego. Komentarz*, Warszawa 2023, Legalis.

[321] Art. 225 § 2 k.p.k.

Z odmiennym trybem postępowania mamy do czynienia w przypadku, gdy dokumenty zawierają informacje objęte tajemnicą obrońcy. Jak wynika bowiem z art. 225 § 3 k.p.k., jeżeli obrońca (tj. adwokat lub radca prawny od 1 lipca 2015 r.) lub inna osoba, od której żąda się wydania rzeczy lub u której dokonuje się przeszukania, oświadczy, że wydane lub znalezione w toku przeszukania pisma lub inne dokumenty obejmują okoliczności związane z wykonywaniem funkcji obrońcy, organ dokonujący czynności (np. policja, ABW) pozostawia te dokumenty wymienionej osobie bez zapoznawania się z ich treścią lub wyglądem. Jeżeli jednak oświadczenie osoby niebędącej obrońcą budzi wątpliwości, organ dokonujący czynności przekazuje te dokumenty – z zachowaniem określonej w poprzednim akapicie procedury – sądowi, który po zapoznaniu się z dokumentami zwraca je w całości lub w części w opieczętowanym opakowaniu osobie, od której je zabrano, albo wydaje postanowienie o ich zatrzymaniu dla celów postępowania[322]. W doktrynie jednak pewne wątpliwości pojawiają się odnośnie do tego, czy aplikanta adwokackiego i radcowskiego należy uznać za obrońcę, czy inną osobę. Na przykład Tomasz Grzegorczyk pojęcia „obrońca" i „wykonywanie funkcji obrońcy" użyte w art. 225 § 3 k.p.k. rozumie szeroko, tj. nie tylko jako obrońcę w postępowaniu karnym, ale i w innych postępowaniach przewidzianych przez ustawy, w jakich „instytucja ta funkcjonuje, choćby nie był to adwokat, np. w postępowaniu dyscyplinarnym czy o wykroczenie"[323]. Według Piotra Hofmańskiego obrońcą w rozumieniu art. 225 § 3 k.p.k. jest „osoba wpisana na listę adwokatów, a więc osoba, która może wykonywać funkcję obrońcy w procesie karnym"[324]. To z kolei oznacza, że aplikanta adwokac-

[322] Art. 225 § 3 k.p.k.

[323] T. Grzegorczyk, *Kodeks postępowania karnego oraz ustawa o świadku koronnym. Komentarz*, Warszawa 2008, s. 504.

[324] P. Hofmański, *Komentarz do art. 225 Kodeksu postępowania karnego*, [w:] P. Hofmański (red.), *Kodeks postępowania karnego*, t. 1, *Komentarz do arty-*

kiego, jak i aplikanta radcowskiego należy uznać za inną osobę. Potwierdza to także art. 77 u.p.a. (odpowiednio art. 35^1 u.r.p.), który stanowi „po sześciu miesiącach aplikacji adwokackiej aplikant adwokacki może zastępować adwokata przed sądami, organami ścigania, organami państwowymi, samorządowymi i innymi instytucjami, z wyjątkiem Sądu Najwyższego, Naczelnego Sądu Administracyjnego, Trybunału Konstytucyjnego i Trybunału Stanu". Ponadto pewne zastrzeżenia budzi treść art. 225 § 3 zd. 2 k.p.k. „Skoro przyjmuje się, że tajemnica obrońcy ma charakter bezwzględny to wskazany przepis na podstawie którego istnieje możliwość zabezpieczenia dokumentów objętych tą tajemnicą – w razie pojawienia się wątpliwości co do oświadczenia innej osoby – podważa jej charakter. Warto dodać, że TK uznał przecież, że: «jedynym przepisem Konstytucji, na którym można oprzeć bezwzględny nakaz zachowania tajemnicy zawodowej przez przedstawiciela zawodu prawniczego, jest art. 42 ust. 2, przewidujący prawo do obrony. Z przepisu tego niewątpliwie wynika konstytucyjne prawo każdej osoby, przeciwko której prowadzone jest postępowanie karne, do nieskrępowanego kontaktu z obrońcą. To prawo […] jest zagwarantowane przez kodeks postępowania karnego w sposób niepodważalny […]. Dlatego w sytuacji, gdy ustawodawca uznaje prawo do korzystania z pomocy obrońcy za wartość konstytucyjną (art. 42 ust. 2 Konstytucji)[325]» to wydaje się, że powinien on w sposób bezwzględny chronić tajemnicę obrońcy. Tymczasem okazuje się, że tak nie jest, ponieważ w razie pojawienia się wątpliwości co do oświadczenia innej osoby niż obrońca, organ dokonujący czynności przekazuje dokumenty objęte tajemnicą obrońcy sądowi z zachowaniem rygorów określonych w art. 225 § 3 k.p.k. Być może w takiej sytuacji należałoby odstąpić od zabezpieczenia dokumentów do czasu zaję-

---

kułów 1–296, Warszawa 2011, s. 1254. Por. M. Rusinek, *Tajemnica zawodowa i jej ochrona w polskim procesie karnym*, Warszawa 2007, s. 192.

[325] Wyrok TK z dnia 22 listopada 2004 r., SK 64/03.

cia stanowiska w tej kwestii przez samego obrońcę (dotyczyłoby to oczywiście tych przypadków gdy złożenie takiego oświadczenia jest możliwe), co zapewniłoby wówczas charakter bezwzględny tej tajemnicy. Ponadto niewykluczone jest, że inna osoba (np. pracownik kancelarii) nie będzie wiedziała o możliwości złożenia oświadczenia we wskazanych wyżej przypadkach, co może wiązać się z tym, że w sytuacji gdy dokument zawiera informacje stanowiące tajemnicę zawodową, będzie – ze względu na brak oświadczenia – mógł zostać zweryfikowany przez organ dokonujący zatrzymania rzeczy lub przeszukania. Wydaje się, że w celu uniknięcia takich sytuacji, adwokaci jak i radcy prawni powinni poinformować o takim uprawnieniu swoich pracowników"[326].

Drugi ze wskazanych wcześniej przepisów, tj. art. 226 k.p.k., odnosi się do procedury wykorzystania dokumentów jako dowodów w procesie karnym. Zgodnie z tym przepisem „w kwestii wykorzystania dokumentów zawierających informacje niejawne lub tajemnicę zawodową, jako dowodów w postępowaniu karnym, stosuje się odpowiednio zakazy i ograniczenia określone w art. 178–181. Jednakże w postępowaniu przygotowawczym o wykorzystaniu, jako dowodów, dokumentów zawierających tajemnicę lekarską decyduje prokurator". Przyjęcie takiego rozwiązania oznacza, że w przypadku, gdy w dokumencie znajdują się informacje niejawne o klauzuli tajności „tajne" lub „ściśle tajne", to sąd lub prokurator zwraca się do właściwego naczelnego organu administracji rządowej o zwolnienie z tajemnicy[327]. Natomiast gdy dokument zawiera informacje niejawne o klauzuli tajności „zastrzeżone" lub „poufne" albo informacje objęte tajemnicą związaną z wykonywanym zawodem lub funkcją, to wówczas sąd lub prokurator w drodze postanowienia zwalnia z tajemnicy[328]. Jeśli chodzi

[326] M. Jabłoński, J. Węgrzyn, *Ochrona tajemnic…*, s. 192.
[327] Zob. art. 179 § 3 k.p.k.
[328] Zob. art. 180 § 1 k.p.k.

o dokumenty zawierające informacje objęte tajemnicą notarialną, adwokacką, radcowską, doradcy podatkowego lub dziennikarską[329], należy podkreślić, że w takim przypadku mogą one zostać wykorzystane tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. W postępowaniu przygotowawczym w przedmiocie wykorzystania dokumentów objętych wskazaną wyżej tajemnicą jako dowodów – decyduje sąd na posiedzeniu bez udziału stron, w terminie nie dłuższym niż 7 dni od daty doręczenia wniosku prokuratora. Na postanowienie sądu przysługuje zażalenie[330]. Należy przy tym zaznaczyć, że jeżeli dokumenty zawierają tajemnicę obrońcy, wówczas nie mogą one stanowić dowodu w sprawie[331]. W przypadku zaś tajemnicy lekarskiej art. 226 k.p.k. przewiduje wyjątek. Mianowicie w postępowaniu przygotowawczym o wykorzystaniu jako dowodów dokumentów zawierających tajemnicę lekarską decyduje prokurator.

[329] Odnośnie do tajemnicy dziennikarskiej należy podkreślić, że jeżeli dokumenty zawierają informacje stanowiące tę tajemnicę, to wówczas zwolnienie z tajemnicy dziennikarskiej – zgodnie z art. 180 § 3 k.p.k. – nie może dotyczyć danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnienie powyższych danych. Przy czym, zgodnie z art. 180 § 4 k.p.k., powyższe ograniczenie nie stosuje się, jeżeli informacja dotyczy przestępstwa, o którym mowa w art. 240 § 1 k.p.k.

[330] Zob. art. 180 § 2 k.p.k.

[331] Zob. art. 178 pkt 1 k.p.k.

Rozdział VIII

Realizacja praw osób, których dane dotyczą – aspekty formalne

Odnosząc się do zagadnienia realizacji praw osób, których dane dotyczą, należy w pierwszej kolejności wskazać katalog praw podmiotu danych, który obejmuje:

1) prawo dostępu do danych osobowych (art. 15 RODO);
2) prawo do sprostowania danych (art. 16 RODO);
3) prawo do usunięcia danych zwane także prawem do bycia zapomnianym (art. 17 RODO);
4) prawo do ograniczonego przetwarzania (art. 18 RODO);
5) prawo do przenoszenia danych (art. 20 RODO);
6) prawo do sprzeciwu (art. 21 RODO);
7) prawo do niepodlegania decyzjom, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu (art. 22 RODO).

