meritum

OCHRONA DANYCH OSOBOWYCH

redakcja naukowa Dominik Lubasz

Edyta Bielak-Jomaa, Iwona Bogucka, Jan Byrski, Witold Chomiczewski, Michał Czerniawski
Michał Ćwiakowski, Dominika Dörre-Kolasa, Karolina Gałęzowska, Maciej Gawroński
Urszula Góral, Agnieszka Grzelak, Mirosław Gumularz, Tomasz Izydorczyk
Mariusz Jagielski, Damian Karwala, Xawery Konarski, Patrycja Kozik, Dominik Lubasz
Joanna Łuczak-Tarka, Arwid Mednis, Monika Namysłowska, Zbigniew Okoń, Aneta Sieradzka
Monika Susałko, Adam Szkurłat, Dariusz Szostek, Agnieszka Świerczyńska
Marek Świerczyński, Katarzyna Witkowska-Nowakowska, Mirosław Wróblewski
Krzysztof Wygoda, Natalia Zawadzka

2. WYDANIE

Wolters Kluwer

meritum

OCHRONA DANYCH OSOBOWYCH

redakcja naukowa Dominik Lubasz

Edyta Bielak-Jomaa, Iwona Bogucka, Jan Byrski, Witold Chomiczewski, Michał Czerniawski
Michał Ćwiakowski, Dominika Dörre-Kolasa, Karolina Gałęzowska, Maciej Gawroński
Urszula Góral, Agnieszka Grzelak, Mirosław Gumularz, Tomasz Izydorczyk
Mariusz Jagielski, Damian Karwala, Xawery Konarski, Patrycja Kozik, Dominik Lubasz
Joanna Łuczak-Tarka, Arwid Mednis, Monika Namysłowska, Zbigniew Okoń, Aneta Sieradzka
Monika Susałko, Adam Szkurłat, Dariusz Szostek, Agnieszka Świerczyńska
Marek Świerczyński, Katarzyna Witkowska-Nowakowska, Mirosław Wróblewski
Krzysztof Wygoda, Natalia Zawadzka

2. WYDANIE

Wolters Kluwer

WARSZAWA 2022

Stan prawny na 31 października 2021 r.

Wydawca: *Monika Pawłowska*

Redaktor prowadzący: *Adam Choiński*

Opracowanie redakcyjne: *JustLuk*

Projekt okładki i stron tytułowych: *Wojtek Janikowski*

Autorzy:

dr Edyta Bielak-Jomaa – rozdział III.13;
sędzia NSA dr Iwona Bogucka – rozdział IV.4;
adw. dr hab. Jan Byrski, prof. UEK – rozdział XVII;
r.pr. Witold Chomiczewski – rozdziały: III.3.C–G, I–J, N, 5.C–H, 6.J; XVIII;
r.pr. dr Michał Czerniawski – rozdział I; II.1–4, 6;
adw. Michał Ćwiakowski – rozdział XI;
r.pr. dr Dominika Dörre-Kolasa – rozdział IX;
Karolina Gałęzowska – rozdział IV.5;
r.pr. Maciej Gawroński – rozdział XI;
Urszula Góral – rozdział III.14–15;
adw. dr hab. Agnieszka Grzelak, prof. ALK – rozdziały: IV.3; V.1–5, 10–15;
r.pr. dr Mirosław Gumularz – rozdziały: III.16.B; IV.9; V.6, 7.B, D–F, 8; XIV;
inż. Tomasz Izydorczyk – rozdział III.7.E;
dr hab. Mariusz Jagielski, prof. UŚ – rozdział VIII;
r.pr. dr Damian Karwala – rozdziały: III.12; XII;
adw. Xawery Konarski – rozdział VI;
r.pr. Patrycja Kozik – rozdziały: III.11; IV.7–8; V.6, 7.A, C, 9;
r.pr. dr Dominik Lubasz – rozdziały: III.1–2, 3.A–B, H, K–M, 4, 5.A–B, 6.A–B, 7.A–B, D, F–G, 10, 17; IV.1–2, 6, 12; XXI; XXIII;
dr Joanna Łuczak-Tarka – rozdziały: III.16.A, C; IV.10–11; XIII;
r.pr. dr Arwid Mednis – rozdział III.8;
dr hab. Monika Namysłowska, prof. UŁ – rozdział XXI;
r.pr. dr Zbigniew Okoń – rozdział XIX;
dr Aneta Sieradzka – rozdział X;
r.pr. Monika Susałko – rozdział III.6.C–I, 7.C;
adw. Adam Szkurłat – rozdział XV;
r.pr. dr hab. Dariusz Szostek, prof. UO – rozdział XX;
adw. Agnieszka Świerczyńska – rozdział XXIII;
adw. dr hab. Marek Świerczyński, prof. UKSW – rozdział XXII;
Katarzyna Witkowska-Nowakowska – rozdział III.9;
r.pr. Mirosław Wróblewski – rozdziały: IV.3; V.1–5, 10–15;
dr Krzysztof Wygoda – rozdział II.5;
adw. Natalia Zawadzka – rozdziały: VII; XVI

© Copyright by Wolters Kluwer Polska Sp. z o.o., 2022

ISBN: 978-83-8246-501-3
2. wydanie

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

księgarnia internetowa www.profinfo.pl

ISBN PDF-a: 978-83-8286-262-1

SPIS TREŚCI

Strona		Numer
11	Słowo wstępne	
13	Wykaz skrótów	
	CZĘŚĆ I	
21	Rozdział I. Ochrona danych osobowych w prawie międzynarodowym	
22	1. Wprowadzenie	1
24	2. Rada Europy – Europejska Konwencja Praw Człowieka	6
27	3. Rada Europy – Konwencja 108 i rezolucje	11
35	4. Organizacja Współpracy Gospodarczej i Rozwoju – rekomendacja z 23.09.1980 r. w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami	23
36	5. Rezolucje ONZ	25
37	6. Podsumowanie	27
39	Rozdział II. Prawo do ochrony danych osobowych jako prawo podstawowe (Karta Praw Podstawowych Unii Europejskiej, europejskie prawo pierwotne i wtórne, Konstytucja RP)	
40	1. Wprowadzenie	28
42	2. Prawo do ochrony danych osobowych w pierwotnym prawie europejskim	31
43	3. Dyrektywa 95/46	33
45	4. Prawo do ochrony danych osobowych w Karcie Praw Podstawowych Unii Europejskiej	39
47	5. Prawo do ochrony danych osobowych w Konstytucji RP	43
59	6. Prawo do ochrony danych osobowych jako prawo podstawowe – podsumowanie	65

Strona		Numer
61	Rozdział III. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)	
68	1. Wprowadzenie	66
73	2. Zakres zastosowania ogólnego rozporządzenia o ochronie danych	85
78	3. Podstawowe pojęcia	100
111	4. Zasady dotyczące przetwarzania danych osobowych	183
119	5. Przesłanki legalizacyjne przetwarzania danych osobowych	222
142	6. Prawa osób, których dane dotyczą	281
215	7. Obowiązki administratora i podmiotu przetwarzającego	461
321	8. Współadministrowanie danymi osobowymi	674
335	9. Powierzenie przetwarzania	709
349	10. Inspektor ochrony danych	737
361	11. Kodeksy postępowania i certyfikacja	765
369	12. Przekazywanie danych osobowych do państw trzecich i organizacji międzynarodowych	777
394	13. Organ nadzorczy	815
406	14. Współpraca i spójność	856
412	15. Europejska Rada Ochrony Danych	869
416	16. Środki ochrony prawnej	883
426	17. Podsumowanie	906
435	Rozdział IV. Ustawa z 10.05.2018 r. o ochronie danych osobowych	
439	1. Wprowadzenie	910
442	2. Zakres zastosowania ustawy o ochronie danych osobowych	918
444	3. Prezes Urzędu Ochrony Danych Osobowych	927
471	4. Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych	990
492	5. Kontrola przestrzegania przepisów o ochronie danych osobowych	1036
500	6. Wyznaczanie inspektora ochrony danych	1069
505	7. Akredytacja i certyfikacja	1091
521	8. Kodeksy postępowania	1130
533	9. Odpowiedzialność cywilna	1156
551	10. Administracyjne kary pieniężne	1201
562	11. Odpowiedzialność karna	1215
569	12. Podsumowanie	1226

Strona			Numer
575		Rozdział V. Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości z uwzględnieniem dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680	
578	1.	Wprowadzenie	1229
587	2.	Zakres zastosowania ustawy o ochronie danych osobowych przetwarzanych w związku ze zwalczaniem i zapobieganiem przestępczości	1234
598	3.	Podstawowe pojęcia	1245
612	4.	Zasady dotyczące przetwarzania danych osobowych	1259
626	5.	Przesłanki legalizacyjne przetwarzania danych osobowych	1272
635	6.	Prawa osób, których dane dotyczą	1282
642	7.	Obowiązki administratora	1311
682	8.	Współadministrowanie danymi	1417
684	9.	Powierzenie przetwarzania danych osobowych	1424
694	10.	Inspektor ochrony danych	1440
707	11.	Przekazywanie danych osobowych do państw trzecich i organizacji międzynarodowych	1448
718	12.	Organ nadzorczy	1452
734	13.	Europejska Rada Ochrony Danych	1468
738	14.	Środki ochrony prawnej i odpowiedzialność karna	1471
749	15.	Podsumowanie	1476
		CZĘŚĆ II	
757		Rozdział VI. Ochrona danych osobowych w sektorze łączności elektronicznej	
758	1.	Wprowadzenie	1477
759	2.	Podstawy prawne	1479
762	3.	Szczegółowe problemy	1487
773	4.	Podsumowanie	1513
775		Rozdział VII. Ochrona danych osobowych w działalności prasowej	
776	1.	Wprowadzenie	1514
776	2.	Podstawy prawne	1517
777	3.	Szczegółowe problemy	1518
797	4.	Podsumowanie	1569
799		Rozdział VIII. Ochrona danych osobowych konsumentów	
800	1.	Wprowadzenie	1570
802	2.	Podstawy prawne	1577

Strona			Numer
805	3.	Szczegółowe problemy	1582
826	4.	Podsumowanie	1628
827		Rozdział IX. Ochrona danych osobowych pracowników	
828	1.	Wprowadzenie	1629
830	2.	Szczegółowe problemy	1630
856	3.	Podsumowanie	1660
859		Rozdział X. Ochrona danych osobowych pacjentów	
860	1.	Wprowadzenie	1661
861	2.	Podstawy prawne	1664
861	3.	Szczegółowe problemy	1665
872	4.	Podsumowanie	1682
875		Rozdział XI. Ochrona danych osobowych w sektorze finansowym i bankowym	
876	1.	Wprowadzenie	1683
876	2.	Podstawy prawne	1686
877	3.	Szczegółowe problemy	1687
903	4.	Podsumowanie	1739
905		Rozdział XII. Ochrona danych osobowych w sektorze ubezpieczeniowym	
906	1.	Wprowadzenie	1740
906	2.	Podstawy prawne	1741
907	3.	Szczegółowe problemy	1742
919	4.	Podsumowanie	1762
923		Rozdział XIII. Ochrona danych osobowych w oświacie	
924	1.	Wprowadzenie	1764
925	2.	Podstawy prawne	1767
926	3.	Szczegółowe problemy	1771
935	4.	Podsumowanie	1790
937		Rozdział XIV. Ochrona danych osobowych w samorządzie terytorialnym	
938	1.	Wprowadzenie	1791
939	2.	Podstawy prawne	1794
940	3.	Szczegółowe problemy	1797
948	4.	Podsumowanie	1826

Strona			Numer
951		Rozdział XV. Ochrona danych osobowych w wymiarze sprawiedliwości	
952	1.	Wprowadzenie	1827
952	2.	Podstawy prawne	1828
953	3.	Szczegółowe problemy	1830
970	4.	Podsumowanie	1879
973		Rozdział XVI. Ochrona danych osobowych w działalności literackiej, artystycznej i akademickiej	
974	1.	Wprowadzenie	1880
974	2.	Podstawy prawne	1882
974	3.	Szczegółowe problemy	1883
982	4.	Podsumowanie	1906
983		Rozdział XVII. Ochrona danych osobowych a tajemnice zawodowe	
984	1.	Wprowadzenie	1908
985	2.	Podstawy prawne	1914
986	3.	Szczegółowe problemy	1915
991	4.	Podsumowanie	1924
995		Rozdział XVIII. Ochrona danych osobowych a *compliance*	
996	1.	Wprowadzenie	1928
997	2.	Podstawy prawne	1930
997	3.	Szczegółowe problemy	1932
1004	4.	Podsumowanie	1945
1005		Rozdział XIX. Ochrona danych osobowych a prawa własności intelektualnej	
1006	1.	Wprowadzenie	1946
1007	2.	Podstawy prawne	1952
1008	3.	Szczegółowe problemy	1953
1030	4.	Podsumowanie	2032
1033		Rozdział XX. Ochrona danych osobowych a *blockchain*	
1034	1.	Wprowadzenie	2036
1034	2.	Podstawy prawne	2038
1035	3.	Szczegółowe problemy	2039
1041	4.	Podsumowanie	2054

Strona		Numer
1043	Rozdział XXI. Ochrona danych osobowych a sztuczna inteligencja	
1044	1. Wprowadzenie	2055
1045	2. Podstawy prawne	2058
1046	3. Szczegółowe problemy	2059
1064	4. Podsumowanie	2121
1069	Rozdział XXII. Ochrona danych osobowych – zagadnienia kolizyjnoprawne	
1070	1. Wprowadzenie	2122
1070	2. Podstawy prawne	2123
1070	3. Szczegółowe problemy	2124
1082	4. Podsumowanie	2155
1087	Rozdział XXIII. Ochrona danych osobowych a ochrona sygnalistów	
1088	1. Wprowadzenie	2157
1089	2. Podstawy prawne	2158
1089	3. Szczegółowe problemy	2159
1108	4. Podsumowanie	2196
1111	O Autorach	
1121	Indeks rzeczowy	

SŁOWO WSTĘPNE

Od 25.05.2018 r. jednolicie w całej Unii Europejskiej stosowane jest rozporządzenie Parlamentu Europejskiego i Rady 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), które zastąpiło dotychczas obowiązujące regulacje dotyczące ochrony danych osobowych we wszystkich państwach członkowskich UE.

Ogólne rozporządzenie o ochronie danych wraz z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 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 uchylające decyzję ramową Rady 2008/977/WSiSW (tzw. dyrektywa policyjna) weszło w skład europejskiego pakietu reform ochrony danych osobowych mających na celu w szczególności unowocześnienie regulacji, zniesienie zbędnych obciążeń administracyjnych oraz usunięcie różnic w ochronie w poszczególnych państwach członkowskich.

Europejska reforma przepisów kształtujących system ochrony danych osobowych stała się głównym przedmiotem badawczym w niniejszej publikacji. Omówienie regulacji unijnych, a także aktów prawa krajowego zapewniających skuteczność ogólnego rozporządzenia w Polsce, jak również implementujących przepisy dyrektywy policyjnej do krajowego porządku prawnego, osadzone jest jednak w szerszym kontekście, uwzględniającym rozwiązania przyjęte w prawie międzynarodowym, podstawy konstytucyjne ochrony danych osobowych, jak też regulacje sektorowe.

Meritum. Ochrona danych osobowych składa się z dwóch części. W pierwszej, ogólnej, opisane zostały podstawy międzynarodowe ochrony danych osobowych, regulacje unijne, tak w prawie pierwotnym, jak i wtórnym, a także regulacje krajowe, począwszy od podstaw konstytucyjnych, a skończywszy na przepisach szczegółowych ustawy o ochronie danych osobowych i ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. W części drugiej problematykę ochrony danych osobowych ujęto z perspektywy poszczególnych sektorów, m.in. łączności elektronicznej, medycyny, oświaty czy bankowości, a także poruszono wybrane problemy szczegółowe związane z ochroną danych osobowych i np. sztuczną inteligencją, *blockchain*, zagadnieniami kolizyjnoprawnymi czy własnością intelektualną.

Publikacja ma charakter kompleksowy. Łączy zagadnienia teoretyczne i konstrukcyjne z kwestiami praktycznymi, które są efektem przemyśleń wielu współautorów. Wkład w jej opracowanie wniosło bowiem 30 autorów o rozległych kompetencjach merytorycznych z zakresu ochrony

danych osobowych, będących praktykami orzekającymi, jak też doradzającymi w dziedzinie ochrony danych osobowych, przedstawicielami nauki i administracji.

Dziękuję Im za zaangażowanie i nieoceniony wkład!

Liczę, że *Meritum. Ochrona danych osobowych* będzie ciekawą propozycją wydawniczą, dostarczającą czytelnikom kompleksowej wiedzy z zakresu ochrony danych osobowych i ułatwiającą prawidłowe stosowanie przepisów.

Z uwagi na dynamikę prawną w obszarze ochrony danych osobowych, tak legislacyjną, jak i orzeczniczą, po roku od wydania pierwszego *Meritum* zdecydowaliśmy się na dokonanie aktualizacji o najnowsze trendy, wytyczne, orzecznictwo organów nadzorczych i sądów, poglądy wyrażone zarówno w piśmiennictwie krajowym, jak i zagranicznym, a także nowe regulacje prawne lub ich projekty, zwłaszcza w zakresie przepisów dotyczących ochrony sygnalistów, i oddanie w Państwa ręce wydania drugiego.

Łódź, październik 2021 r. *dr Dominik Lubasz*

WYKAZ SKRÓTÓW

1. Źródła prawa	
decyzja 2021/914	decyzja wykonawcza Komisji (UE) 2021/914 z 4.06.2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Dz.Urz. UE L 199, s. 31)
dyrektywa 95/46	dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. WE L 281, s. 31, ze zm.)
dyrektywa 96/9	dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z 11.03.1996 r. w sprawie ochrony prawnej baz danych (Dz.Urz. WE L 77, s. 20, ze zm.)
dyrektywa 2000/31	dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. WE L 178, s. 1)
dyrektywa 2002/58	dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. WE L 201, s. 37, ze zm.)
dyrektywa 2011/83	dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z 25.10.2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady (Dz.Urz. UE L 304, s. 64, ze zm.)
dyrektywa 2015/1535	dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z 9.09.2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (ujednolicenie) (Dz.Urz. UE L 241, s. 1)
dyrektywa 2016/680 (dyrektywa policyjna)	dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89)
dyrektywa 2019/770	dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z 20.05.2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.Urz. UE L 136, s. 1)

dyrektywa PSD 2	dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z 25.11.2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.Urz. UE L 337, s. 35)
EKPC	Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284)
k.c.	ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2020 r. poz. 1740 ze zm.)
k.k.	ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2020 r. poz. 1444 ze zm.)
k.k.w.	ustawa z 6.06.1997 r. – Kodeks karny wykonawczy (Dz.U. z 2021 r. poz. 53 ze zm.)
Konstytucja RP	Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)
Konwencja 108	Konwencja Nr 108 Rady Europy sporządzona w Strasburgu 28.01.1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2003 r. Nr 3, poz. 25)
k.p.	ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2020 r. poz. 1320 ze zm.)
k.p.a.	ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2021 r. poz. 735 ze zm.)
k.p.c.	ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2021 r. poz. 1805 ze zm.)
k.p.k.	ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2021 r. poz. 534 ze zm.)
KPP UE	Karta Praw Podstawowych Unii Europejskiej (wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 389)
k.w.	ustawa z 20.05.1971 r. – Kodeks wykroczeń (Dz.U. z 2021 r. poz. 281 ze zm.)
p.p.m.	ustawa z 4.02.2011 r. – Prawo prywatne międzynarodowe (Dz.U. z 2015 r. poz. 1792)
p.p.s.a.	ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2019 r. poz. 2325 ze zm.)
pr. adw.	ustawa z 26.05.1982 r. – Prawo o adwokaturze (Dz.U. z 2020 r. poz. 1651 ze zm.)
pr. aut.	ustawa z 4.02.1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2021 r. poz. 1062)
pr. bank.	ustawa z 29.08.1997 r. – Prawo bankowe (Dz.U. z 2020 r. poz. 1896 ze zm.)
pr. ośw.	ustawa z 14.12.2016 r. – Prawo oświatowe (Dz.U. z 2021 r. poz. 1082 ze zm.)
pr. pras.	ustawa z 26.01.1984 r. – Prawo prasowe (Dz.U. z 2018 r. poz. 1914)
pr. prok.	ustawa z 28.01.2016 r. – Prawo o prokuraturze (Dz.U. z 2021 r. poz. 66 ze zm.)
pr. tel.	ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2021 r. poz. 576)
p.u.s.a.	ustawa z 25.07.2002 r. – Prawo o ustroju sądów administracyjnych (Dz.U. z 2021 r. poz. 137)
p.u.s.p.	ustawa z 27.07.2001 r. – Prawo o ustroju sądów powszechnych (Dz.U. z 2020 r. poz. 2072 ze zm.)
rozporządzenie 864/2007 (Rzym II)	rozporządzenie (WE) nr 864/2007 Parlamentu Europejskiego i Rady z 11.07.2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych (Dz.Urz. UE L 199, s. 73)
rozporządzenie 593/2008 (Rzym I)	rozporządzenie Parlamentu Europejskiego i Rady nr 593/2008 z 17.06.2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Dz.Urz. UE L 177, s. 6)

rozporządzenie 765/2008	rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z 9.07.2008 r. ustanawiające wymagania w zakresie akredytacji i uchylające rozporządzenie (EWG) nr 339/93 (Dz.Urz. UE L 218, s. 30, ze zm.)
rozporządzenie 1215/2012 (Bruksela I bis)	rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z 12.12.2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz.Urz. UE L 351, s. 1, ze zm.)
rozporządzenie 2016/679 (RODO)	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1)
rozporządzenie 2018/1725	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z 23.10.2018 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 (Dz.Urz. UE L 295, s. 39)
TFUE	Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 47)
TUE	Traktat o Unii Europejskiej (wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 13)
TWE	Traktat ustanawiający Wspólnotę Europejską (wersja skonsolidowana 2006) (Dz.Urz. UE C 321E, s. 1)
u.d.i.p.	ustawa z 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 r. poz. 2176 ze zm.)
u.d.u.r.	ustawa z 11.09.2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2021 r. poz. 1130 ze zm.)
u.f.p.	ustawa z 27.08.2009 r. o finansach publicznych (Dz.U. z 2021 r. poz. 305 ze zm.)
u.o.b.d.	ustawa z 27.07.2001 r. o ochronie baz danych (Dz.U. z 2021 r. poz. 386)
u.o.d.o.	ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
u.o.d.o. z 1997 r.	ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.)
u.o.d.o.z.p.	ustawa z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125)
u.o.f.f.e.	ustawa z 28.08.1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych (Dz.U. z 2020 r. poz. 105 ze zm.)
u.o.i.n.	ustawa z 5.08.2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742)
u.o.k.k.	ustawa z 16.02.2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2021 r. poz. 275)
u.p.k.	ustawa z 30.05.2014 r. o prawach konsumenta (Dz.U. z 2020 r. poz. 287 ze zm.)
u.p.p.p.	ustawa z 1.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2021 r. poz. 1132 ze zm.)
u.r.p.	ustawa z 6.07.1982 r. o radcach prawnych (Dz.U. z 2020 r. poz. 75 ze zm.)
u.s.o.z.n.r.	ustawa z 13.04.2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U. z 2021 r. poz. 514 ze zm.)
ustawa o Policji	ustawa z 6.04.1990 r. o Policji (Dz.U. z 2021 r. poz. 1882 ze zm.)
ustawa o RPD	ustawa z 6.01.2000 r. o Rzeczniku Praw Dziecka (Dz.U. z 2020 r. poz. 141)
ustawa o RPO	ustawa z 15.07.1987 r. o Rzeczniku Praw Obywatelskich (Dz.U. z 2020 r. poz. 627 ze zm.)
ustawa o SG	ustawa z 12.10.1990 r. o Straży Granicznej (Dz.U. z 2021 r. poz. 1486 ze zm.)