Oprócz wskazanych wyżej praw istotne znaczenie z punktu widzenia osoby, której dane dotyczą, mają także obowiązki informacyjne wynikające z art. 13 i 14 RODO. Ich realizacja umożliwia m.in. weryfikację, czy przetwarzane przez administratora dane osoby, której one dotyczą, są zgodne z prawem. Przekazanie osobie, której dane dotyczą (podmiotowi danych) informacji w postaci klauzul informacyjnych, które odnoszą się do procedury zbierania i przetwarzania danych osobowych, pozwala jej w każdym czasie wystąpić z żądaniem realizacji wskazanych wyżej praw, oczywiście o ile zajdą ku temu odpowiednie przesłanki.

W praktyce **realizacja żądania praw podmiotu danych** ma formę wniosku kierowanego do administratora lub współadministratora[332]. W przypadku stosunku współadministrowania konieczne jest, aby współadministratorzy w drodze wspólnych uzgodnień (co następuje w formie tzw. umowy o współadministrowanie) w przejrzysty sposób określili odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonania przez osobę, której dane dotyczą, przysługujących jej praw oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają[333]. Co również istotne, zasadnicza treść tych uzgodnień jest udostępniana podmiotom, których dane dotyczą[334]. „Za zasadniczą uznać należy tę część uzgodnień pomiędzy administratorami, która ujawnia ich tożsamość, cele i sposoby przetwarzania danych, a także zakresy ich odpowiedzialności dotyczącej wypełniania obowiązków wynikających z tego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw”[335]. Artykuł 26 RODO – bo o nim tu mowa – „nie wskazuje wprawdzie sposobu udostępniania osobom, których dane dotyczą, treści uzgodnień […] jednak mając na względzie istotę tej regulacji oraz to, że na gruncie RODO osoba, której dane dotyczą i ochrona jej interesów pozostaje w centrum regulacji, za uzasadnione przyjmować należy możliwe szerokie kolportowanie tej informacji w każdy sposób zapewniający

[332] Ze stosunkiem współadministrowania mamy do czynienia, jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, art. 26 ust. 1 RODO.

[333] Art. 26 ust. 1 RODO.

[334] Art. 26 ust. 2 RODO.

[335] M. Sakowska-Baryła, *Komentarz do art. 26*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie*…, s. 306.

efektywne poinformowanie podmiotu danych przetwarzanych w warunkach współadministrowania"[336]. Czynność ta może nastąpić np. poprzez zamieszczenie treści uzgodnień na stronach internetowych współadministratorów lub za pośrednictwem punktu kontaktowego, o którym mowa w art. 26 ust. 1 zd. 3 RODO[337]. Niezależnie jednak od poczynionych ustaleń osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wobec każdego z administratorów[338], co świadczy o pozostawieniu podmiotowi danych swobody w wyborze adresata żądania, a tym samym i skutecznej jego realizacji.

W procesie realizacji praw podmiotu danych nie można wykluczyć sytuacji wystąpienia przez osobę, której dane dotyczą, z przedmiotowym żądaniem do podmiotu przetwarzającego[339] (tzw. procesor). W praktyce przetwarzanie przez podmiot przetwarzający danych osobowych w imieniu administratora odbywa się na podstawie umowy (tzw. umowa powierzenia przetwarzania danych osobowych) lub innego instrumentu prawnego (np. porozumienia administracyjnego zawieranego między podmiotami ze sfery publicznej, tj. organami administracji publicznej)[340], w których należy określić elementy treści wynikające z art. 28 ust. 3 RODO. Wśród nich jest i ten, który przewiduje, aby podmiot przetwarzający w miarę możliwości pomagał administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III[341]. W zależności więc od treści umowy

---

[336] *Ibidem*.

[337] *Ibidem*, s. 307.

[338] Art. 26 ust. 3 RODO.

[339] Podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane w imieniu administratora, art. 4 pkt 8) RODO.

[340] P. Fajgielski, *Komentarz do art. 28*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa*…

[341] Art. 28 ust. 3 lit. e) RODO.

pomoc w realizacji tego obowiązku może polegać na przekazaniu administratorowi wniosku podmiotu danych (np. o ich usunięcie) lub na jego realizacji przez podmiot przetwarzający. Bez względu jednak na przyjęte ustalenia należy mieć na uwadze, że odpowiedzialność za realizację praw podmiotu danych ponosi zawsze administrator.

Wniesienie przez osobę, której dane dotyczą, wniosku o realizację przysługujących jej praw nakłada na podmiot zobowiązany (tj. administratora, współadministratora lub podmiot przetwarzający) obowiązek podjęcia określonych czynności związanych z jego realizacją. Pierwszą czynnością jest **weryfikacja wniosku i tożsamości wnioskodawcy**, co jest szczególnie istotne, aby nie dopuścić do sytuacji udostępnienia danych osobie nieuprawnionej. Na tym etapie należy zweryfikować przedmiot żądania oraz ustalić, czy podmiot zobowiązany przetwarza dane osobowe wnioskującego. Weryfikacja tożsamości wnioskodawcy odbywa się w sposób przyjęty przez administratora po uprzednim jego dostosowaniu do charakteru przetwarzanych danych. Weryfikacja, o której mowa, może więc polegać m.in. na podaniu wysłanego przez administratora kodu weryfikacyjnego przesłanego w formie SMS-a, zalogowaniu się do konta, za pomocą którego administrator świadczy określone usługi, czy udzieleniu odpowiedzi na zadawane przez administratora pytania. W kwestii tej wypowiedział się także PUODO, podkreślając, że „praktyka żądania dodatkowych danych weryfikacyjnych może wydawać się zbyt restrykcyjna, jednak nie można jej uznać za nadmierną w przedstawionej sytuacji. Żądanie dodatkowych danych identyfikacyjnych ma na celu maksymalną ochronę samych danych znajdujących się w bazie, jak również procedury ich udostępniania. Takie zabezpieczenie ma na celu zapobieżenie udostępnieniu danych osobie nieupoważnionej, przetwarzanych przez B. S.A informacji stanowiących tajemnicę bankową. Wobec tego, samo udostępnienie danych żądanych na podstawie art. 33 ustawy, powinno nastąpić po uprzedniej, rzetelnej weryfikacji tożsamości osoby wnioskodawcy.

Podwójna weryfikacja za pomocą numeru PESEL oraz serii i numeru dowodu osobistego pozwala ustalić w sposób niebudzący wątpliwości tożsamość osoby wnioskodawcy. Należy również podkreślić, że przy przekazywaniu tak istotnych informacji B. S.A powinien zachować szczególną uwagę i mieć pewność, że przekazywane informację są udostępnianie osobie uprawnionej"[342]. W innej sprawie PUODO zwrócił zaś uwagę, że „weryfikacja tożsamości powinna obejmować cyfrową identyfikację osoby, której dane dotyczą, na przykład poprzez mechanizm uwierzytelniania, taki jak te same dane uwierzytelniające, których osoba, której dane dotyczą, używa, by zalogować się do usług internetowych oferowanych przez administratora. Motyw 63 preambuły RODO stanowi z kolei, że w miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji. Z kolei zgodnie z motywem 64 preambuły RODO, administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą"[343].

W procesie weryfikacji tożsamości osoby występującej z żądaniem realizacji przysługujących jej praw nie można wykluczyć, że administrator może mieć **uzasadnione wątpliwości co do tożsamości tej osoby**. W takiej sytuacji może on zażądać dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości[344] przy zachowaniu

[342] Decyzja PUODO z dnia 10 grudnia 2018 r., ZSPR.440.783.2018.
[343] Decyzja PUODO z dnia 20 grudnia 2018 r., ZSPU.440.99.2018.
[344] Art. 12 ust. 6 RODO.

wyrażonej w art. 5 ust. 1 lit. c) RODO zasady minimalizacji danych. „Jest to o tyle zrozumiałe, że stosując komunikację elektroniczną, nie korzystamy zazwyczaj z bezpiecznych podpisów i innych środków dających wysoki stopień pewności co do tożsamości użytkownika. Administratorzy też nie zawsze dysponują stosownymi możliwościami, a typowa wiadomość mailowa jest na tyle mało wiarygodna, że uzasadnione wątpliwości mogą pojawić się nader często. Oczywiście w przypadku wcześniejszego potwierdzenia adresu e-mail przez wnioskodawcę administrator nie powinien utrudnić uzyskania informacji w tej drodze”[345]. Oprócz wskazanej wyżej sytuacji należy mieć na uwadze jeszcze jedną, a mianowicie tę, która dotyczy **przetwarzania informacji niewymagających identyfikacji**. Ma ona zastosowanie w przypadku, gdy cele, w których administrator przetwarza dane osobowe, nie wymagają (np. w celu statystycznym) lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, administrator nie ma wówczas obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do niniejszego rozporządzenia[346]. Jeżeli we wskazanych wyżej przypadkach administrator może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym tę osobę. W takich przypadkach zastosowania nie mają art. 15–20, chyba że osoba, której dane dotyczą, w celu wykonania praw przysługujących jej na mocy tych artykułów dostarczy dodatkowych informacji pozwalających ją zidentyfikować[347]. „Sytuacja taka może wystąpić w razie chęci dostępu do danych z monitoringu wizyjnego, gdy usiłujemy ustalić, kto «przetarł» nasz samochód na parkingu przed centrum handlowym. Może też wystąpić w innych okolicznościach.

---

[345] K. Wygoda, *Komentarz do art. 12*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie*…, s. 204.

[346] Art. 11 ust. 1 RODO.

[347] Art. 11 ust. 2 RODO.

Ważne, że dostarczenie «dodatkowych informacji pozwalających zidentyfikować» wnioskodawcę nie polega na przedstawieniu dowodu osobistego, tylko na podaniu szczegółów pozwalających «namierzyć» konkretne informacje o wnioskodawcy w naszych zasobach"[348].

W procesie realizacji praw przysługujących osobie, której dane dotyczą, istotne znaczenie dla tej osoby ma **forma wniesionego żądania oraz termin jego obsługi**. Przepisy RODO pozostawiają w tym zakresie pełną swobodę podmiotowi danych. Wniesione żądanie może mieć zatem formę pisemną, elektroniczną lub ustną, choć w tym ostatnim przypadku wydaje się, że będzie ona rzadko stosowana ze względów dowodowych. Administrator w celu ułatwienia wykonania praw przysługujących osobie, której dane dotyczą, może przygotować np. przeznaczony do tego celu formularz, platformę, za pośrednictwem której możliwa będzie realizacja żądania, niemniej jednak wskazane przez administratora sposoby wystąpienia z przedmiotowym żądaniem nie są wiążące dla podmiotu danych. Istotne znaczenie w procesie tym prawodawca unijny przypisał – prowadzonej z podmiotem danych – transparentnej komunikacji. Jak wynika bowiem z treści art. 12 ust. 1 RODO, administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem prowadzić z osobą, której dane dotyczą, komunikację[349]. „Podjęcie odpowiednich

---

[348] M. Gawroński, *Przetwarzanie danych niewymagających identyfikacji*, [w:] M. Gawroński (red.), *op. cit.*, s. 164.

[349] Do zasady przejrzystości odnosi się także motyw 58 RODO. Zgodnie z jego treścią „zasada przejrzystości wymaga, by wszelkie informacje kierowane do ogółu społeczeństwa lub osoby, której dane dotyczą, były zwięzłe, łatwo dostępne i zrozumiałe, by były formułowane jasnym i prostym językiem, a w stosownych przypadkach, dodatkowo wizualizowane. Informacje te mogą być przekazywane w formie elektronicznej, na przykład za pomocą strony internetowej, gdy są kierowane do ogółu społeczeństwa. Dotyczy to w szczególności sytuacji, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że osobie, której dane dotyczą, trudno jest dowiedzieć się i zrozumieć, czy dotyczące jej dane osobowe są zbierane, przez kogo oraz w jakim celu, na przykład w przypadku reklamy w internecie.

środków przez administratora to […] nakaz kierujący go w stronę zasad prakseologicznych związanych z projektowaniem procesów, które mają się zakończyć uzyskaniem odpowiedniej jakości efektu. […]. W przypadku podejmowania działań zmierzających do prowadzenia wszelkiej komunikacji na mocy art. 15–22 i 34 RODO w sprawie przetwarzania schemat postępowania administratora będzie ulegał modyfikacji. Administrator w zależności od rodzaju wniosku czy relacji będzie się musiał zachować adekwatnie do potrzeb. Wspólną osią wszystkich podejmowanych działań mieszczących się w tej grupie powinna być następująca sekwencja:

1) ocena i/lub identyfikacja kategorii osób, których dane są i/lub mają być przetwarzane, do których przynależy osoba, z którą się komunikujemy;
2) ocena możliwości poznawczych osoby, z którą komunikujemy się na tle grupy, do której została zakwalifikowana (z uwagi na ewentualną konieczność zmodyfikowania formy przekazu, np. osoba dorosła, ale niedowidząca czy niewidoma, o czym poinformowała nas we wniosku, być może będzie wymagała zamiany formatu korespondencji na poddający się mechanicznemu odczytowi przez typowe oprogramowanie umożliwiające głośne czytanie);
3) przygotowanie odpowiednio zindywidualizowanej odpowiedzi na wniosek dostosowanej do możliwości poznawczych adresata (w jakim zakresie jest to obligatoryjne i możliwe?);
4) przekazanie korespondencji w formie niezakłócającej i/lub nieutrudniającej procesu zapoznania się z nimi (oraz zrozumienia go) przez adresata”[350].

Zważywszy że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty – gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć”.

[350] K. Wygoda, *Przejrzyste informowanie, przejrzysta komunikacja i tryb wykonywania praw – obowiązki administratora danych*, [w:] B. Fischer, M. Sakowska-Baryła (red.), *Realizacja praw osób*…, s. 81 i n.

Spełnienie więc wymogu prowadzenia z podmiotem danych transparentnej komunikacji wiąże się z koniecznością przygotowania przez administratora zrozumiałego i przejrzystego przekazu, tj. takiego, który jest łatwy w odbiorze (pozbawiony specjalistycznych wyrażeń) i rzeczowy, udostępniony w czytelnej formie, na którą składa się zarówno układ tekstu, jak i jego czcionka. Jeśli chodzi o **termin obsługi żądania**, to należy podkreślić, że administrator zobowiązany jest bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania, udzielić osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem wniesionym na podstawie art. 15–22 RODO. W razie potrzeby termin ten może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, przy czym w terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia[351]. W sytuacji jednak, gdy administrator nie podejmie działań w związku z żądaniem osoby, której dane dotyczą (np. nie usunie danych), to wówczas niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje tę osobę o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem[352]. Mając powyższe na względzie, należy podkreślić, że bieg „miesięcznego terminu rozpoczyna dzień otrzymania żądania przez administratora, a nie np. dzień nadania korespondencji z takim żądaniem u operatora pocztowego. Mimo że przyjęte w treści komentowanego przepisu sformułowanie w postaci «informacji o działaniach podjętych w związku z żądaniem» może rodzić trudności interpretacyjne, przyjąć należy, że art. 12 co do zasady zobowiązuje administratora, aby w terminie nieprzekraczającym 1 miesiąca dokonał merytorycznej

[351] Art. 12 ust. 3 RODO.
[352] Art. 12 ust. 4 RODO.

oceny treści żądania i uczynił mu zadość (np. poprzez udzielenie informacji czy usunięcie danych) lub odmówił jego spełnienia. Przedłużenie tego terminu jest bowiem dopuszczalne jedynie z uwagi na skomplikowany charakter żądania lub liczbę żądań"[353]. Przykładem takiej sytuacji jest sprawa, w której Rektor Uniwersytetu w odpowiedzi na wniosek skarżącego w przedmiocie udzielenia informacji dotyczącej sposobu przetwarzania danych osobowych – wyjaśnił, że z uwagi na to, że skarżący był „studentem i doktorantem U […], to jego dane osobowe zostały zawarte w dokumentacji przebiegu studiów, a ponadto znajdują się w dokumentach związanych z postępowaniami sądowoadministracyjnymi, których skarżący jest stroną (m.in. wyroki, skargi do sądu). Do korespondencji tej został ponadto załączony plik, w formie skompresowanego i zabezpieczonego hasłem archiwum, zawierający skany dokumentów będących w posiadaniu różnych jednostek U […]. Tym samym Uniwersytet […] wykonał ciążące na nim obowiązki zgodnie z wymogami wspomnianego już rozporządzenia Rady (UE). […]. Rektor Uniwersytetu […] dodał, że załatwienie wniosku skarżącego było nad wyraz trudnym logistycznie i faktycznie procesem. Już sam fakt, że jego osoba i liczne sprawy z nim związane, głównie spory, absorbowały liczne jednostki organizacyjne U […], kłopotem było ustalenie, które jednostki mogą posiadać jakiekolwiek dane osobowe skarżącego. Poza tym ilość dokumentacji wymagającej zgromadzenia i zeskanowania też była niebagatelna, co wymagało od uczelni dużego nakładu czasu by móc zrealizować żądanie skarżącego"[354]. Ze względu więc na skomplikowany charakter żądania, termin załatwienia wniosku został wydłużony o miesiąc.

W procesie realizacji praw przysługujących osobie, której dane dotyczą, zarówno komunikacja, jak i wszelkie podejmowane przez

---

[353] J. Łuczak, *Komentarz do art. 12*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 472.

[354] Postanowienia WSA w Łodzi z dnia 08 lutego 2019 r., II SAB/Łd 176/18.

podmiot zobowiązany działania są wolne od opłat. Jeżeli jednak żądania podmiotu danych są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
b) odmówić podjęcia działań w związku z żądaniem (art. 12 ust. 5 RODO).