ustawa o UFG	ustawa z 22.05.2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz.U. z 2021 r. poz. 854 ze zm.)
ustawa sektorowa	ustawa z 21.02.2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. poz. 730)
u.ś.o.z.	ustawa z 27.08.2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. z 2021 r. poz. 1285 ze zm.)
u.ś.u.d.e.	ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
u.u.p.	ustawa z 19.08.2011 r. o usługach płatniczych (Dz.U. z 2021 r. poz. 1907 ze zm.)
u.w.i.o.ś.	ustawa z 16.09.2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. z 2020 r. poz. 158)
u.z.p.t.	ustawa z 9.07.2003 r. o zatrudnianiu pracowników tymczasowych (Dz.U. z 2019 r. poz. 1563)
u.z.z.	ustawa z 23.05.1991 r. o związkach zawodowych (Dz.U. z 2019 r. poz. 263 ze zm.)
2. Organy orzekające	
ETPC	Europejski Trybunał Praw Człowieka
NSA	Naczelny Sąd Administracyjny
SN	Sąd Najwyższy
TK	Trybunał Konstytucyjny
TS/TSUE	Trybunał Sprawiedliwości/ Trybunał Sprawiedliwości Unii Europejskiej
WSA	Wojewódzki Sąd Administracyjny
3. Czasopisma i publikatory	
CBOSA	Centralna Baza Orzeczeń Sądów Administracyjnych
Dz.U.	Dziennik Ustaw
Dz.Urz. UE	Dziennik Urzędowy Unii Europejskiej
EPS	Europejski Przegląd Sądowy
HUDOC	internetowa Baza Orzecznictwa Europejskiego Trybunału Praw Człowieka
ICLQ	International & Comparative Law Quarterly
KPP	Kwartalnik Prawa Prywatnego
M.P.	Monitor Polski
M. Praw.	Monitor Prawniczy
ONSA	Orzecznictwo Naczelnego Sądu Administracyjnego
OSNC	Orzecznictwo Sądu Najwyższego. Izba Cywilna
OSNKW	Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa
OSNP	Orzecznictwo Sądu Najwyższego. Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych
OSP	Orzecznictwo Sądów Polskich

OTK	Orzecznictwo Trybunału Konstytucyjnego
OTK-A	Orzecznictwo Trybunału Konstytucyjnego. Seria A
PiP	Państwo i Prawo
PiZS	Praca i Zabezpieczenie Społeczne
PME	Prawo Mediów Elektronicznych
PPH	Przegląd Prawa Handlowego
PPP	Przegląd Prawa Publicznego
Prok. i Pr.	Prokuratura i Prawo
Prz. Sejm.	Przegląd Sejmowy
PS	Przegląd Sądowy
PSM	Przegląd Stosunków Międzynarodowych
RabelsZ	Rabels Zeitschrift für ausländisches und internationales Privatrecht
RPEiS	Ruch Prawniczy, Ekonomiczny i Socjologiczny
R. Pr.	Radca Prawny
SC	Studia Cywilistyczne
TPP	Transformacje Prawa Prywatnego
ZNUJ	Zeszyty Naukowe Uniwersytetu Jagiellońskiego
ZNUJ PPWI	Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej
ZNUJ PWiOWI	Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Wynalazczości i Ochrony Własności Intelektualnej
4. Inne	
ABI	administrator bezpieczeństwa informacji
ABW	Agencja Bezpieczeństwa Wewnętrznego
AIS	*Account Information Service*
AML	*anti-money laundering*
BCR	*binding corporate rules*
CBA	Centralne Biuro Antykorupcyjne
CNIL	Commission Nationale de l'Informatique et des Libertés
DLT	*distributed ledger technology*
DPIA	*data protection impact assessment*
EDPS	*European Data Protection Supervisor*
ENISA	Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji
EROD	Europejska Rada Ochrony Danych
GIODO	Generalny Inspektor Ochrony Danych Osobowych
ICO	*Information Commissioner's Office*
IOD	inspektor ochrony danych
KNF	Komisja Nadzoru Finansowego
KRI	Krajowe Ramy Interoperacyjności
KRRiT	Krajowa Rada Radiofonii i Telewizji

KSSiP	Krajowa Szkoła Sądownictwa i Prokuratury
OECD	Organizacja Współpracy Gospodarczej i Rozwoju
PBUK	Polskie Biuro Ubezpieczycieli Komunikacyjnych
PIH	Państwowa Inspekcja Handlowa
PIS	*Payment Initiation Service*
RPO	Rzecznik Praw Obywatelskich
RPP	Rzecznik Praw Pacjenta
SCC	*Standard Contractual Clauses*
SI	sztuczna inteligencja
TPPs	*Third Party Providers*
UFG	Ubezpieczeniowy Fundusz Gwarancyjny
UODO	Urząd Ochrony Danych Osobowych

CZĘŚĆ I

ROZDZIAŁ I

Ochrona danych osobowych w prawie międzynarodowym

Michał Czerniawski

SPIS TREŚCI

1. **Wprowadzenie** 1

2. **Rada Europy – Europejska Konwencja Praw Człowieka** 6

A. Wstęp do Europejskiej Konwencji Praw Człowieka 6
B. Orzecznictwo Europejskiego Trybunału Praw Człowieka 8

3. **Rada Europy – Konwencja 108 i rezolucje** 11

A. Konwencja 108 Rady Europy z 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu 28.01.1981 r. 11
B. Rezolucje Rady Europy 19
C. Modernizacja Konwencji 108 22

4. **Organizacja Współpracy Gospodarczej i Rozwoju – rekomendacja z 23.09.1980 r. w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami** 23

5. **Rezolucje ONZ** 25

A. Rezolucja 34/169 Zgromadzenia Ogólnego ONZ: Kodeks Postępowania Funkcjonariuszy Porządku Prawnego 25
B. Rezolucja 45 (95) Zgromadzenia Ogólnego ONZ: Wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych 26

6. **Podsumowanie** 27

1. Wprowadzenie

Podstawa prawna: Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych oraz Protokół dodatkowy do Konwencji dotyczący organów nadzoru i transgranicznych przepływów danych sporządzony w Strasburgu 8.11.2001 r. (Dz.U. z 2006 r. Nr 3, poz. 15); Protokół nr 223 modernizujący Konwencję 108, otwarty do podpisu 10.10.2018 r.; Oświadczenie rządowe z 27.08.2002 r. w sprawie mocy obowiązującej Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonej w Strasburgu dnia 28 stycznia 1981 r. (Dz.U. z 2003 r. Nr 3, poz. 26); ustawa z 16.10.2019 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. poz. 2284); Rezolucja 34/169 Zgromadzenia Ogólnego ONZ: Kodeks Postępowania Funkcjonariuszy Porządku Prawnego; Rezolucja 45 (95) Zgromadzenia Ogólnego ONZ: Wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych; Powszechna Deklaracja Praw Człowieka, Paryż, 10.12.1948 r.; Międzynarodowy Pakt Praw Obywatelskich i Politycznych, otwarty do podpisu w Nowym Jorku 19.12.1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167); Konwencja o Organizacji Współpracy Gospodarczej i Rozwoju, wraz z Protokołami dodatkowymi nr 1 i 2 do tej Konwencji, stanowiącymi jej integralną część sporządzone w Paryżu 14.12.1960 r. (Dz.U. z 1998 r. Nr 76, poz. 490); Rezolucja (73) 22 Rady Europy, Rezolucja (74) 29 Rady Europy, OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Konwencja o ochronie praw człowieka i podstawowych wolności.

1 Ochrona danych osobowych do dnia dzisiejszego nie doczekała się regulacji międzynarodowej, która standaryzowałaby zasady przetwarzania danych osobowych na świecie. Przyjęte przez unijnego prawodawcę rozwiązania, tj. dyrektywa 95/46 oraz RODO, stosunkowo restrykcyjne, mimo upływu ponad 20 lat od ich wypracowania, nie znalazły także na świecie zbyt wielu naśladowców. Nieco inaczej sytuacja ma się w odniesieniu do prawa do prywatności. W tym zakresie bowiem istnieją standardy globalne, a powstałe kilkadziesiąt lat temu przepisy wciąż można efektywnie stosować w społeczeństwie informacyjnym. Na poziomie międzynarodowym prawo do prywatności proklamowano po raz pierwszy w Powszechnej Deklaracji Praw Człowieka (1948), a następnie w Międzynarodowym Pakcie Praw Obywatelskich i Politycznych (1966).

> ***WAŻNE!*** Zgodnie z art. 12 Powszechnej Deklaracji Praw Człowieka:
> „nikt nie może być poddany arbitralnemu ingerowaniu w jego życie prywatne, rodzinne, domowe lub korespondencję. (…) Każdy człowiek ma prawo obrony przeciwko takim ingerencjom i atakom".

Z kolei zgodnie z art. 29 ust. 2 tejże Deklaracji:
„w korzystaniu ze swych praw i wolności człowiek podlega jedynie takim ograniczeniom, które są ustalone przez prawo wyłącznie w celu zapewnienia odpowiedniego uznania i poszanowania prawom i wolnościom innych oraz uczynienia zadość wymogom moralności, porządku publicznego i powszechnego dobrobytu".

2 Deklaracja, uchwalona niedługo po II wojnie światowej, nad którą prace rozpoczęły się już w roku 1945, była odpowiedzią na działalność reżimów totalitarnych, przede wszystkim nazistowskich Niemiec. Był to istotny punkt zwrotny i pierwsze tak znaczące dokonanie Organizacji Narodów Zjednoczonych w obszarze ochrony praw człowieka i w tym też kontekście należy umiejscawiać prawo do prywatności. Choć w momencie powstania deklaracja była

jedynie rezolucją Zgromadzenia Ogólnego ONZ i nie tworzyła prawa międzynarodowego ani nie miała wiążącego charakteru, obecnie uznaje się ją za powszechnie obowiązujące prawo zwyczajowe.

3 **Koncepcja „prywatności" jest znacznie starsza od prawa ochrony danych osobowych.** Pierwszą próbę zdefiniowania tego pojęcia podjęto pod koniec XIX w. W owym czasie utożsamiano „prywatność" z „prawem do bycia pozostawionym w spokoju" (ang. *right to be let alone*), a pierwsi definicję prywatności, rozumianej właśnie w ten sposób, sformułowali dwaj amerykańscy prawnicy S.D. Warren i L.D. Brandeis. Z kolei jeśli chodzi o sądy czy też wymiar sprawiedliwości w ogólności, to pojęciem prawa do prywatności jako pierwszy posłużył się Sąd Najwyższy Michigan w 1881 r. w sprawie DeMay v. Roberts. Z. Mielnik wskazuje, iż „prywatność" – szeroko rozumiana – jest to stan, w którym jednostka podejmuje decyzje bez ingerencji ze strony osób trzecich [Z. Mielnik, *Prawo do prywatności (zagadnienia wybrane)*, RPEiS 1996/2, s. 29]. **Prywatność można w pewnym uproszczeniu definiować jako sprawowanie kontroli nad dotyczącymi danej osoby informacjami.** W szczególności prawo do prywatności pozwala na wyodrębnienie tzw. prywatności informacyjnej – prawa jednostki umożliwiającego kontrolowanie treści i obiegu dotyczących jej informacji [A. Mednis, *Ochrona prawna danych osobowych a zagrożenia prywatności – rozwiązania polskie* [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 167; G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003, s. 13]. Rola tego uprawnienia w społeczeństwie informacyjnym rośnie i wiązać z nim można choćby prawo do bycia zapomnianym. A. Kopff w pierwszej polskiej publikacji poświęconej zagadnieniu prywatności określa ją jako „prawo jednostki do życia własnym życiem układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej" [A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego (Zagadnienia konstrukcyjne)*, SC 1972/20, s. 6 i n.]. Według A. Kopffa życiem prywatnym jest to wszystko, co ze względu na uzasadnione odosobnienie się jednostki od ogółu społeczeństwa służy jej do fizycznego i psychicznego rozwoju oraz zachowania pozycji społecznej. M. Safjan wskazuje, iż **jest to zarówno obszar intymności i odosobnienia od innych, jak i sfera wolności i decydowania o samym sobie** [M. Safjan, *Czy prywatność jest wartością chronioną w społeczeństwie demokratycznym?*, „Rzeczpospolita" z 23.02.1998 r.]. W epoce społeczeństwa informacyjnego i Internetu na znaczeniu wydaje się zyskiwać, widoczny w części z powyższych definicji, aspekt „wolnościowy" kontrolowania dotyczących siebie informacji i rozporządzania dotyczącymi siebie informacjami, w tym własnymi danymi osobowymi. Nie powinno budzić wątpliwości, że istotnym uzupełnieniem prywatności w Internecie staje się prawo do ochrony danych osobowych. Prawo do ochrony danych osobowych jest koncepcją, która w polskim porządku prawnym pojawiła się dzięki aktom prawa międzynarodowego i unijnego. Jest to stosunkowo nowy obszar prawa, wyrosły właśnie na gruncie prawa do prywatności i choć obecnie jest to samodzielna dziedzina prawa, to wciąż łączy ją z prawem do prywatności szereg kwestii.

> **WAŻNE!** Prawa do ochrony danych osobowych nie można utożsamiać z prawem do prywatności. Są to odrębne koncepcje i tak np. naruszenie prawa do ochrony danych osobowych nie w każdym przypadku będzie stanowić naruszenie prawa do prywatności i *vice versa*.

4 Prawo do prywatności i jego ewolucja pozostaje pod silnym wpływem postępu technicznego. Dzieje się tak choćby dlatego, iż korzystanie z otwartej sieci komputerowej, jaką jest Internet, wiąże się z pozostawianiem po sobie dużych ilości cyfrowych śladów, np. adresów IP urządzeń wykorzystywanych do łączenia się z siecią czy też logów. Coraz częściej użytkownicy cyberprzestrzeni są przedmiotem inwigilacji i monitorowania ich aktywności. Tego typu działania

podejmują tak podmioty prywatne (np. w celu profilowania), jak i organy państwa. A. Mednis już w 1995 r. wskazywał, iż:

> „[j]ednym z czynników wpływających na ewolucję poglądów jest niewątpliwie rozwój techniki, w tym środków umożliwiających ingerencję w życie prywatne jednostek wbrew ich woli i bez ich wiedzy" [A. Mednis, *Prawna ochrona danych osobowych*, Warszawa 1995, s. 5].

W 2006 r. ten sam autor wskazywał, iż:

> „współczesne technologie (stale zresztą rozwijane) doprowadziły do sytuacji, w której prawie każdy może zgromadzić o nas takie informacje, jakich jeszcze 40 lat temu nie byłyby w stanie zebrać tajne służby nawet najbardziej totalitarnych reżimów" [A. Mednis, *Prawo do prywatności a interes publiczny*, Kraków 2006, s. 7].

Zmienia się także socjologiczne postrzeganie prywatności – zwłaszcza w pokoleniu, które dorastało już w czasach, w których Internet był powszechnie dostępny. W nim następuje bowiem wręcz rutynowe upublicznianie informacji o sobie w Internecie, w szczególności za pośrednictwem portali społecznościowych. Percepcja „prywatności" jako wartości zmienia się powoli. Jej ochronie nie sprzyja rozwój takich zjawisk jak choćby Web 2.0, u którego podstaw leży dzielenie się informacjami w Internecie.

5 Jak już wspomniano, pierwszy akt prawa międzynarodowego, który wprost wskazuje na konieczność ochrony prywatności, stanowi Deklaracja Praw Człowieka Organizacji Narodów Zjednoczonych z 1948 r. Oczywiste jest, że ze względu na czas jej przyjęcia nie mogła ona odpowiadać na zagrożenia dla prywatności, które niesie ze sobą postęp technologiczny, ustanowiła natomiast podstawy, na których do dnia dzisiejszego opierają się wszelkie rozwiązania dotyczące ochrony prywatności. To właśnie ochrona praw człowieka była punktem wyjścia dla unijnego ustawodawcy przy wprowadzaniu przepisów o ochronie danych osobowych. K. Kowalik-Bańczyk wskazuje, iż:

> „[w] obrębie Unii Europejskiej dane osobowe są tradycyjnie traktowane jako wartość związana z prawem do prywatności, stąd ich rozbudowany system ochrony" [K. Kowalik-Bańczyk, *Sposoby regulacji handlu elektronicznego w prawie wspólnotowym i międzynarodowym*, LEX 2006].

Takie podejście wyróżnia europejskie regulacje np. na tle przepisów amerykańskich, które wywodzą się z przepisów konsumenckich i w których to konsument jest przedmiotem ochrony, a uprawnienia regulacyjne wykonuje Federalna Komisja Handlu (ang. Federal Trade Commission). Rola ochrony danych osobowych w Unii Europejskiej uległa w ostatnich latach dużemu wzmocnieniu. Prócz coraz większej liczby spraw przed Trybunałem Sprawiedliwości Unii Europejskiej odniesienia do niej znajdują się w Karcie Praw Podstawowych, która wraz z wejściem w życie traktatu lizbońskiego stała się aktem prawa wiążącym wszystkie państwa członkowskie Unii Europejskiej. Z kolei z punktu widzenia prowadzenia biznesu i gospodarki harmonizacja przepisów o ochronie danych osobowych jest ważnym aspektem budowy Jednolitego Rynku Cyfrowego, mającego za zadanie stymulować rozwój i wzmocnić konkurencyjność gospodarek Unii Europejskiej w społeczeństwie informacyjnym.

2. Rada Europy – Europejska Konwencja Praw Człowieka

A. Wstęp do Europejskiej Konwencji Praw Człowieka

6 Z perspektywy europejskiej w prawie międzynarodowym **szczególną rolę odgrywa Konwencja o ochronie praw człowieka i podstawowych wolności** – umowa międzynarodowa zawarta

przez państwa członkowskie Rady Europy. Artykuł 8 EKPC był pierwszym przepisem dotyczącym ochrony danych osobowych w Europie, znajduje zastosowanie do ochrony danych osobowych jedynie w ograniczonym zakresie [J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015, s. 36]. Konwencja została sporządzona w Rzymie 4.11.1950 r., weszła w życie w 1953 r. Na przestrzeni lat została zmieniona szeregiem protokołów (w sumie dotychczas przyjęto 17 protokołów, w tym protokół 14bis, który wygasł 1.06.2010 r.). Ustęp 1 art. 8 EKPC stanowi, iż każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Z kolei ust. 2 tego artykułu podkreśla, iż:

> „[n]iedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa 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".

Artykuł 14 EKPC zaznacza, iż:

> „[k]orzystanie z praw i wolności wymienionych w niniejszej Konwencji powinno być zapewnione bez dyskryminacji wynikającej z takich powodów jak płeć, rasa, kolor skóry, język, religia, przekonania polityczne i inne, pochodzenie narodowe lub społeczne, przynależność do mniejszości narodowej, majątek, urodzenie bądź z jakichkolwiek innych przyczyn".

WAŻNE! Nad przestrzeganiem postanowień Europejskiej Konwencji Praw Człowieka czuwa Europejski Trybunał Praw Człowieka z siedzibą w Strasburgu. Rozpatruje on skargi dotyczące przestrzegania przez strony postanowień tego aktu prawnego.

W zakresie art. 8 EKPC i ochrony prywatności orzecznictwo doczekało się bogatego dorobku. 7
Na podstawie tego przepisu Komitet Ministrów, o czym szerzej poniżej, wydał także dwie rezolucje:

- Resolution (73) 22 on the protection of the privacy of individuals vis-à – vis electronic data banks in the private sector [Rezolucja (73) 22 o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze prywatnym], 26.09.1973 r.;
- Resolution (74) 29 on the protection of the privacy of individuals vis – à-vis electronic data banks in the public sector [Rezolucja (74) 29 o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze publicznym], 20.09.1974 r.

Komitet Ministrów wydał także kilka niewiążących zaleceń. Europejska Konwencja Praw Człowieka nie gwarantuje prawa do prywatności w sposób bezwzględny. Dopuszcza możliwość ograniczenia wymienionych w niej praw z takich powodów jak bezpieczeństwo państwowe, integralność terytorialna, bezpieczeństwo publiczne, zapobieganie zakłóceniom porządku lub przestępstw, ochrona zdrowia i moralności, ochrona dobrego imienia i praw innych osób, zapobieganie ujawnieniu informacji poufnych czy też zagwarantowanie powagi i bezstronności władzy sądowej.

WAŻNE! **Artykuł 8 EKPC**

Prawo do poszanowania życia prywatnego i rodzinnego

1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.
2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, 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 innych osób.

B. Orzecznictwo Europejskiego Trybunału Praw Człowieka

8 W celu zapewnienia przestrzegania praw zagwarantowanych w Europejskiej Konwencji Praw Człowieka (w tym prawa do prywatności) ustanowiony został Europejski Trybunał Praw Człowieka (art. 19 EKPC). Samo prawo do prywatności było przedmiotem szeregu skarg do Trybunału. Sądy i trybunały państw uznających kompetencję Europejskiego Trybunału Praw Człowieka odwołują się do tych orzeczeń.
Jedną z kluczowych różnic między orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej a Europejskiego Trybunału Praw Człowieka jest to, iż to drugie dotyczy w dużo większej mierze oceny ingerencji w prawo do prywatności przez organy państwa i tego, czy była ona uzasadniona. **Tak jak w przypadku ochrony danych osobowych, także w przypadku prawa do prywatności państwa dysponują pewną dyskrecjonalnością i mogą ograniczać jego zakres m.in. ze względów bezpieczeństwa narodowego czy walki z przestępczością. Natomiast ta uznaniowość nie jest swobodna, podlega ograniczeniom i państwa mogą ją stosować wyłącznie przy spełnieniu szeregu wymogów.** Wszelkie ograniczenia treści prawa do prywatności muszą także spełniać przesłankę bycia „koniecznym w demokratycznym społeczeństwie".

> ***WAŻNE!*** Orzecznictwo Europejskiego Trybunału Praw Człowieka koncentruje się na szeroko rozumianym poszanowaniu życia prywatnego, a nie na ochronie danych osobowych jako takiej.

Ważne jest, aby wszelkie działania organów państwa były podejmowane z poszanowaniem prawa do życia prywatnego. Stąd tak ważne, obecne także w orzecznictwie Europejskiego Trybunału Praw Człowieka, zasady proporcjonalności i legalności przetwarzania danych.