Użyte we wskazanym przepisie zwroty niedookreślone mogą w praktyce stwarzać problemy z identyfikacją żądania. W doktrynie podkreśla się, że żądanie ewidentnie nieuzasadnione to żądanie pozorne, a więc takie, w którym „żądający, wskazując konkretne uprawnienie (czyli powołując się na art. 15, 16 17 itp. RODO), w rzeczywistości chce otrzymać informacje wykraczające poza ramy uprawnień wskazanych w RODO bądź formułuje takie kryteria lub sposoby generowania informacji lub formy ich przekazania, które nie są niezbędne lub możliwe do realizacji z punktu widzenia wywiązywania się przez administratora z obowiązków informacyjnych lub komunikacyjnych. W szczególności chodzi tu o sytuacje, w których istnieją negatywne przesłanki realizacji żądania zawarte bezpośrednio w przepisach RODO (na przykład art. 17 ust. 3 RODO)”[355]. Z kolei żądanie nadmierne „to takie, które przekracza granice wynikające z uprawnień zagwarantowanych osobie w treści RODO. Administrator będzie więc zmuszony do każdorazowej oceny okoliczności faktycznych i wcześniej (lub równolegle) realizowanych żądań kierowanych do niego przez tego samego uprawnionego. Dokonując

[355] M. Jabłoński, K. Wygoda, *Praktyczne znaczenie podstawowych pojęć RODO – wybrane zagadnienia*, Wrocław 2019, s. 111. Na temat przesłanek wyłączających prawo do bycia zapomnianym zob. M. Jabłoński, J. Węgrzyn, *Prawo do bycia zapomnianym*, Wrocław 2021, s. 182 i n.

oceny, administrator musi więc wziąć pod uwagę takie elementy, jak: zakres i czas oddzielający kolejne wystąpienia, ich tożsamość przedmiotową oraz fakt, czy i jakie zmiany dotyczą przetwarzania danych, a także zasadności ponownego powoływania się na te same prawa przez występującego (w odniesieniu do zmiany stanu faktycznego, które zaistniały od czasu poprzedniego żądania). Warto jednak zaznaczyć, że żądaniem nadmiernym może być oczywiście to samo żądanie powtarzane cyklicznie przez tego samego uprawnionego. Konieczne jednak będzie wykazanie przez administratora, że wcześniejsze jego działania dotyczyły przekazania informacji tożsamych z tymi, które otrzyma występujący. Jednak w tym wypadku będziemy mieli do czynienia z żądaniem nadmiernym ze względu na swój ustawiczny charakter"[356].

Realizacja żądania podmiotu danych wiąże się nie tylko ze wskazanymi wyżej czynnościami podejmowanymi przez podmiot zobowiązany. Na mocy bowiem art. 19 RODO **administrator zobowiązany jest poinformować o sprostowaniu lub usunięciu danych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18 – każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagało niewspółmiernie dużego wysiłku**. Ponadto administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli ona

[356] M. Jabłoński, K. Wygoda, *Praktyczne znaczenie…*, s. 112. Warto zauważyć, że wskazani autorzy przyjmują, iż „żądanie ustawiczne (nadmierne) będzie identyfikowane z takim, które będzie spełniać równocześnie co najmniej dwie przesłanki:

– dojdzie do obiektywnego stwierdzenia, że mamy do czynienia z wystąpieniem tego samego uprawnionego, czyli cały czas tej samej osoby, której dane dotyczą (tożsamość podmiotowa);

– ten sam uprawniony w sposób ciągły, powtarzalny będzie występował o to samo, co uzyskał już wcześniej od administratora (tożsamość podmiotowa)".

Zob. również: D. Kuźnicka-Błaszkowska, *Practitioners' Corner Excessive Use of Data Access Rights in the Practice of Imposing Administrative Fines*, „European Data Protection Law Review" 2024, nr 1, s. 105–110.

tego zażąda. Jak wynika z treści wskazanego przepisu, obowiązek, o którym w nim mowa, dotyczy odbiorców. W myśl art. 4 pkt 9 RODO „odbiorcą" jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania. W prezentowanym wyżej ujęciu odbiorcą będzie m.in. inny administrator lub podmiot przetwarzający (procesor). Odbiorcą nie będzie natomiast sąd, prokuratura lub policja.

Należy zauważyć, że **obowiązek powiadomienia odbiorców nie ma charakteru absolutnego**. Zwolnienie administratora z tego obowiązku jest bowiem możliwe w dwóch przypadkach, tj.

1) braku możliwości powiadomienia odbiorcy (np. zlikwidowanego podmiotu, który był odbiorcą danych[357]) lub
2) wystąpienia niewspółmiernie dużego wysiłku w celu powiadomienia odbiorcy. Z sytuacją taką będziemy mieli do czynienia „wówczas, gdy wysiłek włożony w przekazanie informacji jest nieproporcjonalny w stosunku do niedogodności spowodowanych brakiem takich informacji u osoby, której dane dotyczą"[358]. A mianowicie, gdy „dane zostały ujawnione odbiorcy wiele lat temu i administrator nie jest w stanie obecnie, pomimo podjętych prób, nawiązać z nim kontaktu"[359].

---

[357] M. Czerniawski, *Komentarz do art. 19 RODO*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *op. cit.*, s. 541.

[358] P. Barta, M. Kawecki, P. Litwiński, *Komentarz do art. 19 RODO*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie…*; zob. również M. Jabłoński, D. Kuźnicka-Błaszkowska, *op. cit.*, s. 505–518.

[359] M. Czerniawski, *op. cit.*, s. 541.

Poza tym należy mieć na uwadze rozwiązania przyjęte w przepisach szczególnych pozwalające na możliwość ograniczenia obowiązku powiadomienia odbiorcy. Jako przykład warto wskazać:

- art. 16a ust. 1 ustawy z dnia 26 maja 1982 r. – Prawo o adwokaturze (t.j. Dz. U. z 2024 r. poz. 1564), w którym wyraźnie zaznaczono, że przepisy art. 15 ust. 1 i 3, art. 18 i art. 19 RODO stosuje się w zakresie, w jakim nie naruszają obowiązku zachowania przez adwokata tajemnicy, o której mowa w art. 6;
- art. 5a ust. 1 ustawy z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz. U. z 2024 r. poz. 499), w którym wyraźnie zaznaczono, że przepisy art. 15 ust. 1 i 3, art. 18 i art. 19 RODO stosuje się w zakresie, w jakim nie naruszają obowiązku zachowania przez radcę prawnego tajemnicy, o której mowa w art. 3.

„W piśmiennictwie jako przykład zastosowania omawianego ograniczenia wskazuje się m.in. sytuację, gdy klient zakończył współpracę z kancelarią i zażądał usunięcia jego danych osobowych, w tym zawartych w projektach umów, w których znajdowały się również dane osób trzecich – wówczas informowanie odbiorców o usunięciu danych mogłoby naruszać tajemnicę zawodową”[360].

Nie ulega wątpliwości, że w procesie realizacji praw podmiotu danych przeprowadzenie wskazanych wyżej czynności jest niezbędne do skutecznego wywiązania się przez podmiot zobowiązany z nałożonych na niego obowiązków. Nie można jednak zapomnieć, że **obsługa żądania wniesionego przez podmiot danych wymaga odpowiedniego udokumentowania**, co ma bezpośredni związek z zasadą rozliczalności wyrażoną w art. 5 ust. 2 RODO. W praktyce wykazanie zasady rozliczalności w kontekście obsługi żądania podmiotu danych (realizacji praw) może nastąpić poprzez wdrożenie w danej organizacji procedury ochrony danych, której jednym z ele-

[360] P. Fajgielski, *Komentarz do art. 19 RODO*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa*…

mentów składowych jest dokument dotyczący zasad obsługi praw podmiotu danych, tj. osoby, której dane dotyczą. Warto mieć powyższe na względzie, tym bardziej że naruszenia przepisów dotyczących praw osób, których dane dotyczą, o których mowa w art. 12–22, podlegają administracyjnej karze pieniężnej w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Rozdział IX

Rola, kompetencje i zadania Inspektora Ochrony Danych

Na gruncie RODO szczególną rolę odgrywa Inspektor Ochrony Danych (IOD). Zgodnie z art. 37 rozporządzenia powinien on zostać powołany, gdy administrator lub podmiot przetwarzający spełnia chociaż jeden z poniższych warunków:

1) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
2) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
3) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Niezależnie od tego administrator i podmiot przetwarzający mogą dobrowolnie wyznaczyć inspektora ochrony danych osobowych. W takim jednak wypadku muszą oni spełnić wszystkie wymagania, jakie RODO nakłada na podmioty, które obligatoryjnie dokonały powołania IOD. Dotyczy to zarówno publikowania danych kontaktowych IOD, jak również obowiązku zawiadomienia o jego powołaniu organu nadzorczego.

Co jest szczególnie istotne, IOD **powinien cieszyć się odpowiednim stopniem niezależności**. Na podstawie art. 38 RODO można uznać, że chodzi tutaj o niezależność organizacyjną, finansową, kompetencyjną i osobistą. Służą temu gwarancje określone w przywołanym przepisie. Należą do nich: niezwłoczne i właściwe włączanie IOD we wszystkie sprawy dotyczące ochrony danych osobowych; zapewnienie zasobów niezbędnych do wykonania jego zadań; zapewnienie dostępu do operacji przetwarzania i danych osobowych; zapewnienie zasobów niezbędnych do utrzymania jego wiedzy fachowej. Administrator i podmiot przetwarzający muszą zapewnić taki sposób funkcjonowania organizacji, **aby IOD nie otrzymywał instrukcji dotyczących wykonywania jego zadań**. IOD nie może być odwoływany ani karany za wypełnienie swoich zadań. Inspektor podlega bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

Podmioty danych powinny mieć zapewnioną możliwość kontaktowania się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na gruncie RODO.

Inspektor ochrony danych ma następujące zadania:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4) współpraca z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Inspektor ochrony danych powinien posiadać odpowiednie kwalifikacje zawodowe, fachową wiedzę, w szczególności na temat prawa i praktyk w dziedzinie ochrony danych, oraz umiejętności niezbędne do wypełnienia zadań, o których mowa w art. 39 RODO. Dotyczy to zarówno wiedzy na temat prawa ochrony danych osobowych w Unii Europejskiej i Polsce, jak również znajomości specyfiki danego sektora. W przypadku organów i podmiotów publicznych IOD powinien też posiadać wiedzę w zakresie procedur administracyjnych i funkcjonowania jednostki[361]. Inspektor ochrony danych musi mieć pełną wiedzę na temat sposobu funkcjonowania i podejmowania decyzji u administratora lub podmiotu przetwarzającego, w którym wykonuje swoje zadania. IOD nie musi posiadać ukończonych studiów prawniczych, wręcz przeciwnie – w tej roli znakomicie sprawdzają się również osoby z wykształceniem technicznym.

Inspektor ochrony danych może być zatrudniony na podstawie umowy o pracę lub wykonywać swoje zadania na podstawie innego typu umowy. Nie jest też wykluczone, aby osoba ta wykonywała inne obowiązki i zadania, jednak nie powinny one powodować konfliktu interesów. W wykonywaniu swoich zadań IOD wydaje rekomendacje – ostateczną decyzję podejmuje administrator lub podmiot przetwarzający i to oni ponoszą odpowiedzialność na gruncie

[361] Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów*…

RODO. Oczywiste jest, że IOD może ponosić odpowiedzialność za np. wprowadzenie administratora w błąd lub niezachowanie należytej staranności – jest to jednak odpowiedzialność cywilnoprawna, zgodna z obowiązującą strony umową.

Bibliografia

Literatura

Abu Gholeh M., Kuźnicka-Błaszkowska D., *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych osobowych. Aspekty praktyczne*, Warszawa 2020.

Andress J., *Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie*, Gliwice 2022.

Bach-Golecka D., Stankiewicz R. (red.), *Organizacja systemu ochrony zdrowia. System Prawa Medycznego*, t. 3, Warszawa 2020.

Banaszak B., *Prawo konstytucyjne*, Warszawa 2015.

Barta P., Kawecki M., Litwiński P., *Komentarz do art. 5*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021.

Barta P., Kawecki M., Litwiński P., *Komentarz do art. 19 RODO*, [w:] P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021.

Bernaczyk M., *Źródła prawa*, [w:] *Konstytucja i prawo konstytucyjne. Zarys wykładu*, Warszawa 2021.

Bierzanek R., Symonides J., *Prawo międzynarodowe publiczne*, Warszawa 2005.

Błażewski M., Behr J., *Środki prawne ochrony danych osobowych*, Wrocław 2018.

Boehm F., *Information sharing and data protection in the area of freedom, security and justice. Towards harmonised data protection principles for information exchange at EU-level*, Berlin–Heidelberg 2012.

Botha J., Pieterse H., *Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security*, http://hdl.handle.net/10204/11946 [dostęp: 29.08.2025].

Braciak J., *Prawo do prywatności*, Warszawa 2004.

Brodzisz Z., *Komentarz do art. 307*, [w:] J. Skorupka (red.), *Kodeks postępowania karnego. Komentarz*, Warszawa 2023.

Byrski J., Hoser H., *Ocena celowości przetwarzania danych osobowych*, „ABI Expert" 2020, nr 3.

Cavoukian A., *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices and Mapping of Fair Information Practices*, https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf [dostęp: 24.06.2025].

Cooley T., *A Treatise On The Law Of Torts*, 1st ed., Chicago 1880.

Cope G.B., Jr., *Toward a Right of Privacy as a Matter of State Constitutional Law*, „Florida State University Law Review" 1977, vol. 5, iss. 4.

Corrales Compagnucci M., Minssen T., Seitz C., Aboy M., *Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Transfers in the Pharmaceutical Sector After Schrems II Invalidation of the EU-US Privacy Shield*, „European Data Protection Law Review" 2020, vol. 3.

Czapliński W., Wyrozumska A., *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 2014.

Czech M., *Umowa powierzenia przetwarzania danych osobowych jako instrument ich ochrony*, rozprawa doktorska napisana pod kierunkiem prof. dr hab. Teresy Mróz, Białystok 2019.

Czerniawski M., *Komentarz do art. 19 RODO*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Diggelmann O., Cleis M.N., *How the Right to Privacy Become a Human Right*, „Human Rights Law Review" 2014, vol. 14, iss. 3.

Dobber T. *et al.*, *Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?*, „The International Journal of Press/Politics" 2021, t. 26, nr 1.

Dobosz I., *Tajemnica korespondencji jako dobro osobiste i jej ochrona w prawie cywilnym*, Kraków 1989.

Dominiak M., Gawroński M., *Zasady przetwarzania danych osobowych*, [w:] M. Gawroński (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa 2018.

Drobek P., *Komentarz do art. 5*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Drożdżowski Ł., *Zakres ochrony danych genetycznych na gruncie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, „Forum Prawnicze" 2022, nr 4(72).

Dybka W., *Dane osobowe dotyczące konsumenta jako przedmiot świadczenia*, „Kwartalnik Prawa Prywatnego" 2023, z. 1.

Dziomdziora W., *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021.

Fajgielski P., *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław 2007.

Fajgielski P., *Komentarz do art. 5*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa 2022.

Fajgielski P., *Komentarz do art. 19 RODO*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa 2022

Fajgielski P., *Komentarz do art. 28*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa 2022

Fajgielski P., *Rzetelność jako ogólna zasada przetwarzania danych osobowych*, „Gdańskie Studia Prawnicze" 2021, nr 4(52).

Fehler W., *O pojęciu bezpieczeństwa informacyjnego*, [w:] M. Kubiak, S. Topolewski (red.), *Bezpieczeństwo informacyjne w XXI wieku*, Siedlce–Warszawa 2016.

Gałęzowska K., *Dane biometryczne a dane behawioralne*, dodatek „Monitora Prawniczego" 2022, nr 21.

Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2019.

Gawroński M., *Przetwarzanie danych niewymagających identyfikacji*, [w:] M. Gawroński (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa 2018.

Georgieva L., Kuner Ch., *Article 9*, [w:] Ch. Kuner, L.A. Bygrave, Ch. Docksey, *The EU Generall Data Protection Regulation (GDPR). A Commentary*, Oxford 2020.

Gliszczyńska-Grabias A., Sękowska-Kozłowska K., *Komentarz do art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych*, [w:] R. Wieruszowski (red.), *Międzynarodowy Pakt Praw Obywatelskich i Politycznych. Komentarz*, Warszawa 2012.

Głębocki Ł., *Umowa powierzania przetwarzania danych osobowych zgodnie z RODO*, „Informacja w Administracji Publicznej" 2018, nr 1.

Gonschior A., *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej*, [w:] D. Kornobis-Romanowska (red.), *Aktualne problemy prawa Unii Europejskiej i prawa międzynarodowego – aspekty teoretyczne i praktyczne*, Wrocław 2017.

Grabski S., *Rozliczalność, czyli dlaczego nie można zapomnieć o RODO*, „ABI Expert" 2020, nr 1.

Grzegorczyk T., *Kodeks postępowania karnego oraz ustawa o świadku koronnym. Komentarz*, Warszawa 2008.

Grzelak A., *Projekt reformy ochrony danych osobowych – czy rzeczywiście powstaje jednolity i spójny system?*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace" 2014, nr 4.

Gumularz M., Kawecki M., *Prawo do poinformowania w przypadku zbierania danych od osoby, której dane dotyczą*, [w:] B. Fisher, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą na podstawie rodo*, Wrocław 2017.

Hancock J.T., Bailenson J.N., *The Social Impact of Deepfakes*, „Cyberpsychology, Behavior, and Social Networking" 2021, t. 24, nr 3.

Hijmans H., *The European Union as a guardian of Internet privacy. The story of art 16 TFEU*, Cham 2016.

Hofmański P., *Komentarz do art. 225 Kodeksu postępowania karnego*, [w:] P. Hofmański (red.), *Kodeks postępowania karnego*, t. 1, *Komentarz do artykułów 1-296*, Warszawa 2011

Izydorczyk T., *Analiza oparta na ryzyku (risk-based approach)*, [w:] M. Kołodziej (red.), *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych*, Warszawa 2017.

Izydorczyk T., *Ocena ryzyka naruszenia praw lub wolności osób i ocena skutków dla ochrony danych* [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017.

Jabłoński M., Kuźnicka-Błaszkowska D., *„Disproportionate Effort" in the Meaning of Article 14 of the General Data Protection Regulation*, „Przegląd Prawa Konstytucyjnego" 2021, nr 6.

Jabłoński M., Radziszewski T., *Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych*, Wrocław 2012.

Jabłoński M., Węgrzyn J., *Ochrona tajemnic osób wykonujących prawnicze zawody zaufania publicznego*, Wrocław 2018.

Jabłoński M., Węgrzyn J., *Prawo do bycia zapomnianym*, Wrocław 2021.

Jabłoński M., Węgrzyn J., *Prawo dostępu do danych osobowych i ich treści*, Toruń 2023.

Jabłoński M., Węgrzyn J., *Zmiana modelu ochrony danych osobowych – podejście oparte na ryzyku, privacy by design i privacy by default*, [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017.

Jabłoński M., Wygoda K., *Dostęp do informacji i jego granice*, Wrocław 2000.

Jabłoński M., Wygoda K., *Praktyczne znaczenie podstawowych pojęć RODO – wybrane zagadnienia*, Wrocław 2019.

Jaśkowska M., *Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego*, Toruń 2002.

Kaczmarek A., Łapińska A., Miłocha A., Młotkiewicz M., *Nowa optyka w ocenie ryzyka*, „ABI Expert" 2017, nr 4.