9 Szczególnie istotny dla wykładni art. 8 EKPC w kontekście prawa do prywatności i ochrony danych osobowych wydaje się wyrok w sprawie S. i Marper v. Zjednoczone Królestwo (wyrok z 4.12.2008 r., 30562/04 i 30566/04, S. i Marper v. Zjednoczone Królestwo, HUDOC). W sprawie tej Trybunał stwierdził m.in., że ingerencję uważa się za konieczną w społeczeństwie demokratycznym, jeśli odpowiada pilnej potrzebie społecznej, a w szczególności jeśli jest proporcjonalna do realizowanego uprawnionego celu, a racje przedstawione przez władze krajowe na jej uzasadnienie są odpowiednie i wystarczające. Pod uwagę należy brać naturę prawa, jego znaczenie dla jednostki, charakter ingerencji czy realizowanego celu. Europejski Trybunał Praw Człowieka potwierdził w niej także, że art. 8 EKPC może obejmować też zagadnienia z obszaru ochrony danych osobowych. Wskazał, że **ochrona danych osobowych może być elementem respektowania prawa do życia prywatnego** i ma fundamentalne znaczenie dla korzystania z prawa do poszanowania życia prywatnego i rodzinnego zagwarantowanego w art. 8 EKPC. Prawo krajowe musi zapewnić odpowiednie zabezpieczenia przed użyciem danych osobowych niezgodnym z gwarancjami tego artykułu. Potrzeba zabezpieczeń jest większa w przypadku ochrony danych osobowych poddawanych automatycznemu przetwarzaniu. Prawo krajowe musi w szczególności zapewnić, aby dane takie były istotne ze względu na cel ich gromadzenia oraz zachowane w formie umożliwiającej identyfikację osoby, której dotyczą, nie dłużej niż przez okres wymagany ze względu na wymieniony cel.

> ***WAŻNE!*** Prawo krajowe musi zapewnić odpowiednie gwarancje skutecznej ochrony przechowywanych danych osobowych przed niewłaściwym użyciem lub nadużyciem.

10 W swoim orzecznictwie Trybunał w Strasburgu zajmował się m.in. kwestiami: retencji i przechowywania danych medycznych (wyroki: 30562/04 i 30566/04, S. i Marper v. Zjednoczone Kró-

lestwo; z 18.04.2013 r., 19522/09, M.K. v. Francja; z 4.06.2013 r., 7841/08 i 57900/12, Peruzzo i Martens v. Republika Federalna Niemiec; z 6.06.2013 r., 1585/09, Avilkina i inni v. Federacja Rosyjska, czy z 15.04.2014 r., 50073/07, Radu v. Republika Mołdawii, HUDOC), ochrony grup szczególnie zagrożonych, w tym dzieci (wyrok z 7.07.1989 r., 10454/83, Gaskin v. Zjednoczone Królestwo, HUDOC) czy przetwarzania danych przez organy państwa (wyroki: z 26.03.1987 r., 9248/81, Leander v. Szwecja; z 16.02.2000 r., 27798/95, Amann v. Szwajcaria, HUDOC, § 69). Europejski Trybunał Praw Człowieka poświęcił sporo uwagi m.in. kwestii **legalności przetwarzania danych osobowych przez rządy i ich przedstawicieli**. Ryzykiem przy ocenie zgodności przetwarzania danych z prawem jest zwłaszcza brak obiektywności organów państwa przy jej dokonywaniu. Ważne jest, jakie zabezpieczenia praw przewidują krajowe systemy prawne. W szczególności przetwarzane dane nie mogą być nadmierne w stosunku do celów, dla których są przetwarzane, oraz pozwalać na identyfikację podmiotu danych dłużej, niż jest to niezbędne (wyroki: 30562/04 i 30566/04, S. i Marper v. Zjednoczone Królestwo; z 4.05.2000 r., 28341/95, Rotaru v. Rumunia; z 27.08.1997 r., 20837/92, M.S. v. Szwecja, HUDOC). Osoby fizyczne muszą dysponować efektywnymi środkami dochodzenia swoich praw. Tytułem przykładu w sprawie Khelili v. Szwajcaria (orzeczenie z 18.10.2011 r., 16188/07, Khelili v. Szwajcaria, HUDOC) Trybunał wskazał, że samo zarejestrowanie przez władze publiczne danych dotyczących życia prywatnego jednostki może stanowić ingerencję w rozumieniu art. 8 EKPC. Sporo uwagi poświęcił też kwestii wyważania praw; w orzeczeniach z 7.02.2012 r., 39954/08, Axel Springer AG v. Niemcy czy z 10.05.2011 r., 48009/08, Mosley v. Zjednoczone Królestwo, HUDOC, dokonywał wyważenia prawa do wolności wypowiedzi z prawem do poszanowania życia prywatnego.

3. Rada Europy – Konwencja 108 i rezolucje

A. Konwencja 108 Rady Europy z 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu 28.01.1981 r.

W Europie przez wiele lat prymat, jeśli chodzi o wyznaczanie standardów w obszarze ochrony danych osobowych, wiodła Rada Europy, a najważniejszym z efektów jej prac jest Konwencja 108 z 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. 11

> *WAŻNE!* Konwencja 108 została otwarta do podpisu w 1981 r. Weszła ona w życie 1.10.1985 r. po jej ratyfikacji przez Francję, Republikę Federalną Niemiec, Norwegię, Hiszpanię i Szwecję. Polska ratyfikowała Konwencję 108 dopiero 24.04.2002 r.

Konwencja określa minimalne dla państw-stron wymogi dotyczące ochrony danych osobowych. Do dziś pozostaje ona jednym z najważniejszych aktów prawnych w zakresie ochrony prywatności i danych osobowych. Jest także wciąż jedyną prawnie wiążącą umową wielostronną w dziedzinie ochrony danych osobowych. Na przestrzeni lat była uzupełniana, a niedawno zakończyły się prace zmierzające do jej modernizacji – Konwencja ma już bowiem ponad 30 lat i konieczne stało się jej dostosowanie do realiów społeczeństwa informacyjnego za pomocą odpowiedniego protokołu zmieniającego. Przed protokołem zmieniającym, który jednak nie jest jeszcze stosowany, najważniejszym uzupełnieniem jej tekstu wydaje się Protokół 12

dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych, CETS nr 181 (2001), który dotyczy zagadnienia przekazywania danych osobowych, a który miał na celu dostosowanie postanowień Konwencji do przepisów dyrektywy 95/46 i zminimalizowanie ryzyka konfliktów pomiędzy przepisami Konwencji, umożliwiającymi swobodne przekazywanie danych pomiędzy państwami-stronami, a przepisami dyrektywy 95/46, które co do zasady pozwalają na swobodny przepływ danych osobowych wyłącznie w ramach Europejskiego Obszaru Gospodarczego. Do protokołu dodatkowego nie przystąpiły jednak wszystkie państwa-strony Konwencji.

13 Stronami Konwencji są głównie państwa wchodzące w skład Rady Europy. **Pierwszym krajem spoza Europy, który przystąpił do Konwencji 108, był Urugwaj.** Uczynił to w sierpniu 2013 r. Kolejnym państwem spoza Europy był Mauritius, który uczynił to w październiku 2016 r. **Aktualnie Konwencja liczy 55 państw-stron: 47 państw członkowskich Rady Europy, Wyspy Zielonego Przylądka, Mauritius, Meksyk, Senegal, Tunezja, Urugwaj, Maroko i Argentyna.** Kolejne kraje – w tym Burkina Faso – zostały zaproszone do przystąpienia do traktatu.

Konwencja 108			
Państwa członkowskie Rady Europy			
Państwo	**Data podpisania**	**Data ratyfikacji**	**Data rozpoczęcia stosowania**
Albania	09.06.2004	14.02.2005	01.06.2005
Andora	31.05.2007	06.05.2008	01.09.2008
Armenia	08.04.2011	09.05.2012	01.09.2012
Austria	28.01.1981	30.03.1988	01.07.1988
Azerbejdżan	03.05.2010	03.05.2010	01.09.2010
Belgia	07.05.1982	28.05.1993	01.09.1993
Bośnia i Hercegowina	02.03.2004	31.03.2006	01.07.2006
Bułgaria	02.06.1998	18.09.2002	01.01.2003
Chorwacja	05.06.2003	21.06.2005	01.10.2005
Cypr	25.07.1986	21.02.2002	01.06.2002
Czechy	08.09.2000	09.07.2001	01.11.2001
Dania	28.01.1981	23.10.1989	01.02.1990
Estonia	24.01.2000	14.11.2001	01.03.2002
Finlandia	10.04.1991	02.12.1991	01.04.1992
Francja	28.01.1981	24.03.1983	01.10.1985
Gruzja	21.11.2001	14.12.2005	01.04.2006
Niemcy	28.01.1981	19.06.1985	01.10.1985
Grecja	17.02.1983	11.08.1995	01.12.1995
Węgry	13.05.1993	08.10.1997	01.02.1998
Islandia	27.09.1982	25.03.1991	01.07.1991
Irlandia	18.12.1986	25.04.1990	01.08.1990
Włochy	02.02.1983	29.03.1997	01.07.1997
Łotwa	31.10.2000	30.05.2001	01.09.2001

Konwencja 108			
Państwa członkowskie Rady Europy			
Państwo	**Data podpisania**	**Data ratyfikacji**	**Data rozpoczęcia stosowania**
Liechtenstein	02.03.2004	11.05.2004	01.09.2004
Litwa	11.02.2000	01.06.2001	01.10.2001
Luksemburg	28.01.1981	10.02.1988	01.06.1988
Malta	15.01.2003	28.02.2003	01.06.2003
Monako	01.10.2008	24.12.2008	01.04.2009
Czarnogóra	06.09.2005	06.09.2005	06.06.2006
Holandia	21.01.1988	24.08.1993	01.12.1993
Północna Macedonia	24.03.2006	24.03.2006	01.07.2006
Norwegia	13.03.1981	20.02.1984	01.10.1985
Polska	21.04.1999	23.05.2002	01.09.2002
Portugalia	14.05.1981	02.09.1993	01.01.1994
Mołdawia	04.05.1998	28.02.2008	01.06.2008
Rumunia	18.03.1997	27.02.2002	01.06.2002
Federacja Rosyjska	07.11.2001	15.05.2013	01.09.2013
San Marino	02.03.2015	28.05.2015	01.09.2015
Serbia	06.09.2005	06.09.2005	01.01.2006
Słowacja	14.04.2000	13.09.2000	01.01.2001
Słowenia	23.11.1993	27.05.1994	01.09.1994
Hiszpania	28.01.1982	31.01.1984	01.10.1985
Szwecja	28.01.1981	29.09.1982	01.10.1985
Szwajcaria	02.10.1997	02.10.1997	01.02.1998
Turcja	28.01.1981	02.05.2016	01.09.2016
Ukraina	29.08.2005	30.09.2010	01.01.2011
Wielka Brytania	14.05.1981	26.08.1987	01.12.1987
Państwa niebędące członkami Rady Europy			
Argentyna		25.02.2019 akcesja	01.06.2019
Burkina Faso		–	–
Wyspy Zielonego Przylądka		19.06.2018 akcesja	01.10.2018
Mauritius		17.06.2016 akcesja	01.10.2016
Meksyk		28.06.2018 akcesja	01.10.2018
Maroko		28.05.2019 akcesja	01.09.2019
Senegal		25.08.2016 akcesja	01.12.2016
Tunezja		18.07.2017 akcesja	01.11.2017
Urugwaj		10.04.2013 akcesja	01.08.2013

Źródło: obecnie niedostępna lista ratyfikacji na stronie WWW Council of Europe, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108.

14 Konwencja 108 oddziałuje jedynie w sferze publicznoprawnej – wiąże państwa, które ją ratyfikowały, i nie wywołuje skutków prawnych po stronie ich obywateli. Niemniej stanowiła pierwszy i dotychczas najważniejszy krok w stronę harmonizacji przepisów o ochronie danych osobowych na poziomie międzynarodowym. Konwencja 108 w art. 1 stanowi, iż:

> „[c]elem niniejszej konwencji jest zapewnienie każdej osobie fizycznej, bez względu na narodowość lub miejsce zamieszkania, poszanowania jej praw i podstawowych wolności na terytorium każdej ze stron konwencji, a w szczególności jej prawa do prywatności w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych («ochrona danych»)".

Odnosi się ona więc do automatycznego przetwarzania danych w sektorze publicznym i prywatnym. Jak słusznie wskazuje P. Litwiński, z perspektywy ochrony praw osób, których dane dotyczą, najistotniejszym przepisem Konwencji 108 jest jej art. 4, który wprowadza zasadę minimum ochrony danych osobowych [P. Litwiński, *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, Warszawa 2009, s. 19]. Przepis ten nakłada na strony Konwencji obowiązek dostosowania swoich wewnętrznych porządków prawnych do podstawowych zasad, które Konwencja 108 wprowadza (rozdział II Konwencji 108).

WAŻNE! **Podstawowe zasady Konwencji 108**:
- zasada adekwatności danych oraz związania celem zbierania danych;
- obowiązek odpowiedniego zabezpieczenia danych;
- obowiązek respektowania uprawnień informacyjnych osób, których dane dotyczą.

15 Zgodnie z art. 5 Konwencji 108:

> „[d]ane osobowe będące przedmiotem automatycznego przetwarzania powinny być: a) pozyskiwane oraz przetwarzane rzetelnie i zgodnie z prawem; b) gromadzone dla określonych i usprawiedliwionych celów i nie mogą być wykorzystywane w sposób niezgodny z tymi celami; c) odpowiednie, rzeczowe, niewykraczające poza potrzeby wynikające z celów, dla których są gromadzone; d) dokładne i w razie potrzeby uaktualniane; e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy niż jest to wymagane ze względu na cel, dla którego dane te zgromadzono".

16 Konwencja 108 na długo przed dyrektywą 95/46 (ratyfikowały ją wszystkie państwa członkowskie Unii Europejskiej) wprowadziła szereg rozwiązań, które zostały następnie przyjęte i rozwinięte przez unijnego ustawodawcę. Między innymi rozróżniała kategorię tzw. danych sensytywnych – danych szczególnie chronionych. Zgodnie z art. 6 Konwencji 108:

> „[d]ane osobowe ujawniające pochodzenie rasowe, poglądy polityczne, przekonania religijne lub inne, jak również dane osobowe dotyczące stanu zdrowia lub życia seksualnego nie mogą być przetwarzane automatycznie, chyba że prawo wewnętrzne zawiera odpowiednie gwarancje ochrony. To samo stosuje się do danych dotyczących skazujących wyroków karnych".

Konwencja 108 zawiera także m.in. postanowienia dotyczące obowiązku informacyjnego. Zgodnie z art. 8 Konwencji 108:

> „każda osoba powinna mieć zapewnione prawo do:
> a) ustalenia, czy istnieje zautomatyzowany zbiór danych osobowych, zawierający dane jej dotyczące, poznania podstawowych celów jego utworzenia, a także tożsamości, miejsca zamieszkania lub siedziby administratora tego zbioru;
> b) otrzymania, w rozsądnych odstępach czasu i bez zbędnej zwłoki oraz nadmiernych kosztów, potwierdzenia obecności danych jej dotyczących w zautomatyzowanym zbiorze oraz do uzyskania, w czytelnej formie, wglądu do tych danych;

c) uzyskania możliwości sprostowania lub usunięcia danych jej dotyczących, jeżeli zostały one przetworzone z naruszeniem przepisów prawa wewnętrznego zapewniających przestrzeganie zasad ustanowionych w artykułach 5 i 6 niniejszej konwencji;
d) złożenia skargi w przypadku odmowy odpowiedzi na żądanie potwierdzenia obecności w zbiorze lub odmowy wglądu do danych jej dotyczących, sprostowania lub usunięcia tych danych, w myśl zasad określonych w punktach b i c".

17 Jak wskazują J. Barta, P. Fajgielski i R. Markiewicz, Konwencja zachęca „kraje niemające regulacji na tym polu [ochrony danych osobowych – przyp. aut.] do wydania odpowiednich przepisów, ukierunkowując prace legislacyjne w tym zakresie i pozostawiając pewien margines swobody w kształtowaniu rozstrzygnięć odpowiadających danemu systemowi prawa" [J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, s. 46]. Margines swobody wydaje się przy tym niezbędny, gdyż trudno oczekiwać, aby w praktyce państwa trzecie od razu przyjmowały przepisy zapewniające poziom ochrony praw osób, których dane dotyczą, zbliżony do poziomu europejskiego.

18 Konwencja 108 w art. 2 zawiera cztery definicje.
Dane osobowe określa jako każdą informację dotyczącą osoby fizycznej o określonej tożsamości lub dającej się zidentyfikować („osoba, której dane dotyczą").
Zbiór zautomatyzowany jest zdefiniowany jako każdy zbiór danych będących przedmiotem automatycznego przetwarzania.
Automatyczne przetwarzanie oznacza następujące operacje wykonane w całości lub częściowo za pomocą procedur zautomatyzowanych: gromadzenie danych, stosowanie do nich operacji logicznych lub arytmetycznych, ich modyfikowanie, usuwanie, wybieranie lub rozpowszechnianie.
Administrator zbioru danych – zdefiniowano go jako „osobę fizyczną lub prawną, władzę publiczną, agencję lub każdy inny organ właściwy na podstawie prawa wewnętrznego do określenia celu, któremu ma służyć zautomatyzowany zbiór danych, kategorii gromadzonych danych osobowych oraz sposobu przetwarzania, jakiemu dane będą poddawane".
Konwencja 108 w art. 5 wskazuje, iż:

„[d]ane osobowe będące przedmiotem automatycznego przetwarzania powinny być:
a) pozyskiwane oraz przetwarzane rzetelnie i zgodnie z prawem;
b) gromadzone dla określonych i usprawiedliwionych celów i nie mogą być wykorzystywane w sposób niezgodny z tymi celami;
c) odpowiednie, rzeczowe, niewykraczające poza potrzeby wynikające z celów, dla których są gromadzone;
d) dokładne i w razie potrzeby uaktualniane;
e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy niż jest to wymagane ze względu na cel, dla którego dane te zgromadzono".

Harmonizacja przepisów prawa państw-stron Konwencji 108 ma umożliwiać swobodny przepływ danych osobowych pomiędzy nimi. Zgodnie z art. 12 ust. 2 Konwencji 108 jej strona nie może, uzasadniając to wyłącznie ochroną prywatności, zabronić przepływu danych osobowych przez granice na terytorium innej strony lub uzależniać tego przepływu od wydania specjalnego zezwolenia. Postanowienie to nie obowiązuje w sytuacji, gdy dane państwo wprowadziło u siebie bardziej restrykcyjne wymogi, które nie obowiązują w państwie, do którego dane mają zostać przekazane. Jednocześnie dozwolone jest zabronienie przepływu danych osobowych pomiędzy stronami Konwencji 108, jeżeli ma to na celu niedopuszczenie do obejścia przepisów prawa – gdy przepływ następuje z terytorium jednej strony, przez terytorium innej strony, na terytorium państwa niebędącego stroną Konwencji (art. 12 ust. 3).

WAŻNE! Pomimo że Konwencja 108 jest wiążąca dla państw, które ją ratyfikowały, nie podlega nadzorowi sądowemu Europejskiego Trybunału Praw Człowieka.

B. Rezolucje Rady Europy

19 W prace nad ochroną danych osobowych na poziomie Rady Europy, prócz samej Konwencji 108, wpisują się wydane w 1973 i 1974 r. rezolucje Komitetu Ministrów Rady Europy. Poświęcone one były kwestii ochrony sfery prywatności osób fizycznych w aspekcie wykorzystywania elektronicznych banków danych:
– w sektorze prywatnym – rezolucja 22 (73),
– w sektorze publicznym – rezolucja 29 (74).

20 Rezolucja 22 (73), dotycząca sektora prywatnego, wprowadza 10 zasad przetwarzania informacji dla sektora prywatnego. Między innymi podkreśla, że wszelkie rejestrowane informacje muszą być precyzyjne, adekwatne i aktualne. Informacje dotyczące sfery intymnej bądź inne mogące stanowić źródło dyskryminacji nie powinny co do zasady podlegać przetwarzaniu. **Wszelkie informacje powinny być adekwatne i niezbędne do celu przetwarzania.** Nie wolno ich pozyskiwać podstępnymi i nieuczciwymi metodami. Rezolucja wzywa do **ustalenia reguł czasowych, po przekroczeniu których pewne kategorie danych nie mogą być dłużej przechowywane lub wykorzystywane**. Wskazuje, że bez odpowiedniej podstawy informacje nie mogą być wykorzystane do celów innych niż te, dla których były zarejestrowane, ani też nie mogą być udostępniane osobom trzecim. Ustanawia także wymogi w zakresie zabezpieczeń.

21 Rezolucja 29 (74) wprowadza **osiem zasad przetwarzania informacji dla sektora publicznego**. Zgodnie z nią ważne są transparentność i przekazywanie opinii publicznej informacji o tworzeniu, funkcjonowaniu i rozwoju elektronicznych banków danych w sektorze publicznym. Rejestrowane informacje o osobach fizycznych powinny być precyzyjne, niezbędne, aktualne i adekwatne do celu przetwarzania, a zebrane informacje poprawne i adekwatne. Zbieranie informacji ze sfery intymnej bądź mogących stanowić źródło dyskryminacji może się odbywać tylko w przypadkach przewidzianych przez ustawę bądź inne unormowania specjalne. Zaleca się wprowadzenie okresów retencji danych. Wyjątkiem od tej zasady jest przetwarzanie informacji do celów statystycznych, naukowych lub historycznych. Dostęp do informacji, których nie można swobodnie udostępnić opinii publicznej, powinien być ograniczony do osób, którym są one potrzebne **w związku z pełnieniem funkcji zawodowych**. Zgodnie z ww. rekomendacją jeśli dane osobowe wykorzystuje się do celów statystycznych, nie mogą być one rozpowszechniane, chyba że w sposób uniemożliwiający powiązanie tego rodzaju informacji **z określoną osobą**.

C. Modernizacja Konwencji 108

22 Na forum Rady Europy w ostatnich latach toczyły się prace nad modernizacją tekstu Konwencji. Komitet T-PD przyjął swoją ostateczną propozycję w tym zakresie w listopadzie 2012 r. [Consultative Committee (T-PD) 'Modernisation of Convention 108: Final Document' T-PD(2012)4Rev4_en, Strasbourg, 18.12.2012]. CAHDATA – specjalna komisja utworzona *ad hoc* przez Komitet Ministrów Rady Europy – ukończyła swoje prace nad nowym tekstem w grudniu 2014 r. Zwieńczeniem tych prac było podpisanie w dniu 10.10.2018 r. przez 21 państw-stron dotychczasowej Konwencji 108 nowego traktatu Rady Europy mającego na celu modernizację Konwencji [Protokół zmieniający Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS nr 108)]. Jednym

z powodów, dla których prace nad modernizacją Konwencji trwały tak długo, były toczące się równolegle w Unii Europejskiej negocjacje dotyczące RODO i dyrektywy 2016/680. Artykuł 13 zmodernizowanego dokumentu wprost wskazuje, że strony mogą udzielić osobom, których dane dotyczą, szerszych środków ochrony niż przewidziane w Konwencji, co pozostawia stronom będącym państwami członkowskimi UE swobodę w zakresie wprowadzenia silniejszej ochrony, jaką przewiduje RODO. Zakończenie prac nad modernizacją Konwencji 108 już po uzgodnieniu tekstu RODO pozwoliło na wyeliminowanie ryzyka zaistnienia sytuacji, w której państwa członkowskie UE podlegałyby sprzecznemu z unijnym reżimowi prawnemu w obszarze ochrony danych osobowych.

Dokument pierwotnie podpisało 20 państw członkowskich Rady Europy: Austria, Belgia, Bułgaria, Czechy, Estonia, Finlandia, Francja, Niemcy, Irlandia, Łotwa, Litwa, Luksemburg, Monako, Holandia, Norwegia, Portugalia, Rosja, Hiszpania, Szwecja i Wielka Brytania, oraz Urugwaj. 16.05.2019 r. podczas szczytu Rady Europy w Helsinkach podpisała go także Polska. Polski parlament wyraził zgodę na ratyfikację zmodernizowanej Konwencji pod koniec 2019 r. (ustawa z 16.10.2019 r. o ratyfikacji Protokołu zmieniającego Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonego w Strasburgu dnia 10 października 2018 r.). **Prezydent RP ratyfikował Konwencję 108+ w dniu 10.06.2020 r.**

Zmiany wprowadzone w Konwencji pozwalają na przystąpienie do niej nie tylko poszczególnym państwom Unii Europejskiej, lecz także samej Unii Europejskiej. W odniesieniu do prawa głosu w ramach Komitetu Konwencji Unia będzie mogła głosować tylko w zakresie obszarów swoich kompetencji liczbą głosów równą liczbie jej państw członkowskich, które są stronami Konwencji. Aby zapobiec sytuacji, w której Unia mogłaby zdominować proces decyzyjny w ramach Komitetu Konwencji, postanowiono, że decyzje mogą być podejmowane wyłącznie „przeważającą większością" (czterech piątych głosów). Z kolei w przypadku najważniejszych decyzji dotyczących przestrzegania postanowień Konwencji przez jej stronę – „podwójną większością" (większością kwalifikowaną w połączeniu ze zwykłą większością głosów państw niebędących członkami UE).

Unia Europejska wydaje się postrzegać Konwencję 108+ jako instrument, do którego przystąpienie może stanowić pierwszy krok dla państw trzecich w kierunku wprowadzenia zbliżonych do europejskich zasad ochrony danych osobowych czy też uzyskania decyzji o adekwatności ochrony zapewnianej przez państwo trzecie.

Zmodernizowana Konwencja jest potocznie nazywana **Konwencją 108+**. Obejmuje ona wszelkiego rodzaju przetwarzanie danych osobowych, a nie – jak wcześniej – jedynie automatyczne przetwarzanie danych, wzmacnia ochronę praw osób, których dane dotyczą, a także mechanizmy kontroli przestrzegania przez państwa wymogów Konwencji. Polski organ ochrony danych osobowych jako **najważniejsze z wprowadzonych przez Konwencję 108+ zmian** wymienia (za stroną UODO: https://uodo.gov.pl/pl/61/552, dostęp: 25.10.2019 r.):

- mocniejsze wymogi dotyczące zasad proporcjonalności i minimalizacji danych oraz zgodności z prawem przetwarzania;
- rozszerzenie rodzajów danych wrażliwych, które będą teraz obejmować dane genetyczne i biometryczne, przynależność do związków zawodowych i pochodzenie etniczne;
- obowiązek zgłaszania naruszeń danych;
- większą przejrzystość przetwarzania danych;
- nowe prawa dla osób w kontekście podejmowania decyzji algorytmicznych, które są szczególnie istotne w związku z rozwojem sztucznej inteligencji;
- większą odpowiedzialność administratorów danych;
- wymóg stosowania zasady „poszanowania prywatności od samego początku";
- stosowanie zasad ochrony danych do wszystkich działań związanych z przetwarzaniem, w tym ze względów bezpieczeństwa narodowego, z ewentualnymi wyjątkami i ograniczeniami.

niami, z zastrzeżeniem warunków określonych przez Konwencję, a w każdym razie z niezależną i skuteczną kontrolą i nadzorem;
– jasny reżim transgranicznych przepływów danych;
– wzmocnione uprawnienia i niezależność organów ochrony danych oraz poprawę podstaw prawnych dla współpracy międzynarodowej.

Warto w tym kontekście odnotować wprowadzenie w Konwencji znanych z RODO praw osoby, której dane dotyczą:
– prawa do niepodlegania decyzjom wydanym wyłącznie w oparciu o zautomatyzowane przetwarzanie danych, a mającym znaczny wpływ na osobę, której dane dotyczą;
– prawa do wniesienia sprzeciwu wobec przetwarzania danych oraz
– prawa do środka odwoławczego w przypadku naruszenia praw osoby, której dane dotyczą.

Ponadto istotną zmianę stanowi brak możliwości całkowitego wyłączenia ze stosowania Konwencji określonych sektorów lub aktywności (np. w obszarze bezpieczeństwa narodowego), jaką przewidywał poprzedni tekst Konwencji. W tym kontekście warto pamiętać, że **Konwencja 108+ znajdzie zastosowanie także do przetwarzania danych przez organy ścigania**.

Na dzień 14.09.2021 r. 13 państw-stron Konwencji 108 ratyfikowało Konwencję 108+:

Państwa członkowskie Rady Europy		
Państwo	**Data podpisania**	**Data ratyfikacji**
Bułgaria	10.10.2018	10.12.2019
Chorwacja	22.03.2019	18.12.2019
Cypr	09.01.2019	21.09.2020
Estonia	10.10.2018	16.09.2020
Finlandia	10.10.2018	10.12.2020
Hiszpania	10.10.2018	28.01.2021
Litwa	10.10.2018	23.01.2020
Malta	02.07.2020	02.11.2020
Polska	16.05.2019	10.06.2020
Serbia	22.11.2019	26.05.2020
Włochy	05.03.2019	08.07.2021
Państwa niebędące członkami Rady Europy		
Mauritius	04.09.2020	04.09.2020
Urugwaj	10.10.2018	05.08.2021

Źródło: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

WAŻNE! Zmodernizowana Konwencja zapewnia również możliwość przystąpienia do niej Unii Europejskiej i organizacji międzynarodowych. Do rozpoczęcia jej stosowania wymagane są jednak bądź ratyfikacja przez wszystkie państwa-strony (art. 37 ust. 1 protokołu zmieniającego), bądź upływ 5 lat od otwarcia do podpisu (dojdzie do tego 10.10.2023 r.), przy spełnieniu warunku ratyfikacji Konwencji przez co najmniej 38 państw-stron (art. 37 ust. 2 protokołu zmieniającego). W świetle powyższego mimo ukończenia negocjacji nie rozpoczęło się jeszcze jej stosowanie.

4. Organizacja Współpracy Gospodarczej i Rozwoju – rekomendacja z 23.09.1980 r. w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami

23 Do powstania międzynarodowych standardów w zakresie ochrony danych osobowych przyczyniły się przede wszystkim dwie organizacje: wspomniana już Rada Europy, a także Organizacja Współpracy Gospodarczej i Rozwoju. To właśnie OECD jako pierwsza podjęła aktywność w tym zakresie. Jest to organizacja międzynarodowa funkcjonująca od 1961 r. i skupiająca 38 wysoko rozwiniętych państw świata. Podstawę jej funkcjonowania stanowi Konwencja o Organizacji Współpracy Gospodarczej i Rozwoju. **Główny cel OECD to wspieranie wzrostu ekonomicznego oraz handlu. Stąd nie powinno dziwić zainteresowanie OECD przetwarzaniem informacji i postępem technologicznym.** Gdy pojawiły się pierwsze krajowe ustawy dotyczące ochrony danych osobowych, aktualności nabrała kwestia ponadnarodowego przepływu danych – istotnego z punktu widzenia gospodarki. Wszelkie ograniczenia transferów danych mogły bowiem przynieść negatywne konsekwencje dla gospodarki. Konkretnym efektem prac OECD były projekty rekomendacji Komitetu ds. Polityki Naukowo-Technologicznej (ang. Committee for Scientific and Technological Policy). W 1979 r. grupa ekspercka przedstawiła swoje wytyczne razem z memorandum wyjaśniającym (ang. *Explanatory Memorandum*). **23.09.1980 r. Rada OECD formalnie przyjęła Wytyczne OECD w zakresie ochrony prywatności i przepływu danych osobowych przez granice** (ang. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, polska wersja językowa wytycznych dostępna jest tutaj: http://www.oecd.org/sti/ieconomy/15590241.pdf, dostęp: 27.10.2019 r.), jako aneks do niemających mocy wiążącej rekomendacji. **Celem** wytycznych było **zapobieżenie nieuzasadnionym ograniczeniom w transferach danych osobowych do państw trzecich**. Należy odnotować, że obejmowały one tak sektor prywatny, jak i publiczny, a także odnosiły się zarówno do zautomatyzowanego, jak i do niezautomatyzowanego przetwarzania danych osobowych. Wytyczne zachęcały też państwa członkowskie OECD do współpracy w zakresie ich implementacji. Podzielono je na następujące części:

- podstawowe zasady do zastosowania przez państwo;
- podstawowe zasady do zastosowania w zakresie międzynarodowym: wolny przepływ i uzasadnione ograniczenia;
- wdrożenie przez państwo;
- współpraca międzynarodowa.

24 Wytyczne OECD wprowadzały następujące **zasady przetwarzania danych do zastosowania przez państwo**:

Zasada	Treść
zasada ograniczonego zbierania	wymóg ustanowienia zasad zbierania danych osobowych, stosowania uczciwych i rzetelnych środków oraz zbierania danych za wiedzą lub zgodą podmiotu danych tam, gdzie jest to właściwe
zasada jakości danych	odpowiedniość danych do celu, w jakim mają być one użyte, niezbędność do jego realizacji, rzetelność, kompletność oraz aktualność danych

Zasada	Treść
zasada określenia celu	cele zbierania określone nie później niż w momencie zbierania, późniejsze użycie ograniczone do tych celów lub innych zgodnych z nimi i określonych podczas każdej zmiany celu
zasada ograniczenia użycia	dane osobowe nie powinny być ujawniane, udostępniane ani używane w żaden inny sposób do celów innych niż określone, z wyjątkiem przypadków: zgody podmiotu danych lub działania z mocy prawa
zasada zabezpieczeń	dane osobowe powinny być odpowiednio zabezpieczone przed ryzykiem w rodzaju utraty danych, nieupoważnionego dostępu, zniszczenia, użycia, modyfikacji lub ujawnienia danych
zasada jawności	ogólna zasada jawności ustaleń, praktyk i polityk dotyczących danych osobowych; dostępne powinny być sposoby ustalania istnienia i istoty danych osobowych, jak również głównego celu ich użycia oraz tożsamości i siedziby administratora danych
zasada udziału jednostki	prawo do otrzymania od administratora danych lub z innego źródła potwierdzenia posiadania lub nieposiadania przez administratora dotyczących jej danych; do otrzymania dotyczących jej danych: 1) w rozsądnym terminie; 2) bezpłatnie lub za umiarkowana opłatą; 3) w odpowiedni sposób oraz 4) w formie dla niej zrozumiałej; do uzyskania informacji o powodach odmowy realizacji żądania potwierdzenia oraz możliwości zakwestionowania takiej odmowy; do zakwestionowania danych odnoszących się do niej, a w wypadku uznania jej racji – prawa do usunięcia, korekty, uzupełnienia lub poprawienia danych
zasada odpowiedzialności	administrator danych powinien być odpowiedzialny za przestrzeganie reguł wprowadzających w życie wyżej opisane zasady

Źródło: opracowanie własne.

WAŻNE! Zasady określone w wytycznych OECD stanowią minimalne standardy ochrony, czyli nic nie stoi na przeszkodzie temu, aby państwa członkowskie OECD mogły wprowadzać bardziej rygorystyczne wymogi w zakresie przetwarzania danych.

5. Rezolucje ONZ

A. Rezolucja 34/169 Zgromadzenia Ogólnego ONZ: Kodeks Postępowania Funkcjonariuszy Porządku Prawnego

25 Rezolucja została przyjęta przy okazji 106. posiedzenia Zgromadzenia Ogólnego ONZ w dniu 17.12.1979 r. Dokument ten stanowi zalecenie dla funkcjonariuszy, którzy z racji pełnionych funkcji pozyskują dane innych osób. Reguluje on postępowanie z danymi osobowymi, które mogą być udostępniane wyłącznie w celu wypełniania obowiązków służbowych, a także dla potrzeb wymiaru sprawiedliwości.

B. Rezolucja 45 (95) Zgromadzenia Ogólnego ONZ: Wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych

14.12.1990 r. Zgromadzenie Ogólne ONZ przyjęło rezolucję zawierającą wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych. Także ta rezolucja nie miała charakteru wiążącego, określając, jakie gwarancje powinny być zapewnione w przepisach krajowych w zakresie komputerowego przetwarzania danych osobowych. 26

6. Podsumowanie

W ciągu ostatnich kilkunastu lat Internet ewoluował z ciekawostki technicznej wykorzystywanej przede wszystkim do pracy przez naukowców do narzędzia niezbędnego w codziennym życiu. Jednocześnie żyjemy w czasach, w których praktycznie każdy internauta ma konto na którymś z portali społecznościowych, robi w sieci zakupy czy korzysta z popularnych aplikacji służących do komunikacji. Od czasu wydania aktów prawa międzynarodowego, takich jak Europejska Konwencja Praw Człowieka czy Konwencja 108, rozwinął się cały segment usług świadczonych *on-line*, o olbrzymim znaczeniu dla gospodarki. Powstały nieznane wcześniej modele biznesowe i sposoby świadczenia usług. Co istotne, pojawiły się także całkowicie nieznane w latach 90. XX w. sposoby przetwarzania danych osobowych, np. przetwarzanie z wykorzystaniem **technologii chmury obliczeniowej, sztuczna inteligencja, Internet rzeczy czy Big Data**, a także zaawansowane środki umożliwiające ingerencję w życie prywatne jednostek wbrew ich woli i bez ich wiedzy. Wszystkie te nowe zjawiska stanowią wyzwanie z perspektywy zarówno zapewnienia skutecznej ochrony danych osobowych, jak i prawa do prywatności. Zasadna wydaje się teza, że prawo do prywatności wraz z postępem technologicznym i nowymi metodami gromadzenia informacji zyskało jeszcze większe znaczenie. Ochrona sfery prywatności, a więc obszaru intymności i odosobnienia od innych, wolności i decydowania o samym sobie, staje się w obecnych warunkach coraz większym wyzwaniem. Jedynym kompleksowym rozwiązaniem pojawiających się na tym tle problemów wydaje się **wypracowanie nowej umowy międzynarodowej, uwzględniającej realia technologiczne i wprowadzającej pewne minimalne, globalne standardy w zakresie ochrony danych osobowych oraz prawa do prywatności**. Warto odnotować, iż umowa taka, aby uzyskać odpowiednie poparcie, musiałaby przewidywać widocznie niższe od unijnych standardy ochrony danych osobowych. Stąd jej wypracowanie może być problematyczne nie tylko dla państw nieposiadających odpowiednich regulacji prawnych, lecz także dla tych o rygorystycznych przepisach o ochronie danych osobowych. Na chwilę obecną pozostaje więc śledzenie rozwoju już istniejących instrumentów, zwłaszcza zmodernizowanej Konwencji 108. 27

Orzecznictwo:

- wyrok ETPC z 15.04.2014 r., 50073/07, Radu v. Republika Mołdawii, HUDOC;
- wyrok ETPC z 6.06.2013 r., 1585/09, Avilkina i inni v. Federacja Rosyjska, HUDOC;
- decyzja ETPC z 4.06.2013 r., 7841/08 i 57900/12, Peruzzo i Martens v. Republika Federalna Niemiec, HUDOC;
- wyrok ETPC z 18.04.2013 r., 19522/09, M.K. v. Francja, HUDOC;
- wyrok ETPC z 7.02.2012 r., 39954/08, Axel Springer AG v. Niemcy, HUDOC;
- wyrok ETPC z 18.10.2011 r., 16188/07, Khelili v. Szwajcaria, HUDOC;

- wyrok ETPC z 10.05.2011 r., 48009/08, Mosley v. Zjednoczone Królestwo, HUDOC;
- wyrok ETPC z 2.09.2010 r., 35623/05, Uzun v. Niemcy, HUDOC;
- wyrok ETPC z 4.12.2008 r., 30562/04 i 30566/04, S. i Marper v. Zjednoczone Królestwo, HUDOC;
- wyrok ETPC z 2.12.2008 r., 2872/02, K.U. v. Finlandia, HUDOC;
- wyrok ETPC z 17.07.2008 r., 20511/03, I. v. Finlandia, HUDOC;
- wyrok ETPC z 3.04.2007 r., 62617/00, Copland v. Zjednoczone Królestwo, HUDOC;
- wyrok ETPC z 4.05.2000 r., 28341/95, Rotaru v. Rumunia, HUDOC;
- wyrok ETPC z 16.02.2000 r., 27798/95, Amann v. Szwajcaria, HUDOC;
- wyrok ETPC z 7.07.1989 r., 10454/83, Gaskin v. Zjednoczone Królestwo, HUDOC;
- wyrok ETPC z 26.03.1987 r., 9248/81, Leander v. Szwecja, HUDOC;
- wyrok ETPC z 2.08.1984 r., 8691/79, Malone v. Zjednoczone Królestwo, HUDOC;
- wyrok ETPC z 6.09.1978 r., 5029/71, Klass i inni v. Niemcy, HUDOC;
- orzeczenie Supreme Court of Michigan, DeMay v. Roberts, sygn. 46 Mich. 160, 9 N.W. 146, 1881 Mich.

Literatura: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015; M. Ciechomska, *Zmiana Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych szansą na powstanie globalnego instrumentu ochrony danych*, M. Praw. 2017/16; U. Góral, S. Kwaśny, *Proces modernizacji Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*, M. Praw. 2014/9; Helsińska Fundacja Praw Człowieka, omówienie orzecznictwa ETPC, https://www.hfhr.pl/publikacje/omowienie-orzeczen-etpcz/ (dostęp: 19.07.2021 r.); A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego (Zagadnienia konstrukcyjne)*, SC 1972/20; K. Kowalik-Bańczyk, *Sposoby regulacji handlu elektronicznego w prawie wspólnotowym i międzynarodowym*, LEX 2006; P. Litwiński, *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, Warszawa 2009; A. Mednis, *Ochrona prawna danych osobowych a zagrożenia prywatności – rozwiązania polskie* [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999; A. Mednis, *Prawna ochrona danych osobowych*, Warszawa 1995; A. Mednis, *Prawo do prywatności a interes publiczny*, Kraków 2006; A. Mednis, *Prywatność od epoki analogowej do cyfrowej – czy potrzebna jest redefinicja?* [w:] *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, red. A. Mednis, Warszawa 2016; Z. Mielnik, *Prawo do prywatności (zagadnienia wybrane)*, RPEiS 1996/2; R. Piotrowski, *Prawo do tożsamości informacyjnej i jego znaczenie w ustroju demokratycznym* [w:] *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka*, t. 1, red. J. Jaskiernia, Warszawa 2013; M. Safjan, *Czy prywatność jest wartością chronioną w społeczeństwie demokratycznym?*, „Rzeczpospolita" z 23.02.1998 r.; G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003; M. Szabłowska, *Ochrona prywatności w krajowych oraz w międzynarodowych systemach prawnych (zagadnienia wybrane)*, „Zeszyty Naukowe Ostrołęckiego Towarzystwa Naukowego" 2006/20; S.D. Warren, L.D. Brandeis, *The Right to Privacy*, „Harvard Law Review" 1890/4.

ROZDZIAŁ II

Prawo do ochrony danych osobowych jako prawo podstawowe (Karta Praw Podstawowych Unii Europejskiej, europejskie prawo pierwotne i wtórne, Konstytucja RP)

Michał Czerniawski, Krzysztof Wygoda

SPIS TREŚCI

1. Wprowadzenie 28
2. Prawo do ochrony danych osobowych w pierwotnym prawie europejskim 31
3. Dyrektywa 95/46 33
4. Prawo do ochrony danych osobowych w Karcie Praw Podstawowych Unii Europejskiej 39
5. Prawo do ochrony danych osobowych w Konstytucji RP 43
6. Prawo do ochrony danych osobowych jako prawo podstawowe – podsumowanie 65

Podstawa prawna: dyrektywa 95/46 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych; dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. WE L 178, s. 1); dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. WE L 201, s. 37, ze zm.); Karta Praw Podstawowych Unii Europejskiej; rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z 18.12.2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.Urz. WE L 8, s. 1); Traktat o funkcjonowaniu Unii Europejskiej; Traktat o Unii Europejskiej; Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzony w Lizbonie dnia 13.12.2007 r. (Dz.U. z 2009 r. Nr 203, poz. 1569); Wniosek rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final, 2017/03(COD).

1. Wprowadzenie

Michał Czerniawski

28 Najpierw w Niemczech (**pierwsza ustawa o ochronie danych osobowych została uchwalona przez kraj związkowy Hesja w 1970 r.**), a później w kolejnych państwach uchwalano akty prawne, których celem jest zapobieganie naruszeniom ochrony danych osobowych.

> ***WAŻNE!*** Pierwsza ustawa o ochronie danych osobowych została uchwalona w Hesji w roku 1970.

Pojawienie się przepisów prawa regulujących kwestie przetwarzania danych osobowych było bezpośrednio związane z postępem technologicznym i automatyzacją procesów przetwarzania danych. A. Mednis [*Prawna ochrona danych osobowych*, Warszawa 1995, s. 5] wskazuje, iż:

> „odpowiedzią na zagrożenia, jakie niósł ze sobą rozwój techniki, było pojawienie się nowych regulacji prawnych, w drodze których starano się stworzyć niezbędne gwarancje ochrony prywatności zapewniające bezpieczeństwo informacji o obywatelach".

J. Barta, P. Fajgielski i R. Markiewicz [J. Barta, P. Fagielski, R. Markiewicz, *Ochrona danych osobowych*, Warszawa 2015, s. 26] podkreślają, że:

> „[p]odstawowej przyczyny zainteresowania regulacją prawną przetwarzania danych osobowych upatrywać należy (…) w zastępowaniu tradycyjnych, manualnych metod gromadzenia i utrwalania informacji o osobach nowoczesnymi, skomputeryzowanymi systemami zapisywania, przetwarzania i udostępniania tego rodzaju danych".

Już w roku 1971 opracowany został projekt niemieckiej ustawy federalnej (która jednak weszła w życie dopiero 8 lat później – 1.01.1979 r.). W latach 70. ubiegłego wieku uchwalone zostały ustawy o ochronie danych osobowych w Szwecji, Francji, Luksemburgu, Austrii, Danii, Norwegii. W latach 80. i na przełomie lat 80. oraz 90. ubiegłego wieku regulacje w zakresie

ochrony danych osobowych uchwaliły m.in.: Islandia (1981), Wielka Brytania (1984), Finlandia (1987), Holandia (1988), Irlandia (1988), Portugalia (1991), Hiszpania (1992), Szwajcaria (1992) i Belgia (1992). Ochrona danych osobowych wywarła też wpływ na prawo konstytucyjne i same ustawy zasadnicze. Prócz przepisów szczegółowych, w drugiej połowie XX w. odniesienia do ochrony danych pojawiły się w wielu konstytucjach państw europejskich – m.in. Portugalii w 1976 r. (art. 35) i Hiszpanii w 1978 r. (art. 18).