Kalinowska N., Litwiński P., *Ocena skutków dla ochrony danych i uprzednie konsultacje – nowe obowiązki podmiotów przetwarzających dane osobowe*, „Monitor Prawniczy" 2017, nr 13.

Kawecki M., Osiej T., *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa 2017.

Kogut-Czarkowska M., *Pseudonimizacja i anonimizacja danych osobowych w badaniach naukowych – wybrane zagadnienia*, „Prawo Nowych Technologii" 2021, nr 1.

Kołodziej M., *Pseudonimizacja w RODO – kiedy i jak stosować?*, „ABI Expert" 2018, nr 2.

Kornobis-Romanowska D., *Rozporządzenie o ochronie danych osobowych – charakter prawny, zakres stosowania i skutek w prawie krajowym państw członkowskich*, [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017

Kotzur M., [w:] R. Geiger, D.E. Khan, M. Kotzurto (red.), *European Union Treaties. a commentary*, Munich 2015.

Kowalski S., *Realizacja obowiązku informacyjnego*, „ABI Expert" 2020, nr 3.

Krausova A., *Online behavior recognition: can we consider it biometric data under gdpr?*, „Masaryk University Journal of Law and Technology" 2018, vol. 12(2).

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016.

Kuczkowska E., *Glosa aprobująca do wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 13 kwietnia 2021 r., sygn. akt II SA/Wa 1898/20*, „Roczniki Administracji i Prawa" 2021, z. 3.

Kumar Gupta V., *The right to privacy in India: A comparative study with global implications*, „International Journal of Law, Justice and Jurisprudence" 2024, nr 4(1).

Kuźnicka D., *Organ nadzorczy w RODO : nowe wyzwanie w zakresie administracji publicznej?*, [w:] M. Pisz, M. Przychodzki, M. Radajewski (red.), *Zagadnienia współczesnego prawa publicznego*, Poznań 2018.

Kuźnicka-Błaszkowska D., *European Union: The Role of the GDPR in Preventing Sexual Abuse*, „European Data Protection Law Review" 2022, nr 8(4).

Kuźnicka-Błaszkowska D., *Informacje o tożsamości płciowej jako dane osobowe*, „ABI Expert" 2022, nr 2.

Kuźnicka-Błaszkowska D., *Practitioners' Corner Excessive Use of Data Access Rights in the Practice of Imposing Administrative Fines*, „European Data Protection Law Review" 2024, nr 1.

Kuźnicka-Błaszkowska D., Jabłoński M., *Information on Gender Identity as Personal Data under EU and US Data Protection Models*, „Białostockie Studia Prawnicze" 2024, nr (3)29.

Kuźnicka-Błaszkowska D., Joachimska J., *When Your Phone Knows You're Pregnant Even If You Don't: Period Tracking Applications and Threats to Privacy*, „Journal of International Women's Studies" 2025, vol. 27, iss. 1, Article 9.

Kwaśnik J., *Dane osobowe jako kluczowy obiekt zainteresowania cyberprzestępców*, „Annales Canonici" 2020, z. 1.

Lee T., *The global rise of „fake news" and the threat to democratic elections in the USA*, „Public Administration and Policy" 2019, t. 22, nr 1.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008.

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

Litwiński P., *Spełnienie obowiązku informacyjnego*, „ABI Expert" 2016, nr 1.

Łuczak J., *Komentarz do art. 12*, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2010.

Maciejewski M., *Prawo informacji – zagadnienia podstawowe*, [w:] W. Góralczyk (red.), *Prawo informacji. Prawo do informacji*, Warszawa 2006.

Marcon A., Rachul C., Caulfield T., *The consumer representation of DNA ancestry testing on YouTube*, „New Genetics and Society" 2021, nr 2.

Matthews T., *Deepfakes, Fake Barns, and Knowledge from Videos*, „Synthese" 2023, t. 201, nr 2.

Mednis A., *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych osobowych*, „Monitor Prawniczy" 2016, nr 20.

Nerka A., *Komentarz do art. 5*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Nowak M., *U.N. Covenant on Civil and Political Rights, CCPR Commentary*, Kehl–Strassburg–Arlington 2005.

Ochocki T., *Mechanizmy domyślnej ochrony danych w fazie projektowania*, „ABI Expert" 2020, nr 3.

Olejniczak K., *Ochrona danych genetycznych – od koncepcji indywidualnej do grupowej*, „Przegląd Prawa Medycznego" 2024, nr 3.

Panowicz-Lipska J., [w:] M. Gutowski (red.), *Kodeks cywilny*, t. I, *Komentarz. Art. 1–449[11]*, Warszawa 2016.

Pawłowski J., Zdrodowski B., Kuliczkowski M., *Słownik terminów z zakresu bezpieczeństwa*, Toruń 2020.

Prusiński P., *Informacje jako strategiczne aktywa przedsiębiorstw*, [w:] J.J. Brdulak, P. Sobczak (red.), *Wybrane problemy zarządzania bezpieczeństwem informacji*, Warszawa 2014.

Quinn P., Quinn L., *Big genetic data and its big data protection challenges*, „Computer Law & Security Review" 2018, vol. 34, nr 5.

Rojszczak M., *Reforma krajowych przepisów o ochronie danych a kwestia niezależności organów nadzorczych na tle rozporządzenia 2016/679 i dyrektywy 2002/58 – uwagi krytyczne*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, nr 4(7).

Rusinek M., *Tajemnica zawodowa i jej ochrona w polskim procesie karnym*, Warszawa 2007.

Rzucidło J., *Elektroniczny rząd. Aspekty konstytucyjnoprawne*, Warszawa 2015.

Rzymowski J., *Zasada rozliczalności w RODO*, „ABI Expert" 2018, nr 1.

Sakowska-Baryła M., *Komentarz do art. 26*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Sherwani M., *The Right to Privacy under International Law and Islamic Law: A Comparative Legal Analysis*, „Kardan Journal of Social Sciences and Humanities" 2018, vol. 1, iss. 1.

Sibiga G., *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003.

Siemieniak P., *Wymagania dokumentacyjne przetwarzania danych*, „ABI Expert" 2017, nr 2.

Skorupka J., *Komentarz do art. 225*, [w:] J. Skorupka (red.), *Kodeks postępowania karnego. Komentarz*, Warszawa 2023.

Sobczak J., *Prawo do prywatności, wolność słowa i druku*, [w:] L. Wiśniewski (red.), *Wolności i prawa jednostki oraz ich gwarancje w praktyce*, Warszawa 2006.

Sobczak J., [w:] A. Wróbel (red.), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz*, t. 1, Warszawa 2012.

Sobczak J., [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2013.

Sokołowicz W., Srzednicki A., *ISO. System zarządzania jakością oraz inne systemy oparte na* normach, Warszawa 2006.

Stańczak U., *Prawo do poinformowania w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą*, [w:] B. Fisher, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą na podstawie rodo*, Wrocław 2017.

Stefaniak S., Suszek-Borowska H., *Rozliczalność przetwarzania danych a systemy informatyczne*, „ABI Expert" 2018, nr 2.

Sukhorolsky P., Hutsaliuk V., *Processing od genetic data under GDPR: unresolved conflict of interests*, „Masaryk University Journalof Law and Technology" 2020, t. 14.

Suploveda M. *et al.*, *Human rights reference handbook*, Ciudad Colón 2004.

Szpor G., [w:] I. Lipowicz, Z. Niewiadomski, K. Strzyczkowski, G. Szpor, *Prawo administracyjne. Część materialna*, Warszawa 2004.

Szyszkowski W., *Rozważania o prywatności*, [w:] L. Antonowicz, W. Skrzydło, W. Śladkowski, J. Ziembiński, M. Granat (red.), *Wybrane problemy prawa konstytucyjnego*, Lublin 1985.

Verdoliva L., *Media Forensics and DeepFakes: An Overview*, „IEEE Journal of Selected Topics in Signal Processing" 2020, t. 14, nr 5.

Westin A.F., *Privacy & Freedom*, London–Sydney–Toronto 1967.

Westin A.F., *Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part I, The Current Impact of Surveillance on Privacy, Disclosure, and Surveillance*, „Columbia Law Review" 1966, vol. 66.

Westin A.F., *Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part II, Balancing the Conflicting demands of Privacy, Disclosure, and Surveillance*, „Columbia Law Review" 1966, vol. 66.

Węgrzyn J., *Prawo konsumenta do informacji w Konstytucji RP i w prawie unijnym*, Wrocław 2013.

Wiewiórski W., *Privacy by design jako paradygmat ochrony prywatności*, [w:] G. Szpor, W. Wiewiórski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, Warszawa 2012.

Więckowska M., *Analiza ryzyka prywatności*, „ABI Expert" 2017, nr 2.

Więckowska M., *Obowiązek informacyjny*, „ABI Expert" 2018, nr 2.

Więckowska M., *Przewodnik po ocenie skutków dla ochrony danych*, „ABI Expert" 2017, nr 1.

Więckowska M., *RODOwskaz prowadzenia rejestru czynności przetwarzania*, „ABI Expert" 2017, nr 3.

Wygoda K., *Komentarz do art. 12*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Wygoda K., *Modyfikacja przesłanek dopuszczalności przetwarzania danych zwykłych w oparciu o art. 6 RODO a działania podmiotów sektora publicznego*, [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017.

Wygoda K., *Przejrzyste informowanie, przejrzysta komunikacja i tryb wykonywania praw – obowiązki administratora danych*, [w:] B. Fischer, M. Sakowska-Baryła (red.), *Realizacja praw osób, których dane dotyczą, na podstawie rodo*, Wrocław 2017.