29

W 1995 r. uchwalono najważniejszy w Europie, a być może także na świecie, **akt prawny w zakresie ochrony danych osobowych – dyrektywę 95/46 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych**, która harmonizowała zasady przetwarzania danych osobowych w Unii Europejskiej. Dyrektywa, jako akt prawa Unii Europejskiej wymagający implementacji, wymagała przyjęcia przez państwa członkowskie UE odpowiednich rozwiązań legislacyjnych do końca 1998 r. Wszystkie państwa członkowskie Unii Europejskiej uczyniły temu wymogowi zadość. Jednocześnie należy odnotować, że **ochrona danych osobowych do dnia dzisiejszego nie doczekała się regulacji międzynarodowej, która standaryzowałaby zasady przetwarzania danych osobowych na świecie**. Przyjęte przez unijnego prawodawcę rozwiązania, stosunkowo restrykcyjne, nie znalazły także na świecie zbyt wielu naśladowców. Jednocześnie powstałe w XX w. rozwiązania prawne, choć istotnie wpłynęły na sposób postrzegania ochrony danych osobowych, to w związku z szybkim postępem technologicznym obecnie wydają się nieco przestarzałe. W szczególności tak Konwencja 108, jak i dyrektywa 95/46, stanowiące przez długi czas podstawę systemu ochrony danych osobowych w Unii Europejskiej, były projektowane, jeszcze zanim nastąpił gwałtowny rozwój sieci Internet i technik komputerowych. Chociaż uwzględniały one automatyzację procesów przetwarzania danych osobowych (która była bezpośrednią przyczyną ich powstania), to nie mogły brać pod uwagę łatwości przekazywania informacji związanej z upowszechnieniem się Internetu, łatwości, z jaką można obecnie uzyskać dostęp do narzędzi umożliwiających masowe przetwarzanie danych osobowych, a także skali danych, które każdy użytkownik obecnie pozostawia po sobie w cyberprzestrzeni (wniosek dotyczący dyrektywy 95/46 został przedstawiony przez Komisję Europejską 18.07.1990 r., http://eur-lex.europa.eu/legal-content/pl/HIS/?uri=CELEX:31995L0046, dostęp: 25.07.2021 r.). Stąd też konieczne były zastąpienie dyrektywy 95/46 przez rozporządzenie 2016/679, a także prace nad modernizacją Konwencji 108. **Na to, że dyrektywa 95/46 coraz mniej przystaje do obecnych realiów technologicznych, jasno wskazywał także, obserwowany od 2012 r., znaczący wzrost liczby spraw przed Trybunałem Sprawiedliwości Unii Europejskiej, które jej dotyczyły.** Jeszcze kilka lat temu sprawy dotyczące ochrony danych osobowych pojawiały się przed Trybunałem Sprawiedliwości sporadycznie.

WAŻNE! Z istotniejszych spraw przed TSUE dotyczących ochrony danych osobowych w ostatnich latach można wskazać: C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, EU:C:2016:779; C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, EU:C:2015:639; C-362/14, Maximillian Schrems v. Data Protection Commissioner, EU:C:2015:650; C-201/14, Smaranda Bara i in. v. Președintele Casei Naționale de Asigurări de Sănătate i in., EU:C:2015:638; C-212/13, František Ryneš v. Úřad pro ochranu osobnich údajů, EU:C:2014:2428; C-486/12, X, EU:C:2013:836; C-615/13 P, ClientEarth i Pesticide Action Network Europe (PAN Europe) v. Europejski Urząd ds. Bezpieczeństwa Żywności, EU:C:2015:489; C-461/10, Bonnier Audio AB i in. v. Perfect Communication Sweden AB, EU:C:2012:219; C-468/10 i C-469/10, Asociacion Nacional de Establecimientos Financieros de Crédito (ASNEF) oraz Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administración del Estado, EU:C:2011:777; C-614/10, Komisja v. Austria, EU:C:2012:631; C-119/12, Josef Probst v. mr.nexnet GmbH, EU:C:2012:748; C-131/12, Google Spain i Google Inc. v. Agencia Española de Protección de Datos (AEPD) i Mario Costeja González, EU:C:2014:317; C-141/12 i C-372/12, YS v. Minister voor Immigratie, Integratie en Asiel oraz Minister voor Immigratie, Integratie en Asiel v. M i S, EU:C:2014:2081; C-288/12

Komisja v. Węgry, EU:C:2014:237; C-291/12, Michael Schwarz v. Stadt Bochum, EU:C:2013:670; C-293/12 i C-594-12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in., EU:C:2014:238; C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), EU:C:2013:355; C-473/12, Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert i in., EU:C:2013:715; C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), EU:C:2011:771; C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, EU:C:2017:197; C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme" EU:C:2017:336; C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, EU:C:2018:388; C-40/17, Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV, EU:C:2019:629.

30 Unijny prawodawca dostrzegł potrzebę rewizji opracowanych w latach 90. ubiegłego wieku standardów, tak aby zapewnić ochronę danych osobowych dostosowaną do aktualnego stopnia rozwoju technologii i nowych metod przetwarzania danych, a także zwiększyć poziom harmonizacji przepisów w poszczególnych państwach członkowskich. Stąd też w maju 2016 r. uchwalił RODO. Rozporządzenie 2016/679, jako forma aktu prawnego, w przeciwieństwie do dyrektywy, jest stosowane bezpośrednio we wszystkich państwach członkowskich. Aby umożliwić podmiotom danych kontrolę nad dotyczącymi ich informacjami, unijny ustawodawca zdecydował się na przyznawanie osobom fizycznym nowych uprawnień. W Unii Europejskiej są to np. wzmocnione prawo do bycia zapomnianym czy prawo do przenoszenia danych (por. art. 17 i 20 RODO). Na świecie coraz prężniej rozwijają się koncepcje, takie jak *privacy by design* (prywatność w fazie projektowania) oraz *privacy by default* (prywatność jako ustawienie domyślne), które mają na celu uwzględnienie ochrony prywatności już w fazie projektowania konkretnej technologii. Rozszerzono także zakres terytorialny stosowania przepisów o ochronie danych osobowych.

2. Prawo do ochrony danych osobowych w pierwotnym prawie europejskim

Michał Czerniawski

31 Wszelkie rozważania dotyczące prawa unijnego w obszarze ochrony danych osobowych należy rozpocząć od zagadnienia unijnych traktatów. Traktaty przyznają Unii Europejskiej wyłączne kompetencje w określonych dziedzinach. Zgodnie z art. 2 ust. 1 TFUE:

> „jeżeli Traktaty przyznają Unii wyłączną kompetencję w określonej dziedzinie, jedynie Unia może stanowić prawo oraz przyjmować akty prawnie wiążące, natomiast Państwa Członkowskie mogą to czynić wyłącznie z upoważnienia Unii lub w celu wykonania aktów Unii".

Przestrzeń, do której zaliczana jest ochrona danych osobowych, tj. przestrzeń wolności, bezpieczeństwa i sprawiedliwości, zgodnie z art. 4 ust. 2 lit. j TFUE zalicza się do tzw. kompetencji dzielonych między Unią Europejską a państwami członkowskimi. W takim przypadku zarówno Unia, jak i państwa członkowskie mogą stanowić prawo i przyjmować akty prawne w konkretnej dziedzinie. Jednocześnie **państwa członkowskie wykonują swoje kompetencje w zakresie, w jakim Unia nie skorzystała ze swojej prerogatywy**. Z perspektywy ochrony danych osobowych najważniejszy jest art. 16 TFUE.

WAŻNE! Artykuł 16 TFUE (dawny art. 286 TWE) w ust. 1 stanowi, że:

„każda osoba ma prawo do ochrony danych osobowych jej dotyczących".

Ustęp 2 mówi z kolei, 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 Unii oraz przez Państwa Członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów".

32 Artykuł 16 TFUE stanowi wyłącznie o ochronie osób fizycznych. Warto odnotować, że nie odnosi się on w żaden sposób do kwestii obciążeń nakładanych na administratorów danych czy podmioty przetwarzające, zagadnienia te znajdują się poza zakresem Traktatu. Jasno więc wskazuje, że to właśnie **ochrona osób, których dane dotyczą, i ich praw stanowi punkt wyjścia wszelkiej unijnej legislacji**. Przepis ten nie wspomina w żaden w sposób np. o konieczności znalezienia równowagi między ochroną danych osobowych a potrzebami europejskich przedsiębiorców, które mogłyby umożliwić im lepsze i bardziej konkurencyjne funkcjonowanie na globalnym rynku. W trakcie negocjacji RODO można było spotkać się w związku z tym ze stanowiskiem, że przy negocjowaniu tekstu nie powinno się uwzględniać innych kwestii niż ochrona praw osób, których dane dotyczą.

3. Dyrektywa 95/46

Michał Czerniawski

33 Przez ponad 20 lat podstawowym aktem prawa unijnego regulującym kwestie ochrony danych osobowych była dyrektywa 95/46. Prace nad nią toczyły się w latach 90. ubiegłego wieku, tj. w okresie, w którym część państw europejskich miała już przepisy regulujące przetwarzanie danych osobowych. Jak już wspomniano powyżej, Polska nie zaliczała się do tego grona. Przed wejściem w życie ustawy o ochronie danych osobowych z 1997 r. tego typu uregulowania były całkowicie nieznane polskiemu systemowi prawnemu [J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, s. 21]. Ponieważ państwa członkowskie Unii Europejskiej były także stronami Konwencji 108, **postanowienia dyrektywy 95/46 nie mogły być sprzeczne z postanowieniami Konwencji 108**. Jednocześnie art. 11 Konwencji 108 pozwala jej stronom na rozszerzenie zakresu przewidzianej w niej ochrony. Stanowi on, że:

„żaden z przepisów niniejszego rozdziału nie może być interpretowany jako ograniczający albo w inny sposób wpływający na uprawnienia strony do przyznania osobom, których dane dotyczą, szerszego zakresu ochrony niż przewidziany w niniejszej konwencji".

Tak jak w zakresie Europejskiej Konwencji Praw Człowieka właściwy pozostaje Europejski Trybunał Praw Człowieka, tak w zakresie sporów pojawiających się na tle interpretacji dyrektywy 95/46 właściwy był Trybunał Sprawiedliwości Unii Europejskiej.

WAŻNE! Poza zakresem dyrektywy 95/46 znalazły się zagadnienia współpracy policyjnej i sądowej w sprawach karnych. Ze względów traktatowych harmonizacji nie mogły podlegać także przepisy karne.

34 Jednocześnie **dyrektywa 95/46 nie objęła swoim zakresem przetwarzania danych osobowych przez instytucje unijne**. Przetwarzanie danych osobowych przez te podmioty regulowane było przez rozporządzenie 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, które następnie zostało zastąpione przez rozporządzenie 2018/1725 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.

35 Dyrektywa 95/46 to niejedyny akt prawa Unii Europejskiej, który regulował w owym czasie ochronę danych osobowych. Do odnoszących się do tego zagadnienia regulacji należy zaliczyć w szczególności **dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)**, która nadal obowiązuje. Takim aktem prawnym była też dyrektywa 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (**dyrektywa o zatrzymywaniu danych**), unieważniona przez Trybunał Sprawiedliwości Unii Europejskiej w wyroku z 8.04.2014 r., C-293/12 i C-594-12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in., EU:C:2014:238.

36 Tak jak Konwencja 108, **dyrektywa 95/46 określała minimalny poziom ochrony danych osobowych**. Oznacza to, że państwa członkowskie mogły w swoich porządkach prawnych przyjąć bardziej restrykcyjne przepisy. Celem dyrektywy 95/46 była harmonizacja przepisów o ochronie danych osobowych w poszczególnych państwach członkowskich Unii Europejskiej. Intencja ta wyrażona jest choćby w motywach 1, 4, 7 i 8 dyrektywy. Jak się wydaje, o intencji unijnego ustawodawcy najlepiej świadczy motyw 8 preambuły dyrektywy, który wskazuje, że:

> „w celu zniesienia przeszkód w przepływie danych osobowych, stopień ochrony praw i wolności jednostek w zakresie przetwarzania tych danych musi być jednakowy we wszystkich Państwach Członkowskich; cel ten ma żywotne znaczenie dla rynku wewnętrznego, lecz nie może on być osiągnięty przez same Państwa Członkowskie, szczególnie mając na uwadze skalę rozbieżności, jakie obecnie występują między odpowiednimi ustawodawstwami krajowymi oraz potrzebę dokonania koordynacji ustawodawstw Państw Członkowskich w celu zapewnienia jednolitej regulacji transgranicznego przepływu danych osobowych, zgodnie z celem rynku wewnętrznego przewidzianego w art. 7a Traktatu; konieczne są wspólnotowe działania na rzecz zbliżenia ustawodawstw".

Dyrektywa przyjmowała **szerokie rozumienie pojęcia danych osobowych, jak i przetwarzania danych** [J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, s. 65].

37 Choć dyrektywa 95/46 miała za zadanie zharmonizować ochronę danych osobowych w poszczególnych państwach członkowskich, udało jej się ten cel osiągnąć jedynie połowicznie. Jak wskazuje przytoczony powyżej jej motyw 8, celem dyrektywy było zrównanie stopnia ochrony praw i wolności jednostek w zakresie przetwarzania danych osobowych we wszystkich państwach członkowskich. Motyw ten podkreślał także znaczenie swobodnego przepływu danych dla rynku wewnętrznego. Z kolei jej motyw 10 wskazywał, że celem krajowych przepisów prawa dotyczących przetwarzania danych osobowych jest ochrona podstawowych praw i wolności, szczególnie prawa do prywatności, które zostało uznane zarówno w art. 8 EKPC, jak i w zasadach ogólnych prawa wspólnotowego. Z tego powodu zbliżanie przepisów prawa nie powinno wpłynąć na zmniejszenie ochrony, jaką gwarantują, lecz przeciwnie, musi dążyć do zapewnie-

nia jak najwyższego stopnia ochrony we Wspólnocie. Motyw 11 dyrektywy wprost odnosił się do Konwencji 108:

> „zasady ochrony praw i wolności jednostek, szczególnie prawa do prywatności, które zawarte są w niniejszej dyrektywie, utrwalają i umacniają zasady wyrażone w Konwencji Rady Europy z dnia 28 stycznia 1981 r. w sprawie ochrony jednostek w zakresie automatycznego przetwarzania danych osobowych".

38

W 2012 r. rozpoczęto modernizację dyrektywy 95/46. Prace nad nią zostały zakończone w grudniu 2015 r. (zob. Reforma ochrony danych w UE: Rada potwierdza porozumienie z Parlamentem Europejskim, informacja za: http://www.consilium.europa.eu/pl/press/press-releases/2015/12/18-data-protection/, dostęp: 25.07.2019 r.), a w maju 2016 r. oficjalnie opublikowano, mające zastąpić dyrektywę, ogólne rozporządzenie o ochronie danych. Weszło ono w życie **24.05.2016 r. i zaczęło być stosowane od 25.05.2018 r.** (należy podkreślić, że w przypadku aktów prawa unijnego wchodzą one w życie czasami na długo przed momentem, od którego zaczynają być stosowane – państwa członkowskie muszą mieć bowiem czas na dostosowanie swoich przepisów krajowych do wymogów unijnej legislacji). Na szczególną uwagę zasługuje tu sama forma tego aktu prawnego, który **jako unijne rozporządzenie jest bezpośrednio stosowany we wszystkich państwach członkowskich Unii Europejskiej**. Decyzję o zastąpieniu dyrektywy bezpośrednio stosowalnym rozporządzeniem należy ocenić jako ambitną i z pewnością mającą wpływ na sam proces negocjacji nowych przepisów, który ostatecznie pochłonął aż 4 lata. Państwa członkowskie z natury z większym dystansem podchodzą do przepisów bezpośrednio stosowalnych niż do tych, które wymagają implementacji w krajowych porządkach prawnych za pomocą ustaw, a przez to pozwalają na większą elastyczność krajowych prawodawców. **Rozporządzenia** stanowią akty prawne określone w art. 288 TFUE. **Są to akty ogólnego zastosowania, wiążące w całości i bezpośrednio stosowane we wszystkich krajach Unii Europejskiej.** Stanowią one część prawa wtórnego Unii Europejskiej. Przyjmowane są przez instytucje unijne zgodnie z traktatami założycielskimi. Mają na celu zapewnienie jednolitego stosowania prawa unijnego we wszystkich krajach UE. Rozporządzenia mają zastosowanie do abstrakcyjnych kategorii podmiotów prawnych, nie zaś do konkretnych podmiotów prawnych. Właśnie to odróżnia je od decyzji. Rozporządzenia są **wiążące w całości**. **Bezpośrednia stosowalność rozporządzenia oznacza, że natychmiast stanowi ono normę we wszystkich krajach Unii, bez potrzeby jego transpozycji do prawa krajowego.** Do określonych w nim praw i obowiązków dla podmiotów prawnych można się bezpośrednio odwoływać przed sądami krajowymi. Rozporządzenie może być także wykorzystywane jako punkt odniesienia przez podmioty prawne w stosunkach z innymi podmiotami prawnymi, krajami i organami Unii Europejskiej. Skutki prawne rozpoczęcia stosowania rozporządzenia są równocześnie, automatycznie i jednolicie wiążące w każdym prawodawstwie krajowym.

4. Prawo do ochrony danych osobowych w Karcie Praw Podstawowych Unii Europejskiej

Michał Czerniawski

39

Na początku XXI w. Unia Europejska zdecydowała się umieścić ochronę danych osobowych na liście praw, których ochronę gwarantuje Karta Praw Podstawowych UE – dokument zawierający zbiór praw człowieka i obowiązków obywatelskich uznawanych przez Unię Europejską

za mające **charakter fundamentalny**. Dokument ten zawiera „wspólną część podstawowych praw obywatelskich, które w tej czy w innej formie są wpisane do konstytucji i innych aktów prawnych państw członkowskich UE, aby stworzyć spójny zestaw norm dla tworzenia przyszłego prawa UE" [A. Szejna, A. Kosicki, *Karta Praw Podstawowych Unii Europejskiej i jej znaczenie dla Polski i Europy*, Warszawa 2008, s. 5]. Unia jednocześnie stawia sobie za cel ochronę praw podstawowych wynikających z Karty. Należy zwrócić uwagę, że przez wprowadzanie coraz to nowych regulacji dotyczących Internetu i środowiska cyfrowego (począwszy od dyrektywy o handlu elektronicznym, a skończywszy na ogólnym rozporządzeniu o ochronie danych oraz projekcie rozporządzenia o e-Prywatności) Unia Europejska niejako uprzedza wypracowywanie przez państwa członkowskie ewentualnych rozwiązań krajowych i *de facto* ogranicza swobodę państw członkowskich we wprowadzaniu własnych rozwiązań prawnych w tym zakresie (państwa członkowskie nie mogą bowiem regulować sfery, która została już zharmonizowana na poziomie unijnym). Stąd wraz z rosnącą liczbą regulacji na poziomie Unii Europejskiej krajowi prawodawcy mają coraz mniejsze pole manewru i coraz bardziej ograniczoną możliwość wprowadzania własnych przepisów, jest to natomiast korzystne dla harmonizacji prawa w Unii Europejskiej. Oczywiście państwa członkowskie uczestniczą w procesie legislacyjnym na poziomie Unii Europejskiej. Przede wszystkim w ramach Rady Unii Europejskiej, głównego organu decyzyjnego Unii, w której skład wchodzą ministrowie z każdego z państw członkowskich. We współpracy z Parlamentem Rada wydaje w toku procedur legislacyjnych akty prawnie wiążące (rozporządzenia, dyrektywy, decyzje). W najczęściej spotykanej, tzw. zwykłej procedurze ustawodawczej Rada pełni funkcję równorzędną z Parlamentem Europejskim, opracowując własną wersję projektu aktu prawnego przedłożonego przez Komisję Europejską, która jest następnie uzgadniana w ramach tzw. trilogu pomiędzy Radą, Parlamentem a Komisją Europejską. Niemniej **w ramach Rady każde z państw członkowskich posiada jedynie ograniczony wpływ na ostateczny kształt aktu prawnego**. Należy także pamiętać, że w procedurze tej wnioski ustawodawcze są przedkładane przez Komisję Europejską, a nie Radę.

40 **Bardzo duże zmiany w unijnym prawie ochrony danych osobowych przyniósł Traktat z Lizbony.** Wraz z jego wejściem w życie 1.12.2009 r. **zniósł** on **system filarowy Wspólnot Europejskich**, przyznał też m.in. Unii Europejskiej osobowość prawną. Z perspektywy niniejszej pracy szczególne zmiany miały miejsce w odniesieniu do przepisów o ochronie danych osobowych. **Traktat z Lizbony nadał bowiem moc wiążącą postanowieniom Karty Praw Podstawowych.**

> *WAŻNE!* Chociaż Karta Praw Podstawowych została uchwalona i podpisana 7.12.2000 r., to dopiero Traktat z Lizbony, który wszedł w życie 1.12.2009 r., nadał jej moc wiążącą w Unii Europejskiej.

Karta stanowi zbiór fundamentalnych praw człowieka i obowiązków obywatelskich przyjętych przez Komisję, Parlament Europejski i Radę. Ten akt prawny podkreśla wagę, jaką Unia Europejska przywiązuje do ochrony praw człowieka. Karta Praw Podstawowych w tym zakresie uzupełnia Traktaty. W szczególności **obejmuje ona cały zakres praw obywatelskich, politycznych, gospodarczych i społecznych obywateli Unii Europejskiej**. Podzielono je na sześć tytułów: godność, wolności, równość, solidarność, prawa obywatelskie i wymiar sprawiedliwości.

41 **Ochronie prywatności i danych osobowych poświęcone są art. 7 i 8 KPP UE.** Artykuł 7 (Poszanowanie życia prywatnego i rodzinnego) stanowi, że każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się. Z kolei art. 8 reguluje kwestie ochrony danych osobowych. I tak, ust. 1 tego przepisu stanowi, iż każdy ma prawo do ochrony danych osobowych, które go dotyczą. Zgodnie z art. 8 ust. 2 KPP UE, dane te muszą być

przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. Ustęp 3 wprowadza z kolei wymóg kontroli niezależnego organu nad przetwarzaniem danych osobowych.

Jednocześnie art. 51 ust. 1 KPP UE stanowi, iż: 42

> „postanowienia niniejszej Karty mają zastosowanie do instytucji, organów i jednostek organizacyjnych Unii przy poszanowaniu zasady pomocniczości oraz do Państw Członkowskich wyłącznie w zakresie, w jakim stosują one prawo Unii. Szanują one zatem prawa, przestrzegają zasad i popierają ich stosowanie zgodnie ze swymi odpowiednimi uprawnieniami i w poszanowaniu granic kompetencji Unii powierzonych jej w Traktatach".

5. Prawo do ochrony danych osobowych w Konstytucji RP

Krzysztof Wygoda

Zważywszy na fakt, że ochrona danych osobowych jest zjawiskiem relatywnie nowym – praktycznie niewystępującym w Polsce na płaszczyźnie prawnej, w swej czystej postaci, do końca lat 80. ubiegłego wieku – warto zastanowić się, czy obszar ten był w ogóle dostrzegany w regulacjach prawnych. Ku pewnemu zaskoczeniu można uznać, że tak, i to w sposób ciągły. Ukrywał się on jednak pod postacią szeroko ujętej ochrony prywatności jednostki – co nie oznacza oczywiście, że było to świadome działanie prawodawcy, który regulacjom tej sfery życia ludzkiego nie poświęcał zbyt wiele miejsca. 43

Należy też wskazać, że w odróżnieniu od krajów zachodnioeuropejskich samo prawo do prywatności zaczęło odgrywać poważniejszą rolę w regulacjach konstytucyjnych i orzecznictwie sądowym Polski (ale i pozostałych członków byłego bloku państw tzw. demokracji ludowej) stosunkowo niedawno. 44

> Można wskazać, że od przełomu lat 70. i 80. pojawiały się sukcesywnie orzeczenia Sądu Najwyższego nawiązujące do koncepcji prywatności jako dobra osobistego, np. wyroki: z 13.07.1977 r., 19.07.1979 r., 13.09.1979 r., które swe zwieńczenie znalazły w orzeczeniu z 18.01.1984 r. W tym właśnie wyroku w sposób niebudzący wątpliwości potwierdzono prawną ochronę dóbr osobistych występujących w sferze życia prywatnego i rodzinnego oraz sferze intymnej [zob. szerzej J. Braciak, *Prawo do prywatności*, Warszawa 2004 s. 135; J. Sieńczyło-Chlabicz, *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna*, Kraków 2006, s. 62–65].

W pewnym uproszczeniu można bowiem przyjąć, że przed 1989 r. istniejące w systemie prawnym gwarancje jego zachowania były najczęściej traktowane fasadowo. O ile można się było powoływać na te regulacje w ramach relacji występujących na płaszczyźnie horyzontalnego obowiązywania przepisów (w szczególności gdy objęte nim były relacje między osobami fizycznymi), o tyle na płaszczyźnie wertykalnej, w stosunkach państwo – obywatel jego praktyczne znaczenie było bliskie zeru.

Nie znaczy to oczywiście, że polska doktryna prawa nie dostrzegała, iż regulacje prawne dotyczące ochrony prywatności oraz wzrost świadomości istnienia takiego dobra osobistego i dążenie do jego ochrony wywierają coraz silniejszy wpływ na pozycję jednostki we współczesnych państwach demokratycznych. Wskazywano, że na koncepcję prywatności składają się zasady 45

i reguły dotyczące różnych sfer życia jednostki. Ich wspólnym mianownikiem było przyznanie człowiekowi prawa „do życia własnym życiem układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej".

[Szerzej na ten temat zob. np.: A. Kopff, *Koncepcje prawa do intymności i do prywatności życia. Zagadnienia konstrukcyjne*, SC 1972/20; W. Sokolewicz, *Prawo do prywatności* [w:] *Prawa człowieka w Stanach Zjednoczonych*, red. L. Pastusiak, Warszawa 1985.]

Tak rozumianą prywatność odnoszono generalnie do życia: osobistego, rodzinnego, towarzyskiego, nienaruszalności mieszkania, tajemnicy korespondencji i ochrony informacji dotyczących danej osoby – a skrótowo prywatność opisywano jako „prawo do pozostawienia w spokoju" czy „prawo jednostki do bycia pozostawioną samej sobie".

Najczęściej powoływane określenie prawa do prywatności – *a right to be let alone* – pojawiło się w pierwszym wydaniu *Law of Torts* T. Cooleya [1880, 2. wyd. 1888], znalazło się również w artykule *The Right to Privacy* S. Warrena i L. Brandeisa, opublikowanym w „Harvard Law Review" 1890/4, s. 193. To spopularyzowane głównie przez prawników anglosaskich rozumienie terminu *right to privacy* zrośnięte jest nierozerwalnie z najbardziej popularnym pojmowaniem prawa do prywatności w drugiej połowie wieku XX.

Przedstawiciele nauki już na początku lat 90. dostrzegali również fakt, że zapewnieniu prywatności najlepiej służyłoby zagwarantowanie jednostce prawa do „samookreślenia informacyjnego", a więc do jej wyłącznej decyzji pozostawiono by sprecyzowanie tego, kto, czego i w jaki sposób może się o niej dowiedzieć – co ściśle kojarzy się obecnie z ochroną danych osobowych.

Nota bene postulat ten wiąże się ściśle z definicją samej prywatności sformułowaną przez A. Westina, w której terminowi *privacy* odpowiada „żądanie jednostek do decydowania o tym, kiedy i w jakim zakresie informacja o nich ma być dostępna i komunikowana innym" [zob. L. Kański, *Prawo do prywatności, nienaruszalności mieszkania i tajemnicy korespondencji* [w:] *Prawa człowieka. Model prawny*, red. R. Wieruszewski, Ossolineum 1991, s. 321].

Oczywiście te najbardziej klasyczne koncepcje rozumienia prywatności konfrontowane były z podejściem dynamicznym do jego definicji [L. Kański, *Prawo*…, s. 321], gdyż postrzeganie prywatności jest niewątpliwie zmienne, podlega bowiem stałemu działaniu różnorakich czynników kulturowych, społecznych czy ekonomicznych – a świadczy o tym choćby postępujące rozpowszechnienie mediów społecznościowych.

46 Niektóre z ww. elementów definiujących prywatność chronione były wówczas (jak i obecnie) jako dobra samoistne. Nie zmienia to jednak faktu, że dopiero ich kompleksowa ochrona (jak ma to miejsce obecnie) stanowi gwarancję nienaruszalności życia prywatnego, zapewniając jednocześnie poszanowanie godności człowieka i jego egzystencji. Można się nawet pokusić o stwierdzenie, iż dla zachowania godności jednostki niezbędna jest ochrona prywatności człowieka wyrażająca się w nieingerencji (ze strony państwa, ale i innych podmiotów) w pewną określoną sferę życia jednostki i zabezpieczeniu jej przed nieuprawnionymi działaniami zmierzającymi do naruszenia owej sfery. To w obowiązującej obecnie Konstytucji RP wiąże się także z zapewnieniem jednostce prawa dostępu do danych dotyczących jej samej (łącznie z uprawnieniami do ich poprawiania czy usuwania), jeśli by takie znajdowały się w posiadaniu innych niż ona podmiotów – w tym bowiem wypadku mamy do czynienia z permanentną ingerencją w prywatność jako taką.

Zapewnieniu prywatności najlepiej służyłoby zapewne zagwarantowanie jednostce prawa do „samookreślenia informacyjnego", a więc do jej wyłącznej decyzji pozostawiono by sprecyzowanie tego, kto, o czym i w jaki sposób może się o niej dowiedzieć. Stan ten nie zostanie nigdy osiągnięty, choćby z uwagi na występujące w praktyce i całkowicie legalne ograniczenia prawa jednostki przewidziane w art. 8–11 EKPC czy art. 31 ust. 3 Konstytucji RP, które powszechnie uznaje się za

uzasadnione. Konieczne jest oczywiście, by ograniczenia te były formułowane w sposób czyniący zadość wymaganiom konstytucyjnym. Zasadniczo bowiem ograniczenie prawa bądź wolności może nastąpić tylko wówczas, gdy przemawia za tym inna norma, zasada lub wartość, a stopień tego ograniczenia musi pozostawać w odpowiedniej proporcji do rangi interesu, któremu ograniczenie to ma służyć – gdy odwołują się więc do klauzuli konieczności w demokratycznym społeczeństwie, wykazać należy odpowiednio pilną potrzebę społeczną wprowadzenia takich ograniczeń i ich proporcjonalność do realizowanego celu, pamiętając jednocześnie, że wszelkie ograniczenia muszą być przewidziane w akcie o randze ustawy (a zatem mogą być również ujęte w rozporządzeniu UE).

Należy przy tym pamiętać, że w dalszym ciągu w orzecznictwie:

„(…) na ogół przyjmuje się, że prywatność odnosi się m.in. do ochrony informacji dotyczących danej osoby i gwarancji pewnego stanu niezależności, w ramach której człowiek może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu (…)",

jest więc pojęciem szerszym niż sama ochrona danych osobowych.

Por. wyrok TK z 19.05.1998 r., U 5/97, OTK 1998/4, poz. 46. Należy jednak zaznaczyć, że już w 1984 r. Sąd Najwyższy – wyrokiem z 18.01.1984 r., I CR 400/83, LEX nr 2997 – wskazał, iż sfera życia prywatnego stanowi dobro osobiste człowieka podlegające ochronie w trybie art. 23 i 24 k.c. ze względu na otwarty katalog dóbr osobistych sformułowany w tym kodeksie. Istnienie prawa do prywatności znalazło też swe potwierdzenie w późniejszym orzecznictwie Sądu Najwyższego, choćby w orzeczeniu z 8.04.1994 r., III ARN 18/94, LEX nr 9376, w którym sąd ten odniósł koncepcję ochrony dóbr osobistych (art. 23 i 24 k.c.) do sfery życia prywatnego i sfery intymności.

Prywatność *per se* nie jest jednak przedmiotem tego opracowania, zatem choć miała i ma ona niewątpliwy wpływ na postrzeganie ochrony danych osobowych, zwłaszcza w odbiorze społecznym, czas zastanowić się, jaki charakter mają regulacje konstytucyjne poświęcone tej właśnie sferze. Pomocne będzie tu stanowisko TK, który wskazuje, że: **47**

„współczesne rozumienie sfery życia prywatnego w odniesieniu do danych osobowych prowadzi do objęcia ochroną każdej informacji osobowej bez względu na jej zawartość treściową – mogą to być zarówno takie informacje, które narażają osobę na uczucie wstydu czy skrępowania, ale i takie, które mają zawartość całkowicie indyferentną z punktu widzenia moralności czy obyczaju. Przedmiotem ochrony są bowiem na tle nowoczesnych ujęć prywatności wartości akcentujące możliwość prowadzenia swych spraw, decydowania o swym życiu i o rodzajach więzi personalnych z innymi z maksymalną swobodą, a zarazem z najmniejszym stopniem ingerencji świata zewnętrznego w tę sferę, która jest domeną własnej aktywności jednostki. Ów wspólny «korzeń aksjologiczny» prawa do życia prywatnego oraz do ochrony danych osobowych decyduje w dużym stopniu o potrzebie poszukiwania wspólnego uzasadnienia dla uznania za dopuszczalną ingerencji zewnętrznej w świat «odosobnienia jednostki» (…)" (wyrok TK z 12.11.2002 r., SK 40/01, OTK-A 2002/6, poz. 81).

Mimo chęci postrzegania prywatności i ochrony informacji o jednostkach jako zjawisk co najmniej częściowo odrębnych trudno nie dostrzec innego istotnego związku zachodzącego pomiędzy nimi – zgodnie z obowiązującą koncepcją normatywną źródłem obu jest godność ludzka (co wprost wynika z postanowień Konstytucji RP), a ich ochrona ma zapewnić nienaruszalność tej godności. Zdaniem TK art. 47 i 51 obowiązującej Konstytucji pozostają też ze sobą w następującej relacji: **48**

„(…) prawo do prywatności, statuowane w art. 47, zagwarantowane jest m.in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51. Ten ostatni, rozbudowany przepis, odwołując się

aż pięciokrotnie do warunku legalności – *expressis verbis* w ust. 1, 3, 4 i 5 oraz pośrednio przez powołanie się na zasadę demokratycznego państwa prawnego w ust. 2 – stanowi też konkretyzację prawa do prywatności w aspektach proceduralnych (…)" (por. wyrok TK z 19.05.1998 r., U 5/97, OTK 1998/4, poz. 46).

Artykuły 47 i 51 Konstytucji RP są kluczowe dla tego zagadnienia. Pierwszy gwarantuje prawo do prywatności, a drugi ochronę danych o charakterze osobowym. Należy podkreślić, że Konstytucja RP zawiera również inne przepisy regulujące wycinkowo pewne aspekty ochrony danych – jako przykładu można użyć art. 53 ust. 7: „Nikt nie może być obowiązany przez organy władzy publicznej do ujawnienia swego światopoglądu, przekonań religijnych lub wyznania". Z uwagi na ramy opracowania nie będą one jednak przedmiotem szczegółowej analizy.

Tak jednoznaczne identyfikowanie przez Trybunał Konstytucyjny funkcji gwarancyjnej, jaką mają spełniać przepisy art. 51 wobec art. 47 Konstytucji RP, nie jest jednak do końca tożsame z uznaniem ochrony informacji o osobach wyłącznie za zespół zasad technicznie chroniących prywatność. Wydają się one bowiem tworzyć samodzielne prawo podmiotowe jednostki, które nie musi być stale powiązane z ochroną prywatności, ale posiada własną odrębną rolę widoczną w szczególności w sytuacji, gdy przetwarzaniu podlegają dane publicznie dostępne – a osoba, której dane dotyczą, nie ma możliwości decydowania o tym fakcie.

49 Wracając jednak do początku regulacji przetwarzania danych osobowych w polskim systemie prawa, potrzebę zapewnienia im ochrony można było dostrzec, nawet zanim pojawiła się regulacja konstytucyjna. Od początku lat 90. widoczne było dążenie do ustanawiania fragmentarycznych regulacji prawnych określających zasady przetwarzania danych o charakterze osobowym, a za najbardziej aktualny temat, w kontekście konieczności ich ustanowienia, uznawano wówczas problem tzw. lustracji.

[Szerzej o przyczynach późniejszego niż w innych krajach europejskich uregulowania zasad ochrony danych osobowych, jak też o regulacjach prawnych istniejących w Polsce przed wejściem w życie ustawy o ochronie danych osobowych (chodzi tu np. o: art. 2 ust. 1 pkt 2 ustawy z 14.12.1982 r. o ochronie tajemnicy służbowej i państwowej, Dz.U. Nr 40, poz. 271 ze zm., tzw. uchwałę lustracyjną Sejmu z 28.05.1992 r., M.P. Nr 16, poz. 116, czy też art. 81 ust. 5 pkt 4 Ordynacji wyborczej do Sejmu z 28.05.1993 r., Dz.U. Nr 45, poz. 205); zob. np.: B. Banaszak, *Prawo do ochrony danych osobowych w Polsce* [w:] *O prawach człowieka w podwójną rocznicę Paktów. Księga pamiątkowa w hołdzie Profesor Annie Michalskiej*, red. T. Jasudowicz, C. Mik, Toruń 1996, s. 251–254; B. Banaszak, *Lustracja i dekomunizacja w Polsce w świetle praw jednostki w prawie wewnętrznym i międzynarodowym* [w:] *Prawa człowieka. Geneza, koncepcje, ochrona*, red. B. Banaszak, Wrocław 1993 oraz podana tam literatura.]

Co istotne, w tym początkowym okresie, wobec słabej podstawy konstytucyjnej, decydujące znaczenie wymuszające ich ustanowienie miało jednak wyraźne zagwarantowanie prawa do prywatności przez międzynarodowe regulacje dotyczące praw człowieka (stanowią o nim zwłaszcza art. 12 Powszechnej Deklaracji Praw Człowieka, art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych oraz art. 8 EKPC) i powiązanie – przez orzecznictwo europejskie – tego prawa z ogólną zasadą rządów prawa.

Ponieważ zarówno Pakt, jak i Konwencja zostały ratyfikowane przez Polskę, ustalone w nich normy były i są prawem wiążącym polskiego ustawodawcę – choć przyznać trzeba, iż proces ratyfikacji całości (zwłaszcza ich części dotyczących mechanizmów kontrolnych, a szczególnie skargi indywidualnej do ETPC) zakończył się dopiero w latach 90. (wejście w życie: 10.10.1994 r. i 1.11.1998 r.).

Umożliwiało to przyjęcie, że konieczność zapewnienia należytej ochrony prawu do prywatności w aspekcie ochrony informacji o jednostkach jest niezbędnym elementem demokratycznego państwa prawa, co dawało jednocześnie możliwość odwoływania się w warstwie aksjologicznej do art. 1 ówczesnej konstytucji (w wersji z 1989 r.).

W ustawie konstytucyjnej z 17.10.1992 r. o wzajemnych stosunkach między władzą ustawodawczą i wykonawczą Rzeczypospolitej Polskiej oraz o samorządzie terytorialnym (Dz.U. Nr 84, poz. 426 ze zm.), czyli tzw. Małej Konstytucji, z uwagi na jej specyficzny charakter i skupienie na dookreśleniu relacji pomiędzy poszczególnymi organami władzy problematyka ochrony danych, a nawet prywatności, nie była zauważalna.

Wszystko to odbywało się w sytuacji, w której przetwarzanie danych na szerszą skalę w sposób zautomatyzowany dopiero się w Polsce zaczynało, a w komputeryzacji widziano przede wszystkim nośnik postępu cywilizacyjnego oraz wygodne narzędzie zarządzania – nie zwracano przy tym uwagi na związane z tym zagrożenia, które zresztą nie ujawniały się z takim nasileniem jak obecnie. Trudno było w owym czasie przekonać kogokolwiek do konieczności ochrony danych osobowych jako wartości samej w sobie – zwłaszcza wobec palącej potrzeby informatyzacji administracji publicznej.

50

Tworzenie regulacji konstytucyjnych dotyczących ochrony danych nie było zatem priorytetem i w pierwszych projektach nowej konstytucji o danych osobowych nie wspominano właściwie wcale.

Takie podejście, marginalizujące to zagadnienie, widać było czasami nawet w dyskusji toczącej się od rozpoczęcia prac nad polską ustawą o ochronie danych osobowych (na początku lat 90.).

Dopiero pod koniec 1994 r. w dyskusjach i pracach Komisji Konstytucyjnej Zgromadzenia Narodowego zaczęto dostrzegać różne aspekty tego problemu. Pierwsze wzmianki o zagrożeniach związanych z przetwarzaniem danych o obywatelach znaleźć można w sprawozdaniu z posiedzenia podkomisji praw i obowiązków obywateli z 23.11.1994 r. [zob. „Biuletyn Komisji Konstytucyjnej Zgromadzenia Narodowego" 1995/10, s. 95].
W toku dalszych prac problem ochrony danych powracał, od dwunastoustępowego artykułu, mającego jednocześnie gwarantować prawo do prywatności i ochronę danych, poprzez różne skróty i syntezy (rozdzielenie tych dwu materii – artykuł poświęcony danym osobowym miał np. dwa ustępy), do ostatecznego brzmienia art. 51.

[Syntetyczne omówienie prac nad art. 51 Konstytucji RP (pomijające jednak prace podkomisji) prezentuje np. M. Wild [w:] *Konstytucja RP. Komentarz*, t. 1, *Art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016, s. 1224–1226.]

Ta znacząca rozbieżność w podejściu do konieczności wprowadzenia i zakresu projektowanej regulacji wynikała również stąd, że na poziomie ustawowym nie istniał wówczas jednolity wzorzec normatywny, a prace nad stworzeniem ustawy o ochronie danych osobowych toczyły się dość niemrawo.
Oprócz propozycji regulacji całości zjawiska pojawiały się także głosy, które koncentrowały się na niektórych tylko aspektach ochrony danych osobowych, związanych z konkretnymi potrzebami i rozwiązywaniem problemów pojawiających się w praktyce. Chodziło tu głównie o tzw. lustrację, w kontekście której zauważano zazwyczaj niekompletność zasobów archiwalnych MSW, równie często podkreślano, że uniemożliwia to w praktyce dokładne podanie informacji o współpracownikach byłych służb specjalnych PRL, starano się tym samym wskazać, że w tej sytuacji brak warunków do pełnego i obiektywnego zbadania posiadanych danych [por. m.in. B. Banaszak, *Die Aktualität des Lustrationsvorhabens in Polen*, „Datenschutz und Datensicherheit" 1997/3, s. 142–145].

51

Finał był jednak szczęśliwy i uchwalona 2.04.1997 r. Konstytucja zmieniła zasadniczo sytuację ustrojową w kwestii ochrony danych osobowych i prawa do prywatności. Zagwarantowanie w niej *expressis verbis* ogólnego prawa: „do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz prawa do decydowania o swoim życiu osobistym…" (art. 47) oraz niezależne od tego gwarancje ochrony informacji o charakterze osobowym z art. 51 pozwoliły na zaprzestanie praktyki wywodzenia prawa do ich ochrony z art. 23 i 24 k.c. (choć oczywiście

nic nie stoi na przeszkodzie, aby się na Kodeks cywilny powoływać, szczególnie dochodząc odszkodowania). Ochrona prawa do prywatności stała się więc konstytucyjną zasadą, która tylko wyjątkowo, na podstawie samej Konstytucji lub ustaw, może zostać uchylona. W Konstytucji RP podobną rolę pełni też art. 53 ust. 7, który stanowi dodatkową gwarancję w zakresie ograniczenia pozyskiwania informacji przedmiotowo związanej z wolnością sumienia i wyznania.

> Nie ulega wątpliwości, że reguły zeń wynikające, choć sam przepis nie odwołuje się do jakichkolwiek możliwości zawężenia swojego stosowania, tak jak w przypadku pozostałych wolności i praw, podlegać mogą ograniczeniom wynikającym z reguły ogólnej ich wprowadzania ustanowionej w art. 31 ust. 3 Konstytucji RP.

Dotyczy to wszystkich osób przebywających na terytorium RP, prawo to zostało bowiem ukształtowane jako prawo człowieka, a nie wyłącznie obywatela. Nieco inaczej rzecz się ma z podmiotowym zakresem art. 51 Konstytucji RP, najważniejszej regulacji dotyczącej ochrony danych osobowych. W ust. 2 tegoż artykułu mowa jest tylko o obywatelach – z czego można wywieść wniosek, że władze publiczne mogą przetwarzać informacje dotyczące innych osób, przy czym dane te nie muszą spełniać jednocześnie warunku niezbędności w demokratycznym państwie prawnym.

> Takie jednoznaczne podejście prezentuje M. Wild, wskazując, że „zakaz wyrażany przez omawianą normę odnosi się wyłącznie do informacji o obywatelach. Informacje o jednostkach, które nie posiadają polskiego obywatelstwa, nie są objęte jego hipotezą. Z tego względu pozyskiwanie, gromadzenie i udostępnianie informacji o podmiotach innych niż «obywatele» nie może być wprawdzie arbitralne, musi jednak czynić zadość gwarancjom art. 47, a nie art. 51 Konstytucji RP" [M. Wild [w:] *Konstytucja RP*…, t. 1, red. M. Safjan, L. Bosek, s. 1227].
>
> Jak się wydaje, jest to jednak podejście nieuwzględniające całego dorobku Trybunału Konstytucyjnego i doktryny, który wskazuje na konieczność równego traktowania wszystkich osób znajdujących się pod władztwem RP – a ewentualne odrębności możliwe są w przypadku wyraźnego wskazania, że ustrojodawca ma na myśli „obywatela RP", a nie wyłącznie „obywatela" – ten ostatni stanowi bowiem wyraz chęci gwarantowania danego prawa osobom fizycznym, a nie innym podmiotom. Na marginesie należy dodać, że autor ten uznaje, iż „co do zasady, jako błędne należałoby uznać łączne omawianie aspektów podmiotowych czy też przedmiotowych" – art. 51 Konstytucji RP. Tak postawiona teza łatwo może doprowadzić do gubienia kontekstu i funkcji poszczególnych jednostek redakcyjnych tego artykułu – nie da się też w oparciu o nią zdefiniować znaczenia ust. 5, który nakazuje stworzenie odpowiednich gwarancji ustawowych regulujących zasady i tryb gromadzenia danych.