Zięba R., *O tożsamości nauk o bezpieczeństwie*, „Zeszyty Naukowe AON" 2012, nr 1(86).

Żywucka-Kozłowska E., Dziembowski R., *Dane osobowe zmarłego. Uwagi na gruncie prawa i tradycji społecznej*, „Kortowski Przegląd Prawniczy" 2022, nr 4.

Orzecznictwo

Europejski Trybunał Praw Człowieka

Wyrok ETPCz z dnia 24 kwietnia 1990 r. w sprawie *Kruslin p. Francji*, skarga nr 11801/85.

Wyrok ETPCz z dnia 25 marca 1993 r. w sprawie *Costello-Roberts p. Wielkiej Brytanii*, skarga nr 13134/87.

Wyrok ETPCz z dnia 27 sierpnia 1997 r. w sprawie *M.S. p. Szwecji*, skarga nr 20837/92.

Wyrok ETPCz z dnia 24 lutego 1998 r. w sprawie *Botta p. Włochom*, skarga nr 32647/96.

Wyrok ETPCz z dnia 25 marca 1998 r. w sprawie *Kopp p. Szwajcarii*, skarga nr 23224/94.

Wyrok ETPCz z dnia 16 lutego 2000 r. w sprawie *Amann p. Szwajcarii*, skarga nr 27798/95.

Wyrok ETPCz z dnia 6 lutego 2001 r. w sprawie *Bensaid p. Wielkiej Brytanii*, skarga nr 44599/98.

Wyrok ETPCz z dnia 25 września 2001 r. w sprawie *P.G. i J.H. p. Wielkiej Brytanii*, skarga nr 44787/98.

Wyrok ETPCz z dnia 22 października 2002 r. w sprawie *Taylor-Sabori p. Wielkiej Brytanii*, skarga nr 47114/99.

Wyrok ETPCz z dnia 28 stycznia 2003 r. w sprawie *Peck p. Wielkiej Brytanii*, skarga nr 44647/98.

Wyrok ETPCz z dnia 12 czerwca 2003 r. w sprawie *Van Kuck przeciwko Niemcom*, skarga nr 35968/04.

Wyrok ETPCz z dnia 24 czerwca 2004 r. w sprawie *Caroline von Hannover p. Niemcom*, skarga nr 59320/00.

Wyrok ETPCz z dnia 31 maja 2005 r. w sprawie *Vetter p. Francji*, skarga nr 59842/00.

Wyrok ETPCz z dnia 4 grudnia 2005 r. w sprawie *Roman Zakharov p. Rosji*, skarga nr 47143/06.

Wyrok ETPCz z dnia 22 grudnia 2005 r. w sprawie *Wisse p. Francji*, skarga nr 71611/01.

Wyrok ETPCz z dnia 4 grudnia 2008 r. w sprawie *s. i Marper przeciwko Wielkiej Brytanii*, skarga nr 30562/04 i 30566/04.

Wyrok ETPCz z dnia 17 grudnia 2009 r. w sprawie *B.B. p. Francji*, skarga nr 5335/06.

Wyrok ETPCz z dnia 17 grudnia 2009 r. w sprawie *Gardel p. Francji i M.B. p. Francji*, skarga nr 22115/06.

Wyrok ETPCz z dnia 12 stycznia 2010 w sprawie *Gillan i Quinton p. Wielkiej Brytanii*, skarga nr 4158/05 i in.

Wyrok ETPCz z dnia 18 października 2011 r. w sprawie *Khelili p. Szwajcarii*, skarga nr 16188/07.

Wyrok ETPCz z dnia z 13 listopada 2012 r. w sprawie *M.M. p. Wielkiej Brytanii*, skarga nr 24029/07.

Wyrok ETPCz z dnia 18 kwietnia 2013 r. w sprawie *M.K. p. Francji*, skarga nr 19522/09.

Wyrok ETPCz z dnia 29 kwietnia 2014 w sprawie *L.H. p. Łotwie*, skarga nr 52019/07.

Wyrok ETPCz z dnia 18 września 2014 r. w sprawie *Brunet p. Francji*, skarga nr 21010/10.

Wyrok ETPCz z dnia 7 czerwca 2016 w sprawie *Karabeyoğlu p. Turcji*, skarga nr 26012/11.

Wyrok ETPCz z dnia 22 czerwca 2017 r. w sprawie *Aycaguer p. Francji*, skarga nr 8806/12.

Wyrok ETPCz z dnia z 28 listopada 2017 r. w sprawie *Antović i Mirković p. Czarnogórze*, skarga nr 70838/13.

Wyrok ETPCz z dnia 8 lutego 2018 w sprawie *Ben Faiza p. Francji*, skarga nr 31446/12.

Wyrok ETPCz z dnia 24 kwietnia 2018 r. w sprawie *Benedik p. Słowenii*, skarga nr 62357/14.

Wyrok ETPCz z dnia 24 stycznia 2019 w sprawie *Catt p. Wielkiej Brytanii*, skarga nr 43514/15.

Wyrok ETPCz z dnia 13 lutego 2020 r. w sprawie *Gaughran p. Wielkiej Brytanii*, skarga nr 45245/15.

Wyrok ETPCz z dnia 14 kwietnia 2020 r. w sprawie *Dragan Petrović p. Serbii*, skarga nr 75229/10.

Trybunał Sprawiedliwości Unii Europejskiej

Wyrok TSUE z dnia 20 maja 2005 r., w sprawach połączonych *Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kalten-*

leutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische LuftverkehrsAG, oraz między Christą Neukomm, Josephem Lauermannem, C-465/00, C-138/01 i C-139/01.

Wyrok TSUE z dnia 9 listopada 2010 r. w sprawach połączonych *Volker und Marcus Schecke GbR i Hartman Eifert*, C-92/09 i C-93/09.

Wyrok TSUE z dnia 6 października 2015 r. *Maximillian Schrems przeciwko Data Protection Commissioner*, C-362/14.

Wyrok TSUE z dnia 7 marca 2024 r. *w sprawie IAB Europe przeciwko Gegevensbeschermingsautoriteit*, C-604/22.

Wyrok TSUE z dnia 4 października 2024 r. *Agentsia po vpisvaniyata przeciwko OL*, C-200/23.

Sąd Najwyższy

Postanowienie SN – Izba Karna z dnia 30 października 2014 r., I KZP 19/14.

Uchwała SN z dnia 22 stycznia 2003 r., I KZP 43/02.

Wyrok SN – Izba Karna z dnia 8 lutego 2018 r., V KK 224/17.

Sądy administracyjne

Postanowienie WSA w Łodzi z dnia 8 lutego 2019 r., II SAB/Łd 176/18.

Wyrok NSA z dnia 7 sierpnia 2008 r., I OSK 1218/07.

Wyrok NSA z dnia 18 września 2008 r., I OSK 315/08.

Wyrok NSA z dnia 28 sierpnia 2009 r., I OSK 1472/08.

Wyrok NSA z dnia 26 marca 2013 r., I OSK 2863/12.

Wyrok NSA z dnia 3 grudnia 2015 r., I OSK 1166/14.

Wyrok NSA z dnia 29 kwietnia 2016 r., I OSK 252/15.

Wyrok NSA z dnia 18 sierpnia 2016 r., I OSK 864/16.

Wyrok NSA z dnia 6 lipca 2017 r., I OSK 932/16.

Wyrok NSA z dnia 24 kwietnia 2018 r., I OSK 1422/16.

Wyrok NSA z dnia 27 września 2019 r., I OSK 2687/17.

Wyrok NSA z dnia 11 stycznia 2023 r., III OSK 6317/21.

Wyrok NSA z dnia 7 lutego 2023 r., II OSK 2780/21.

Wyrok NSA z dnia 10 października 2024 r., III OSK 4804/21.
Wyrok WSA w Warszawie z dnia 3 stycznia 2011 r., II SAB/Wa 264/10.
Wyrok WSA w Warszawie z dnia 8 grudnia 2011 r., II SA/Wa 1844/11.
Wyrok WSA w Warszawie z dnia 18 marca 2015 r., II SA/Wa 2243/14.
Wyrok WSA w Warszawie z dnia 6 października 2016 r., II SA/Wa 885/16.
Wyrok WSA w Krakowie z dnia 15 września 2017 r., II SA/Kr 1043/17.
Wyrok WSA w Warszawie z dni 10 października 2017 r., II SA/Wa 203/17.
Wyrok WSA w Warszawie z dnia 11 października 2017 r., II SA/Wa 2218/16.
Wyrok WSA w Warszawie z dnia 3 grudnia 2018 r., II SA/Wa 772/18.
Wyrok WSA w Warszawie z dnia 4 marca 2019 r., II SA/Wa 1722/18.
Wyrok WSA w Warszawie z dnia 27 kwietnia 2020 r., II SA/Wa 2543/19.
Wyrok WSA w Warszawie z dnia 7 sierpnia 2020 r., II SA/Wa 809/20.
Wyrok WSA w Warszawie z dnia 26 sierpnia 2020 r., II SA/Wa 2826/19.
Wyrok WSA w Warszawie z dnia 3 września 2020 r., II SA/Wa 2559/19.
Wyrok WSA w Warszawie z dnia 10 lutego 2021 r., II SA/Wa 2378/20.
Wyrok WSA w Warszawie z dnia 13 kwietnia 2021 r., II SA/Wa 1898/20.
Wyrok WSA w Warszawie z dnia 13 maja 2021 r., II SA/Wa 2129/20.
Wyrok WSA w Warszawie z dnia 16 listopada 2021 r., II SA/Wa 1489/21.
Wyrok WSA w Warszawie z dnia 19 kwietnia 2022 r., II SA/Wa 2259/21.
Wyrok WSA w Warszawie z dnia 2 sierpnia 2022 r., II SA/Wa 3687/21.

Decyzje PUODO i innych organów nadzorczych

Decyzja brytyjskiego organu nadzorczego z dnia 5 lipca 2021 r., Mermaids.
Decyzja francuskiego organu nadzorczego z dnia 18 listopada 2020 r., SAN-2020-008.
Decyzja hiszpańskiego organu nadzorczego z dnia 13 lutego 2020 r., PS/00187/2019.
Decyzja hiszpańskiego organu nadzorczego z dnia 7 lipca 2020 r., PS/00134/2020.
Decyzja PUODO z dnia 20 listopada 2018 r., ZWAD.405.10.2018.
Decyzja PUODO z dnia 10 grudnia 2018 r., ZSPR.440.783.2018.

Decyzja PUODO z dnia 20 grudnia 2018 r., ZSPU.440.99.2018.

Decyzja PUODO z dnia 15 marca 2019 r., ZSPR.421.3.2018.

Decyzja PUODO z dnia 18 października 2019 r., ZSPU.421.3.2019.

Decyzja PUODO z dnia 9 grudnia 2020 r., DKN.5131.5.2020.

Decyzja PUODO z dnia 23 czerwca 2022 r., DKN.5131.11.2022.

Decyzja włoskiego organu nadzorczego z dnia 12 listopada 2020 r., 9485681.

Strony internetowe

Biuletyn Informacji Publicznej Wrocławia, https://bip.uni.wroc.pl.

Encyklopedia PWN, hasło: *informacja*, https://encyklopedia.pwn.pl/haslo/informacja;3914686.html.

Klimowicz M., *Przekłuj swoją bańkę*, „Magazyn opinii Pismo", 3.09.2019, https://magazynpismo.pl/przekluj-swojabanke/?fbclid=IwAR0wwvqEveYnmZ99YSxOMVAHkQijaQcE0OE-QbheUjn8TMTAX_FALSfPOZU.

Stefanowicz B., *Informacja*, s. 7, https://depot.ceon.pl/handle/123456789/4341?show=full.

Żabnicka J., *Microsoft usuwa awarię chmury, która spowodowała, że niektóre amerykańskie linie lotnicze wstrzymały loty*, https://itreseller.pl/microsoft-usuwa-awarie-chmury-ktora-spowodowala-ze-niektore-amerykanskie-linie-lotnicze-wstrzymaly-loty/.

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1 z 19.07.2016 r.).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333/80 z 27.12.2022 r., s. 80-152).

Karta praw podstawowych Unii Europejskiej (wersja skonsolidowana Dz. Urz. UE C 202/389 z 7.06.2016 r.).

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.).

Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych podpisana w Strasburgu dnia 28 stycznia 1981 r. (Dz. U. z 2003 r. Nr 3, poz. 25 ze zm.).

Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284 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).

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., s. 1, ze sprost.).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. z 2007 r. Nr 10, poz. 68).

Rozporządzenie Ministra Środowiska z dnia 22 września 2010 r. w sprawie wzoru oraz zawartości i układu publicznie dostępnego wykazu danych o dokumentach informacje o środowisku i jego ochronie (Dz. U. z 2010 r. Nr 186, poz. 1249).

Rozporządzenie Prezesa Rady Ministrów z dnia 27 kwietnia 2011 r. w sprawie przygotowania i przeprowadzenia kontroli stanu zabezpieczenia informacji niejawnych (Dz. U. z 2011 r. Nr 93, poz. 541).

Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. Nr 271, poz. 1603).

Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczenia materiałów i umieszczenia na nich klauzuli tajności (Dz. U. z 2011 r. Nr 288, poz. 1692).

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 (Dz. U. z 2017 r. poz. 2247).

Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiadających za cyberbezpieczeństwo (Dz. U. z 2019 r. poz. 2379).

Rozporządzenie Rady Ministrów z dnia 21 listopada 2022 r. w sprawie portalu danych (Dz. U. z 2022 r. poz. 2415).

Traktat o funkcjonowaniu Unii Europejskiej, wersja skonsolidowana (Dz. Urz. UE C 202/47 z 7.06.2016 r.).

Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli dnia 6 marca 1997 r. (Dz. U. z 2000 r. Nr 64, poz. 740).

Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Albanii w sprawie wzajemnej ochrony informacji niejawnych, podpisana w Tiranie dnia 21 września 2004 r. (Dz. U. z 2005 r. Nr 247, poz. 2093).

Ustawa z dnia 26 maja 1982 r. – Prawo o adwokaturze (Dz. U. z 2022 r. poz. 1184 ze zm.).

Ustawa z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz. U. z 2022 r. poz. 1166).

Ustawa z dnia 26 stycznia 1984 r. – Prawo prasowe (t.j. Dz. U. z 2018 r. poz. 914).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. z 2025 r. poz. 383).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2023 r. poz. 57).

Ustawa z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (t.j. Dz. U. z 2023 r. poz. 1094).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2024 r. poz. 1222).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913).

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2023 r. poz. 1206).

Ustawa z dnia 16 października 2019 r. o ratyfikacji Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonego w Strasburgu dnia 10 października 2018 r. (Dz. U. z 2019 r. poz. 2284).

Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystaniu informacji sektora publicznego (t.j. Dz. U. z 2023 r. poz. 1524).

Zarządzenie Nr 79/2018 Rektora Uniwersytetu Wrocławskiego z dnia 13 czerwca 2018 r. w sprawie ochrony danych osobowych w Uniwersytecie Wrocławskim.

Zarządzenie Prezesa Urzędu Ochrony Konkurencji i Konsumentów z dnia 3 września 2021 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Ochrony Konkurencji i Konsumentów (Dz. Urz. UOKiK z 2021 r. poz. 2).

Zarządzenie Prezesa Urzędu Ochrony Konkurencji i Konsumentów z dnia 7 września 2021 r. w sprawie podstawowych zasad bezpieczeństwa informacji w Urzędzie Ochrony Konkurencji i Konsumentów (Polityka Bezpieczeństwa Informacji) (Dz. Urz. UOKiK z 2021 r. poz. 3).

Inne

CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation.

EDPB, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms.*

European Union Agency for Network and Information Security, *Privacy and Data Protection by Design – from policy to engineering*, Heraklion 2014.

Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty Series - No. 223.

Grupa Robocza Art. 29, *Opinia 4/2007 w sprawie pojęcia danych osobowych*, przyjęta 20 czerwca 2007, 01248/07/PL WP 136.

Grupa Robocza Art. 29, *Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"*, przyjęta 16.02.2010 r., WP 169.

Grupa Robocza Art. 29, *Working Document on Genetic Data*, przyjęty 17 marca 2004 r., 12178/03/EN WP 91.

Grupa Robocza Art. 29, *Wytyczne dotyczące inspektorów ochrony danych ('DPO')* przyjęte w dniu 13 grudnia 2016 r.

Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679*, przyjęte 4.04.2017 r., ostatnio zmienione i przyjęte 4.10.2017 r., WP 248.

Guidelines 07/2020 on the concepts of controller and processor in the GDPR, wersja 1.0, z 2.9.2020 r.

Raport Wysokiego Komisarza ONZ ds. Praw Człowieka z 3.08.2018 „Prawo do prywatności w świecie cyfrowym" A/HRC/39/29.

Rezolucja Parlamentu Europejskiego z 8.05.1979 r. w sprawie ochrony praw jednostek w odniesieniu do postępu technicznego w dziedzinie automatycznego przetwarzania danych PE z dnia 8 maja 1979 (Dz. U. WE C 140 z 8.05.1979 r.).

Uwagi końcowe do sprawozdania Danii z 2001 r., A/56/49 v. II.

Uwagi końcowe do sprawozdania Francji z 2008 r., CCPR/C/FRA/CO/4.

Uwagi końcowe do sprawozdania Kanady z 1999 r., A/54/50 v. I.

Uwagi końcowe do sprawozdania Szwecji z 2009 r., CCPR/C/SWE/CO/6.

Wyjaśnienia Dotyczące Karty Praw Podstawowych (2007/C 303/02).

[…] recenzowany podręcznik jest dziełem pionierskim, ciekawym i bez wątpienia potrzebnym. Autorki z podjętego zadania badawczego wywiązały się znakomicie, przygotowując przystępny, logiczny i dobrze usystematyzowany podręcznik, który nie tylko będzie stanowić nieocenioną pomoc dydaktyczną, ale może przyczynić się do dyskusji naukowych i stanowić podstawę do pogłębionych badań.

dr hab. Paweł Kuczma, prof. UZ

Recenzowany podręcznik dotyczący zarządzania bezpieczeństwem informacji i ochrony danych osobowych stanowi świetną odpowiedź na istotne zapotrzebowanie na tego typu opracowania. Treści w nim zawarte odpowiadają zagadnieniom, które zwykle objęte są zakresem wykładów poświęconych kwestiom zarządzania informacjami, tajemnicom prawnie chronionym, ochronie danych osobowych oraz bezpieczeństwu zasobów informacyjnych. Z tego względu wysoko należy ocenić zarówno ideę powstania recenzowanej pracy, jak i jej realizację.

dr hab. Marlena Sakowska-Baryła, prof. UŁ

ISBN 978-83-68169-09-6 (online)
ISBN 978-83-68169-10-2 (druk)