52 I tu pojawia się pierwszy problem, albowiem sformułowanie: „informacje o obywatelach (…) niezbędne w demokratycznym państwie prawnym" może sprawić pewne trudności interpretacyjne. Trzeba bowiem postawić pytanie, czym właściwie są owe informacje niezbędne i czy należy je utożsamiać wyłącznie z danymi osobowymi obywateli RP.

> „(…) Ogólnie biorąc, wydaje się, iż informacje niezbędne można określić jako te dane, które umożliwiają normalne funkcjonowanie jednostki w zorganizowanym w państwo społeczeństwie i których ujawnienie jest naruszeniem jej prywatności" [B. Banaszak, M. Jabłoński [w:] *Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997 roku*, red. J. Boć, Wrocław 1998, s. 99].

Rozważając ten problem z punktu widzenia organów władzy, za niezbędną uznamy każdą informację, bez posiadania której nie będą one zdolne do podjęcia (czy zakończenia) działań w ramach przyznanych im kompetencji. Co do drugiej części pytania, to odpowiedź powinna być twierdząca, czego konsekwencją będzie (oczywiście tylko w stosunku do obywateli RP – po wejściu Polski do UE rozszerzono to na wszystkich jej obywateli) ograniczenie możliwości

zbierania pewnych kategorii danych w ramach już istniejących, jak i dopiero powstających baz danych. W tym kierunku zmierza też wypowiedź I. Lipowicz, która nie negując całkowicie możliwości działania krajowych i międzynarodowych banków danych i systemów informatycznych o charakterze policyjnym czy medycznym, stwierdza, że:

> „(…) jeżeli zakres podobnych systemów informacyjnych staje się dla wygody administracji zbyt szeroki (inwigilacja na wszelki wypadek szerszych grup społecznych, jednolite konto informacyjne obywatela powstające z integracji setek danych administracyjnych z różnych dziedzin) lub szczegółowość danych prowadzi do tworzenia profilów osobowych (uproszczonej informatycznej charakterystyki jednostki), czy wreszcie dochodzi do ukrytego lub jawnego oznaczenia obywateli za pomocą numerów identyfikacyjnych nie o charakterze porządkowym, lecz znaczącym, mamy do czynienia z przypadkiem wykraczania poza to, co niezbędne w demokratycznym państwie prawnym" [I. Lipowicz, *Konstytucyjne prawo do informacji a wolność informacji* [w:] *Wolność informacji i jej granice,* red. G. Szpor, Katowice 1997, s. 99].

W tym miejscu należy jednak wskazać, że kwestia niezbędności w demokratycznym państwie nie może być utożsamiana wprost z zasadami celowości przetwarzania i jego minimalizacji – które funkcjonują w nieco innym kontekście badania legalności procesów przetwarzania danych osobowych. Nie można wszakże zapominać o konieczności prowadzenia wykładni Konstytucji w sposób przychylny dla prawa unijnego, do czego zobowiązaliśmy się w 2004 r. Chcąc zatem wyprowadzać z Konstytucji zasady dające się pogodzić z regułami wynikającymi z RODO i dyrektywy 2016/680, uwzględniające przy tym konstytucyjny zakaz dyskryminacji i obowiązek równego traktowania, tylko szerokie ujęcie podmiotu chronionego i postrzeganie go jako osoby fizycznej poddanej władztwu RP pozwala zadośćuczynić tym założeniom. Nawet jednak kierując się bezpośrednio wskazówką niezbędności w demokratycznym państwie, trudno jest podać, jaki relewantny element statusu osoby niebędącej obywatelem RP uzasadniłby zbieranie przez władze jej danych w zakresie innym niż niezbędny w państwie demokratycznym. Prawo do ochrony informacji o sobie samym nie jest bowiem uprawnieniem o charakterze politycznym – związanym z realizacją jakiegokolwiek przejawu suwerenności narodu – a tylko odnalezienie takiego uzasadnienia pozwalałoby na różnicowanie traktowania obywateli i innych osób przebywających na terytorium RP. Zarówno ochrona prywatności, jak i danych osobowych przynależą do szerokiej grupy wolności i praw osobistych jednostki (nie tylko z uwagi na systematykę Konstytucji RP, lecz także ze względu na ich istotę), a zatem narodowość czy obywatelstwo nie stanowią *per se* istotnego składnika statusu prawnego osoby, która chce z nich korzystać. Państwo zaś musi tworzyć równe warunki ich realizacji, co jest w pełni zgodne z założeniami aktów unijnych. 53

> Pojawiające się zatem w tej części opracowania określenia „obywatel", „jednostka", „człowiek", „osoba fizyczna" należy traktować synonimicznie, bez przypisywania im prawnych odrębności znaczeniowych.

Wracając jednak do próby określenia samego zakresu omawianych wzorców konstytucyjnych, można posłużyć się cytatem z orzeczenia Trybunału Konstytucyjnego, który wychodząc od analizy treści art. 51 ust. 1 Konstytucji RP, wskazuje, że przepis musi być odczytywany w łączności z pozostałymi ustępami tego artykułu, gdyż dopiero w całości normy te realizują „najbardziej zasadnicze elementy składające się na treść prawa do ochrony życia prywatnego: respekt dla autonomii informacyjnej jednostki, a więc sam obowiązek udostępnienia danych ograniczony do ściśle określonych ustawowo sytuacji; ograniczenie arbitralności ustawodawcy – ustawa nie może zakresu obowiązku kształtować dowolnie, przy czym Konstytucja operuje w tym wypadku ograniczeniami dwojakiego rodzaju (co do formy – obowiązek udostępnienia danych musi być wprowadzony przez ustawę oraz co do materii – obowiązek jest uzasadniony jedynie w takim zakresie, w jakim jest to niezbędne w demokratycznym państwie prawnym); prawo do dostępu 54

do informacji gromadzonych przez władzę publiczną; wreszcie prawo sprostowania informacji nieprawdziwej, niepełnej lub zebranej niezgodnie z ustawą" (por. wyrok TK z 12.11.2002 r., SK 40/01, OTK-A 2002/6, poz. 81).
Artykuł 51 Konstytucji RP, poza uprawnieniami obywatela w sferze ochrony jego prywatności, jest zatem kluczową regulacją dotyczącą zapewnienia mu prawa dostępu do spersonalizowanych podmiotowo informacji znajdujących się w posiadaniu organów państwa i samorządu terytorialnego, a dotyczących jego samego.

> Można nawet twierdzić, że stanowi specyficzne, zindywidualizowane podmiotowo, wzmocnienie ustanowionego w art. 61 Konstytucji RP, ogólnie sformułowanego prawa do uzyskiwania informacji o działalności organów władzy publicznej czy jeszcze szerzej ujętego prawa do pozyskiwania i rozpowszechniania informacji – wynikającego z art. 54 ust. 1 Konstytucji RP.

Jak wskazuje M. Sakowska-Baryła, zapewnia on swego rodzaju autonomię informacyjną jednostki, która:

> „opiera się na zasadzie powstrzymywania się od działania wszelkich podmiotów, które chciałyby uzyskać informacje o jednostce (chyba że miałyby prawo do takiego pozyskania informacji), powiązanej z zasadą nieujawniania innym informacji o sobie bez bycia do tego przymuszonym na mocy przepisów ustawowych" [M. Sakowska-Baryła, *Dostęp do informacji publicznej a ochrona danych osobowych*, Wrocław 2014, s. 26].

55 Użyty w ust. 2 art. 51 zwrot: „urzędowe dokumenty i zbiory danych" sugeruje, że chodzi o wszelkie możliwe źródła informacji znajdujące się w posiadaniu którejkolwiek z trzech głównych władz (czy też tych organów władzy, które wymykają się klasycznemu podziałowi, np. Najwyższa Izba Kontroli, Krajowa Rada Radiofonii i Telewizji, Rzecznik Praw Obywatelskich czy inne instytucje typu „rzecznikowskiego"). Warto też zauważyć, iż pozwala on domagać się dostępu do pojedynczych zapisów/rekordów niebędących częścią większego zbioru.

> Wydaje się, iż umieszczenie informacji o charakterze osobowym w jakimkolwiek piśmie sporządzonym dla potrzeb czy wydanym przez organ władz publicznych pozwala na zakwalifikowanie go jako dokumentu urzędowego i raczej nieistotna jest tu kwestia nośnika informacji – wystarczające jest utrwalenie danych w postaci elektronicznej.

Ustrojodawca nie wyłączył z góry żadnych zbiorów informacji i dokumentów (np. będących w posiadaniu Służby Ochrony Państwa czy Policji), możliwe jest jednak ograniczenie dostępu do nich, o ile zostaną one wprowadzone w drodze ustawy. W tym miejscu należy sięgnąć do art. 31 ust. 3 Konstytucji RP, zawężającego zakres możliwych ograniczeń gwarantowanych konstytucyjnie praw i wolności wyłącznie do sytuacji, gdy jest to „konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw". W pełni odnosi się to do omawianego uprawnienia, z uwagi zaś na to, że „naruszenie istoty praw i wolności obywatelskich będzie miało miejsce wtedy, kiedy regulacja ustawowa uniemożliwi w praktyce korzystanie z tych praw i wolności" [por. B. Banaszak, M. Jabłoński [w:] *Konstytucje*…, s. 69], zasadne zdaje się stwierdzenie, że żaden organ państwa nie może przetwarzać informacji o obywatelach, nie licząc się z możliwością kontroli z ich strony. Zważając dodatkowo na, szczególnie istotną w tym kontekście, zasadę konstytucjonalizmu, stwierdzimy, że bezpośrednie odwoływanie się do przepisów konstytucyjnych powinno być obecnie normą w procesie stosowania prawa.

> ***WAŻNE!*** Zarówno sądy, jak i władza wykonawcza muszą więc działać zgodnie z literą, ale również duchem Konstytucji.

[Szerzej na temat tej zasady zob. np. K. Działocha *Zasada bezpośredniego stosowania konstytucji w dziedzinie wolności i praw obywateli* [w:] *Obywatel – jego wolności i prawa. Zbiór studiów przygotowanych z okazji 10-lecia urzędu Rzecznika Praw Obywatelskich*, Warszawa 1998, s. 26–44 i podana tam literatura.]

Dlatego nawet zbiory danych czy dokumenty zakwalifikowane jako tajne (np. z uwagi na bezpieczeństwo państwa) powinny zostać poddane weryfikacji na wniosek osoby, której dotyczą. I choć zapewne kontrola ta nie powinna przybierać w tym wypadku formy bezpośredniego dostępu zainteresowanego (a nawet gdyby, to po wprowadzeniu pewnych ograniczeń czasowych dotyczących momentu odtajnienia informacji) do owych danych, to dzięki możliwości odwołania się do krajowych organów nadzorczych – kiedyś do Generalnego Inspektora Ochrony Danych Osobowych (GIODO), obecnie do Prezesa UODO, a następnie do WSA i NSA – wyczerpana zostanie droga krajowa.

Obywatel będzie też mógł wnieść skargę konstytucyjną, co wywrze podobny skutek do działań podjętych przez Naczelny Sąd Administracyjny, jeśli zwróci się on do Trybunału Konstytucyjnego w sprawie ustalenia konstytucyjności przepisów, na podstawie których dane objęto klauzulą tajności – wówczas od Trybunału zależeć będzie, czy uzna on takie ograniczenie za uzasadnione. W przypadku gdy będzie miał jakieś wątpliwości, zażąda zapewne dostępu do „spornych" informacji. Jeśli jednostka zamierza zwracać się do organów międzynarodowych, skarga do Trybunału Konstytucyjnego (o ile nie zadziała w tym kierunku Naczelny Sąd Administracyjny) w zasadzie jest obligatoryjna.

Dalej sprawą będzie mógł się zająć Europejski Trybunał Praw Człowieka, który zbada ją pod kątem zachowania postanowień EKPC, zażądać będzie mógł również ujawnienia mu danych objętych klauzulą tajności.

Trybunał w Strasburgu zajmować się będzie wniesioną skargą, badając kolejno:
- czy fakty wskazane przez skarżącego stanowią naruszenie konkretnego prawa lub wolności;
- czy doszło do ingerencji władzy publicznej w korzystanie z danego prawa lub wolności;
- czy ingerencję taką dopuszczało prawo danego kraju i czy była ona konieczna w demokratycznym społeczeństwie.

Na tym ostatnim etapie do prawidłowej oceny zaistniałej sytuacji konieczne może stać się właśnie ujawnienie tajnych informacji, do których dostęp uniemożliwiono obywatelowi.

Warto zaznaczyć, że wejście w życie rozporządzenia 2016/679 doprowadziło do uwypuklenia problemu stosowania zasad ochrony danych osobowych w sytuacji ich przetwarzania przy użyciu metod zautomatyzowanych poza sformalizowanymi zbiorami. Co ciekawe, z uwagi na podniesione wyżej okoliczności problem ten *de facto* nie występował na gruncie konstytucyjnym, gdyż zakładano potencjalny dostęp do informacji znajdujących się nawet w niepowiązanych ze sobą dokumentach. Samo **pojęcie zbioru** występujące w Konstytucji RP nie powinno być jednak postrzegane przez pryzmat jego definicji sformułowanej w aktach poziomu ustawowego na potrzeby stosowania przepisów o ochronie danych osobowych (w szczególności nie należy go utożsamiać z definicją zbioru wyprowadzoną z przepisów ustawy o ochronie danych osobowych z 1997 r.). Ma ono wartość autonomiczną i winno się je postrzegać jako mające uzupełnić zakres uprawnienia jednostki w przypadkach, gdy jej dane przetwarzane będą nie w formie tradycyjnego urzędowego dokumentu (jakkolwiek rozumianego – przy czym należy zwrócić uwagę na czas powstania przepisów konstytucyjnych i ówczesne, relatywnie słabe, wykorzystanie informatycznych metod i form przetwarzania informacji), ale znajdować się one będą we wszelkiego rodzaju bazach danych, rejestrach, chmurach obliczeniowych pozostających w dyspozycji władz. Próba odczytywania sformułowania „zbiór danych" jako wyraz konieczności nadania takiemu zestawowi informacji sformalizowanych kryteriów wyszukiwawczych wydaje się, z punktu widzenia racjonalności konstytucyjnej, pozbawiona sensu, gdyż zawsze można by ją było zniwelować, sięgając po szeroką definicję urzędowego dokumentu jako nośnika danych. Ponadto odwoływanie się do tego typu argumentu (istnienia struktury, w której przechowuje

się dane) jako elementu ograniczającego prawo jednostki gwarantowane konstytucyjnie nie znajduje uzasadnienia w kontekście reguł ustanawiania ograniczeń praw i wolności wypływających z art. 31 ust. 3 Konstytucji RP – gdyż forma techniczna realizacji danego procesu przetwarzania informacji, odnosząca się do sposobu działania władzy, niespecjalnie nadaje się na cechę relewantną umożliwiającą różnicowanie przysługujących konstytucyjnie praw.

57 Trzeba zauważyć, że – literalnie rzecz ujmując – postanowienia Konstytucji RP adresowane są głównie do organów państwa (mowa jest przecież o władzach publicznych czy urzędowych dokumentach i zbiorach danych), nie można jednak na tej podstawie wnioskować, że podmioty niepubliczne nie podlegają ograniczeniom narzuconym przez art. 51. Podejście takie, jako nazbyt wąskie, niezgodne jest również z założeniem horyzontalnego oddziaływania norm konstytucyjnych. Jak słusznie zauważyła I. Lipowicz, będąca niewątpliwą pomysłodawczynią większości rozwiązań konstytucyjnych poświęconych ochronie informacji o charakterze osobowym, w tym oczywiście art. 51, nie ma w jego ust. 1 „podziału na sektor publiczny i prywatny. Oznacza to, że również żądanie informacji ze strony elektrowni czy telekomunikacji wymaga – jeżeli ma stać się obowiązkiem informacyjnym – podstawy ustawowej. Udzielenie informacji o sobie może być częścią umowy, musi jednak pozostawać w jej granicach i dawać swobodę wyboru" [I. Lipowicz, *Konstytucyjne*…, s. 14].
Horyzontalne obowiązywanie konstytucji we wszystkich obszarach, które mogą być nim objęte, i odejście od ściśle wertykalnych relacji państwo – obywatel jest niewątpliwie podstawą jej bezpośredniego stosowania i sprzyja budowaniu społeczeństwa otwartego, a w kontekście omawianych regulacji jest też gwarancją pozwalającą na tworzenie społeczeństwa informacyjnego. Jak największa pewność zakresu przysługujących jednostkom praw jest bowiem elementem upodmiotawiania się społeczeństwa, które w ich obronie może sięgać bezpośrednio do aktu rangi najwyższej, nie czekając na działania legislacyjne ustawodawcy.

> Inaczej oddziaływanie art. 51 widzi jednak M. Wild, bazując na literalnym brzmieniu uprawnień, sformułowanych np. w ust. 3 omawianej regulacji. Autor ten uznaje, że „domaganie się od podmiotów niepublicznych uzyskania dostępu do danych na swój temat nie znajduje zatem podstawy w art. 51 ust. 3, lecz wymaga uzasadnienia na gruncie ogólnego prawa do ochrony życia prywatnego" [M. Wild [w:] *Konstytucja RP*…, t. 1, red. M. Safjan, L. Bosek, s. 1232].

58 Kończąc to krótkie omówienie konstytucyjnego wymiaru ochrony danych osobowych, nie sposób pominąć kwestii konfliktu praw wynikającego z napięcia pomiędzy art. 51 a art. 61 Konstytucji RP. Warto bowiem pamiętać, że prawo do ochrony danych osobowych zostało ujęte w Konstytucji:

> „w taki sposób, że niejako w jego treści zostały bezpośrednio uwzględnione elementy, które powodują z góry jego ukształtowanie jako prawa o zakresie ograniczonym. W konsekwencji, samo zbieranie informacji zawierających dane osobowe, stanowiąc naruszenie sfery prywatności w szerszym zakresie, niekoniecznie jednak będzie automatycznie potraktowane jako naruszenie prawa do ochrony danych osobowych w zakresie działań władzy publicznej – a więc prawa nakierowanego na ochronę pewnego fragmentu prywatności i poddanego szczególnej reglamentacji prawnej (…). Naruszenia prawa konstytucyjnego do ochrony danych osobowych można upatrywać nie tyle więc w samym nałożeniu obowiązku ustawowego (…), ale w nałożeniu tego obowiązku w granicach wykraczających poza ramy wyznaczone przez Konstytucję, a więc z pogwałceniem przez ustawodawcę przesłanki «niezbędności w demokratycznym państwie prawnym»" (por. wyrok TK z 12.11.2002 r., SK 40/01, OTK-A 2002/6, poz. 81).

59 Jak wielokrotnie wskazywał Trybunał Konstytucyjny:

> „zarówno w odniesieniu do osób ubiegających się o funkcje publiczne, jak i osób pełniących takie funkcje, prawo do prywatności podlega istotnym ograniczeniom, uzasadnionym koniecz-

ością zapewnienia w demokratycznym państwie jego bezpieczeństwa (art. 31 ust. 3 Konstytucji). Prawo do prywatności, podobnie jak inne prawa i wolności, nie ma bowiem charakteru absolutnego i z tej też racji może podlegać ograniczeniom. Ograniczenia te winny jednak czynić zadość wymaganiom konstytucyjnym. Przemawiać za nimi muszą inne normy, zasady lub wartości konstytucyjne. Stopień ograniczenia powinien pozostawać w odpowiedniej proporcji do rangi interesu, któremu ograniczenie to służy. Ze względu na zasadę proporcjonalności niezbędne jest porównanie dobra chronionego i poświęcanego oraz zharmonizowanie kolidujących interesów" (wyrok TK z 20.03. 2006 r., K 17/05, OTK-A 2006/3, poz. 30).

Por. np. wyrok TK z 21.10.1998 r., K 24/98, OTK 1998/6, poz. 97, czy wyrok TK z 20.03.2006 r., K 17/05, OTK-A 2006/3, poz. 30. Kwestia ograniczenia prawa do prywatności bywała zresztą przedmiotem i innych orzeczeń Trybunału Konstytucyjnego, również tych pod rządami poprzednich regulacji konstytucyjnych, np.: orzeczenia: z 19.06.1992 r., U 6/92, OTK 1992/1, s. 204; z 26.04.1995 r., K 11/94, OTK 1995/1, s. 132–133; z 21.11.1995 r., K 12/95, OTK 1995/3, s. 141; z 24.06.1997 r., K 21/96, OTK 1997/2, poz. 23; uchwały: z 2.03.1994 r., W 3/93, OTK 1994/1, s. 158–159, oraz z 16.03.1994 r., W 8/93, OTK 1994/1, s. 168; z 24.06.1996 r., W 14/95, OTK 1996/2, s. 136].

Należy przy tym mieć na uwadze, że poza „koniecznością wskazania interesu mieszczącego się w katalogu zawartym w art. 31 ust. 3 Konstytucji, przesłanką legalności wkroczenia w zakres autonomii informacyjnej jednostki jest stwierdzenie, że wprowadzona regulacja ustawodawcza jest w stanie doprowadzić do zamierzonych przez nią skutków (zasada przydatności), jest niezbędna dla ochrony interesu publicznego, z którym jest powiązana (zasada konieczności), a jej efekty pozostają w proporcji do ciężarów nakładanych przez nią na obywatela (zasada proporcjonalności w ścisłym tego słowa znaczeniu; zob. np. wyrok TK w sprawie sygn. K 4/04; por. także wyrok TK z dnia 3 października 2000 r., sygn. K. 33/99, OTK ZU nr 6/2000, poz. 188)" (wyrok TK z 17.06.2008 r., K 8/04, OTK-A 2008/5, poz. 81).

60 Bezpieczeństwo państwa demokratycznego jest jednak sformułowaniem niezwykle pojemnym, którego powierzchowna egzegeza, zdarzająca się, niestety, w procesie stosowania prawa, dość łatwo może doprowadzić do nadużyć powodujących nadmierne ograniczenie innych, niezbędnych w nowoczesnym państwie, wartości czy zasad. Używanie tego rodzaju zwrotów w Konstytucji wydaje się jednak w pełni uzasadnione. Niemniej stosowanie ich przez ustawodawcę, szczególnie w kontekście uzasadniania przetwarzania danych osobowych – w tym ich udostępniania – nie jest najlepszym rozwiązaniem. Większe możliwości zapanowania nad rzeczywistym funkcjonowaniem norm daje tworzenie ich z myślą o zwalczaniu bądź promowaniu konkretnych, wskazanych w przepisach, działań wpływających na zapewnienie szeroko pojmowanego bezpieczeństwa państwa. Wyartykułowane dzięki temu „cele cząstkowe" powinny umożliwić jednoznaczną kwalifikację przydatności przyjętych rozwiązań – jako skutecznych lub nie – oraz ułatwiać ocenę proporcjonalności stosowanych do ich realizacji środków prawnych.

61 Szeroko pojęty dostęp do informacji o osobach pełniących funkcje publiczne nie powinien być postrzegany jako autonomiczny cel działań legislacyjnych – gdyż w takim wypadku nic (poza zaspokajaniem zwykłej ludzkiej ciekawości – co jednak trudno uznać za wartość konstytucyjną) nie uzasadnia odstąpienia od ochrony prywatności jednostki czy ograniczania jej autonomii informacyjnej. Dostęp do danych osobowych grupy ludzi, których relewantną cechą pozwalającą na odejście od zasad ogólnych jest właśnie pełnienie przez nich funkcji publicznych, należy postrzegać jako jeden z co najmniej kilku instrumentów użytych w celu ochrony bezpieczeństwa państwa demokratycznego.

62 Na gruncie Konstytucji RP odnalezienie sformułowań pozwalających na jednoznaczne rozumienie pojęcia osoby pełniącej funkcje publiczne jest, niestety, co najmniej trudne, a być może w ogóle niemożliwe. Zdaniem Trybunału Konstytucyjnego można jednak wskazać na kilka istotnych przesłanek pozwalających na zawężenie kręgu osób potencjalnie narażonych na utratę

pewnej części swej prywatności. Sprawowanie funkcji publicznej wiąże się bowiem z realizacją określonych zadań w ramach struktur szeroko pojętej władzy publicznej.

> „Wskazanie, czy mamy do czynienia z funkcją publiczną, powinno zatem odnosić się do badania, czy określona osoba w ramach instytucji publicznej realizuje w pewnym zakresie nałożone na tę instytucję zadanie publiczne. Chodzi zatem o podmioty, którym przysługuje co najmniej wąski zakres kompetencji decyzyjnej w ramach instytucji publicznej. Podejmując próbę wskazania ogólnych cech, jakie będą przesądzały o tym, że określony podmiot sprawuje funkcję publiczną, można bez większego ryzyka błędu uznać, iż chodzi o takie stanowiska i funkcje, których sprawowanie jest równoznaczne z podejmowaniem działań wpływających bezpośrednio na sytuację prawną innych osób lub łączy się co najmniej z przygotowywaniem decyzji dotyczących innych podmiotów. Spod zakresu funkcji publicznej wykluczone są zatem takie stanowiska, choćby pełnione w ramach organów władzy publicznej, które mają charakter usługowy lub techniczny" (wyrok TK z 11.05.2007 r., K 2/07, OTK-A 2007/5, poz. 48).

63 Dodatkowo można przyjąć, że:

> „kategoria osób pełniących funkcje publiczne nie może obejmować funkcji, stanowisk i zawodów, które nie mają żadnego związku z władztwem publicznym (*imperium*) ani z gospodarowaniem mieniem komunalnym lub majątkiem skarbu Państwa (*dominium*). Cechą relewantną wyróżniającą kategorię «osób pełniących funkcje publiczne» jest rzeczywiste wykonywanie władztwa publicznego bądź gospodarowanie mieniem komunalnym lub Skarbu Państwa" (wyrok TK z 11.05.2007 r., K 2/07, OTK-A 2007/5, poz. 48).

W odniesieniu do tak nieostrego kryterium trudno zatem o jednoznaczną ocenę jego skuteczności czy proporcjonalności. Jeśli jednak oceniać go chcemy przez pryzmat dążeń prawodawcy podejmowanych w celach konkretnych (uznawanych powszechnie za przyczyniające się do wzrostu bezpieczeństwa czy choćby zapewnienia niezbędnego minimum), to głębokość dopuszczalnej ingerencji w sferę prywatności jednostki nie będzie zawsze taka sama. Tytułem przykładu można wskazać choćby na różnice między zakresem danych udostępnianych w celu zapewnienia sprawnego i przyjaznego obywatelowi funkcjonowania organów władzy publicznej a ujawnianiem informacji koniecznych do zwalczania korupcji, nepotyzmu, nadużywania stanowisk w celu osiągania korzyści majątkowych lub osobistych czy wreszcie ochrony przed bezprawnymi naciskami wpływającymi na realizacje kompetencji państwa.

64 Podjęcie działania zakładającego tego typu kontrolę nad procesami związanymi z informowaniem społeczeństwa o istotnych, z punktu widzenia ochrony demokratycznych wartości, szeroko pojmowanych cechach osób pełniących funkcje publiczne winno zaowocować stworzeniem regulacji niesprawiającej trudności w procesie jej stosowania. Pewność i dostateczna określoność norm będą w tym wypadku spełniały założenia dobrej legislacji, ułatwią też niewątpliwie kontrolę stworzonych zasad właśnie pod kątem ich zgodności z Konstytucją – choćby w kontekście ich proporcjonalności. Należy bowiem pamiętać, że w Konstytucji RP możemy łatwo odnaleźć zarówno normy chroniące prywatność (art. 47, 51 czy 53 ust. 7), jak i te gwarantujące prawo do informacji czy – ujmując rzecz szerzej – wolność wypowiedzi (art. 14, 54, 49, 61, 73). Przepisy o dostatecznej jasności ułatwiają też zachowanie zasady, wielokrotnie wyrażanej przez Trybunał Konstytucyjny, z której wynika, że:

> „kolizja praw i zasad na poziomie konstytucyjnym nie może prowadzić w ostatecznym wyniku do pełnej eliminacji jednego z praw pozostających w konflikcie. Problemem wymagającym rozstrzygnięcia jest zawsze w takim wypadku znalezienie pewnego punktu równowagi, balansu dla wartości chronionych przez Konstytucję i wyznaczenie obszaru stosowania każdego z praw" (por. np. wyrok TK z 20.03.2006 r., K 17/05, OTK-A 2006/3, poz. 30).

6. Prawo do ochrony danych osobowych jako prawo podstawowe – podsumowanie

Michał Czerniawski

Prawo do ochrony danych osobowych bardzo szybko uzyskało rangę jednego z bardziej istotnych praw podstawowych w Unii Europejskiej. Nie budzi przy tym wątpliwości, że taki stan rzeczy jest bezpośrednio związany z postępem technologicznym i automatyzacją procesów przetwarzania danych. Jest ono przedmiotem rosnącej liczby orzeczeń Trybunału Sprawiedliwości Unii Europejskiej, a rozpoczęcie stosowania ogólnego rozporządzenia o ochronie danych jeszcze wzmocniło jego znaczenie. Już teraz, mimo niecałych 2 lat od rozpoczęcia stosowania nowych unijnych przepisów, można mówić o „efekcie RODO", gdyż coraz więcej państw świata reguluje w swoich porządkach prawnych kwestie ochrony danych osobowych, a **unijne standardy w obszarze ochrony danych osobowych coraz częściej stają się wzorem dla tego typu analogicznych regulacji**. Jednocześnie należy pamiętać, że prawo do ochrony danych osobowych nie jest prawem bezwzględnym i podlega pewnym ograniczeniom – musi być choćby ważone z innymi prawami podstawowymi, w sytuacji gdy są one ze sobą w sprzeczności. W najbliższych latach należy się spodziewać znaczącego wzrostu liczby spraw przed Trybunałem Sprawiedliwości Unii Europejskiej dotyczących ochrony danych osobowych, co przyczyni się do jeszcze szybszego rozwoju tej gałęzi prawa.

Orzecznictwo:

- wyrok TS z 29.07.2019 r., C-40/17, Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV., EU:C:2019:629;
- wyrok TS z 5.06.2018 r., C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, EU:C:2018:388;
- wyrok TS z 4.05.2017 r., C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA „Rīgas satiksme" EU:C:2017:336;
- wyrok TS z 9.03.2017 r., C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, EU:C:2017:197;
- wyrok TS z 19.10.2016 r., C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, EU:C:2016:779;
- wyrok TS z 6.10.2015 r., C-362/14, Maximillian Schrems v. Data Protection Commissioner, EU:C:2015:650;
- wyrok TS z 1.10.2015 r., C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, EU:C:2015:639;
- wyrok TS z 1.10.2015 r., C-201/14, Smaranda Bara i in. V. Preşedintele Casei Naţionale de Asigurări de Sănătate i in., EU:C:2015:638;
- wyrok TS z 16.07.2015 r., C-615/13 P, ClientEarth i Pesticide Action Network Europe (PAN Europe) v. Europejski Urząd ds. Bezpieczeństwa Żywności, EU:C:2015:489;
- wyrok TS z 11.12.2014 r., C-212/13, František Ryneš v. Úřad pro ochranu osobnich údajů, EU:C:2014:2428;
- wyrok TS z 17.07.2014 r., C-141/12 i C-372/12, YS v. Minister voor Immigratie, Integratie en Asiel oraz Minister voor Immigratie, Integratie en Asiel v. M i S, EU:C:2014:2081;
- wyrok TS z 13.05.2014 r., C-131/12, Google Spain i Google Inc. v. Agencia Española de Protección de Datos (AEPD) i Mario Costeja González, EU:C:2014:317;
- wyrok TS z 8.04.2014 r., C-293/12 i C-594-12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in., EU:C:2014:238;
- wyrok TS z 8.04.2014 r., C-288/12, Komisja v. Węgry, EU:C:2014:237;
- wyrok TS z 12.12.2013 r., C-486/12, X, EU:C:2013:836;
- wyrok TS z 7.11.2013 r., C-473/12, Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert i in., EU:C:2013:715;
- wyrok TS z 17.10.2013 r., C-291/12, Michael Schwarz v. Stadt Bochum, EU:C:2013:670;
- wyrok TS z 30.05.2013 r., C-342/12, Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT), EU:C:2013:355;
- wyrok TS z 22.11.2012 r., C-119/12, Josef Probst v. mr.nexnet GmbH, EU:C:2012:748;

– wyrok TS z 16.10.2012 r., C-614/10, Komisja v. Austria, EU:C:2012:631;
– wyrok TS z 19.04.2012 r., C-461/10, Bonnier Audio AB i in. v. Perfect Communication Sweden AB, EU:C:2012:219;
– wyrok TS z 24.11.2011 r., C-468/10 i C-469/10, Asociacion Nacional de Establecimientos Financieros de Crédito (ASNEF) oraz Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administración del Estado, EU:C:2011:777;
– wyrok TS z 24.11.2011 r., C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), EU:C:2011:771;
– wyrok TK z 17.06.2008 r., K 8/04, OTK-A 2008/5;
– wyrok TK z 11.05.2007 r., K 2/07, OTK-A 2007/5;
– wyrok TK z 20.03.2006 r., K 17/05, OTK-A 2006/3;
– wyrok TK z 12.11.2002 r., SK 40/01, OTK-A 2002/6;
– wyrok TK z 21.10.1998 r., K 24/98, OTK 1998/6;
– wyrok TK z 19.05.1998 r., U 5/97, OTK 1998/4;
– uchwała TK z 24.06.1996 r., W 14/95, OTK 1996/2;
– uchwała TK z 16.03.1994 r., W 8/93, OTK 1994/1;
– uchwała TK z 2.03.1994 r., W 3/93, OTK 1994/1;
– orzeczenie TK z 24.06.1997 r., K 21/96, OTK 1997/2;
– orzeczenie TK z 21.11.1995 r., K 12/95, OTK 1995/3;
– orzeczenie TK z 26.04.1995 r., K 11/94, OTK 1995/1;
– orzeczenie TK z 19.06.1992 r., U 6/92, OTK 1992/1;
– wyrok SN z 8.04.1994 r., III ARN 18/94, LEX nr 9376;
– wyrok SN z 18.01.1984 r., I CR 400/83, LEX nr 2997.

Literatura: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych*, Warszawa 2015; J. Braciak, *Prawo do prywatności*, Warszawa 2004; K. Działocha *Zasada bezpośredniego stosowania konstytucji w dziedzinie wolności i praw obywateli* [w:] *Obywatel – jego wolności i prawa. Zbiór studiów przygotowanych z okazji 10-lecia urzędu Rzecznika Praw Obywatelskich*, Warszawa 1998; I. Lipowicz, *Konstytucyjne prawo do informacji a wolność informacji* [w:] *Wolność informacji i jej granice,* red. G. Szpor, Katowice 1997; L. Kański, *Prawo do prywatności, nienaruszalności mieszkania i tajemnicy korespondencji* [w:] *Prawa człowieka. Model prawny*, red. R. Wieruszewski, Ossolineum 1991; *Konstytucja RP. Komentarz*, t. 1, *Art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016; *Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997 roku*, red. J. Boć, Wrocław 1998; A. Mednis, *Prawna ochrona danych osobowych*, Warszawa 1995; M. Sakowska-Baryła, *Dostęp do informacji publicznej a ochrona danych osobowych*, Wrocław 2014; J. Sieńczyło-Chlabicz, *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna*, Kraków 2006; A. Szejna, A. Kosicki, *Karta Praw Podstawowych Unii Europejskiej i jej znaczenie dla Polski i Europy*, Warszawa 2008.

ROZDZIAŁ III

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Edyta Bielak-Jomaa, Witold Chomiczewski, Urszula Góral, Mirosław Gumularz, Tomasz Izydorczyk, Damian Karwala, Patrycja Kozik, Dominik Lubasz, Joanna Łuczak-Tarka, Arwid Mednis, Monika Susałko, Katarzyna Witkowska-Nowakowska

SPIS TREŚCI

1. **Wprowadzenie** 66

2. **Zakres zastosowania ogólnego rozporządzenia o ochronie danych** 85

A. Zakres przedmiotowy 86
B. Zakres terytorialny 96

3. **Podstawowe pojęcia** 100

A. Wprowadzenie 100
B. Dane osobowe 103
a. Znaczenie pojęcia 103
b. Wszelkie informacje 104
c. Informacje dotyczące osoby fizycznej 105
d. Informacje pozwalające na zidentyfikowanie osoby fizycznej 109
e. Dane anonimowe 113
f. Dane zwykłe i szczególne kategorie danych 114
C. Przetwarzanie 117
a. Znaczenie pojęcia 117
b. Katalog przykładowych operacji na danych osobowych 119
D. Profilowanie 121
a. Znaczenie pojęcia 121
b. Zautomatyzowane przetwarzanie 123
c. Ocena czynników człowieka 124
d. Profilowanie a podejmowanie zautomatyzowanych decyzji 126
E. Administrator 127
a. Znaczenie pojęcia 127
b. Osoba fizyczna, prawna, organ publiczny 129
c. Ustalanie celów i sposobów przetwarzania 130

d. Samodzielne lub wspólne podejmowanie decyzji ... 132
e. Sytuacja szczególna ... 133
F. Podmiot przetwarzający ... 134
a. Znaczenie pojęcia ... 134
b. Osoba fizyczna, osoba prawna, organ publiczny ... 135
c. Przetwarzanie w imieniu administratora ... 136
d. Podstawa prawna powierzenia ... 137
e. Zagadnienia szczególne ... 138
G. Odbiorca ... 139
a. Znaczenie pojęcia ... 139
b. Osoba fizyczna, osoba prawna, organ publiczny ... 141
c. Ujawnianie danych osobowych ... 143
H. Osoba, której dane dotyczą (podmiot danych) ... 144
I. Przedsiębiorca ... 145
a. Znaczenie pojęcia ... 145
b. Rozbieżności pomiędzy wersjami językowymi RODO ... 146
c. Osoba fizyczna, osoba prawna, spółki osobowe i zrzeszenia ... 147
d. Prowadzenie działalności gospodarczej ... 148
e. Wymóg regularności ... 149
J. Grupa przedsiębiorstw ... 150
a. Znaczenie pojęcia ... 150
b. Sprawowanie kontroli ... 151
c. Ważna rola zasady rozliczalności ... 152
K. Usługa społeczeństwa informacyjnego ... 153
a. Znaczenie pojęcia ... 153
b. Odpłatność ... 154
c. Świadczenie na odległość ... 155
d. Świadczenie drogą elektroniczną ... 156
e. Świadczenie na indywidualne żądanie ... 157
L. Podejście oparte na ryzyku ... 158
a. Znaczenie pojęcia ... 158
b. Pojęcie ryzyka ... 159
c. Szacowanie i analiza ryzyka ... 162
d. Obowiązki oparte na analizie ryzyka ... 167
e. Uwzględnienie praw i wolności podmiotów danych ... 168
M. Naruszenie ochrony danych osobowych ... 169
a. Pojęcie naruszenia ochrony danych osobowych ... 169
b. Znaczenie pojęcia ... 170
c. Przesłanki determinujące zaistnienie naruszenia ... 171
d. Kategorie skutków naruszenia bezpieczeństwa ... 173
e. Przesłanka danych osobowych ... 177
N. Organ nadzorczy ... 178
a. Znaczenie pojęcia ... 178
b. Niezależność ... 179
c. Wymogi powołania na stanowisko Prezesa UODO ... 181
d. Właściwość ... 182

4. Zasady dotyczące przetwarzania danych osobowych ... 183

A. Wprowadzenie ... 183
B. Zasada zgodności z prawem i rzetelności ... 185
C. Zasada przejrzystości ... 190
D. Zasada ograniczenia celu ... 195
E. Zasada minimalizacji danych ... 200
F. Zasada prawidłowości ... 205
G. Zasada ograniczenia przechowywania ... 207
H. Zasada integralności i poufności ... 213
I. Zasada rozliczalności ... 218

5. Przesłanki legalizacyjne przetwarzania danych osobowych ... 222

A. Wprowadzenie ... 222
B. Zgoda ... 224
a. Istota przesłanki ... 224
b. Dobrowolność zgody ... 225
c. Konkretność zgody ... 226
d. Świadomość zgody ... 227
e. Jednoznaczność zgody ... 228
f. Wyraźność zgody ... 229
g. Forma zgody ... 230
h. Dodatkowe wymogi dotyczące pisemnej zgody ... 231
i. Wycofanie zgody ... 232
j. Zgoda dziecka ... 233
C. Niezbędność do wykonania umowy lub podjęcia działań przed zawarciem umowy ... 234
a. Istota przesłanek ... 234
b. Działania przed zawarciem umowy ... 237
c. Żądanie podmiotu danych ... 238
d. Niezbędność przetwarzania dla podjęcia działań przed zawarciem umowy ... 239
e. Istnienie umowy ... 240
f. Strona umowy ... 241
g. Wykonanie umowy ... 242

h. Niezbędność przetwarzania dla wykonania umowy ... 244
D. Niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze ... 245
a. Istota przesłanki ... 245
b. Obowiązek prawny ... 247
c. Niezbędność przetwarzania dla realizacji obowiązku ... 248
E. Niezbędność przetwarzania do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej ... 249
a. Istota przesłanki ... 249
b. Żywotne interesy ... 251
c. Niezbędność przetwarzania ... 253
F. Niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi ... 254
a. Istota przesłanki ... 254
b. Dwie sytuacje ... 256
G. Niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią ... 258
a. Istota przesłanki ... 258
b. Zakres podmiotowy ... 259
c. Proces stosowania ... 260
d. Prawnie uzasadniony interes ... 261
e. Niezbędność przetwarzania ... 263
f. Interesy, podstawowe prawa i wolności podmiotu danych ... 264
g. Test równowagi ... 266
h. Zasada rozliczalności ... 268
H. Przetwarzanie szczególnych kategorii danych osobowych ... 269
a. Zakaz przetwarzania szczególnych kategorii danych osobowych ... 269
b. Wyjątki od zakazu przetwarzania szczególnych kategorii danych osobowych ... 270

6. Prawa osób, których dane dotyczą ... 281

A. Wprowadzenie ... 281
a. Zagadnienia ogólne ... 281
b. Przejrzyste informowanie i przejrzysta komunikacja ... 283
B. Prawa informacyjne ... 288
a. Zagadnienia ogólne ... 288
b. Typy obowiązków informacyjnych ... 289
c. Zakres obowiązków informacyjnych ... 292
d. Sposób realizacji obowiązków informacyjnych ... 293
e. Termin realizacji obowiązków informacyjnych ... 297
f. Zmiana celu przetwarzania ... 298
g. Aktualizacja informacji ... 299
h. Wyłączenia z zakresu obowiązku informacyjnego ... 302
C. Realizacja żądań podmiotów danych – zagadnienia ogólne ... 307
a. Prawa wymagające inicjatywy podmiotu danych ... 307
b. Adresat żądania ... 310
c. Identyfikacja podmiotu danych ... 313
d. Forma żądania podmiotu danych ... 319
e. Sposób i termin realizacji żądania podmiotu danych ... 322
f. Koszty realizacji praw podmiotów danych ... 326
g. Realizacja żądań przez przedstawiciela ustawowego lub pełnomocnika ... 328
h. Obowiązek powiadamiania odbiorców danych osobowych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych osobowych ... 332
D. Prawo dostępu ... 335
a. Zagadnienia ogólne i zakres prawa dostępu ... 335
b. Przesłanki ... 340
c. Sposób realizacji żądania ... 344
d. Wyłączenia ... 353
e. Sankcje ... 356
E. Prawo do sprostowania ... 357
a. Zagadnienia ogólne ... 357
b. Przesłanki ... 358
c. Sposób realizacji żądania ... 361
d. Wyłączenia ... 365
e. Sankcje ... 366
F. Prawo do usunięcia danych (prawo do bycia zapomnianym) ... 367
a. Zagadnienia ogólne ... 367
b. Przesłanki ... 372
c. Sposób realizacji żądania ... 379
d. Wyłączenia ... 384
e. Sankcje ... 386

G. Prawo do ograniczenia przetwarzania ... 387
a. Zagadnienia ogólne ... 387
b. Przesłanki ... 393
c. Sposób realizacji żądania ... 396
d. Wyłączenia ... 399
e. Sankcje ... 400
H. Prawo do przenoszenia danych ... 401
a. Zagadnienia ogólne ... 401
b. Przesłanki ... 408
c. Sposób realizacji żądania ... 415
d. Wyłączenia ... 420
e. Sankcje ... 421
I. Prawo sprzeciwu ... 422
a. Zagadnienia ogólne ... 422
b. Przesłanki ... 426
c. Sposób realizacji żądania ... 439
d. Wyłączenia ... 444
e. Sankcje ... 446
J. Zautomatyzowane podejmowanie decyzji ... 447
a. Zagadnienia ogólne ... 447
b. Zautomatyzowane przetwarzanie ... 449
c. Skutki prawne ... 452
d. Oddziaływanie w podobny sposób do skutku prawnego ... 454
e. Wyjątki od zakazu podejmowania zautomatyzowanych decyzji ... 456
f. Gwarancje ... 460

7. Obowiązki administratora i podmiotu przetwarzającego ... 461

A. Wprowadzenie ... 461
B. Obowiązek zapewnienia zgodności ... 468
C. *Data Protection by Design* ... 476
a. Zagadnienia ogólne ... 476
b. Elementy koncepcji *privacy by design* ... 487
Podejście proaktywne, a nie reaktywne i zaradcze, nie naprawcze ... 488
Prywatność jako ustawienie domyślne (*privacy by default*) ... 489
Prywatność włączona w projekt ... 490
Pełna funkcjonalność rozumiana jako osiąganie sumy dodatniej, a nie sumy zerowej ... 491
Ochrona prywatności od początku do końca cyklu życia informacji ... 492
Transparentność i przejrzystość ... 493
Poszanowanie dla prywatności użytkowników ... 494
c. Wytyczne Europejskiej Rady Ochrony Danych ... 495
d. Sposób realizacji wymogu *data protection by design* ... 496
e. Sankcje ... 499
D. Obowiązki dokumentacyjne ... 500
a. Zagadnienia ogólne ... 500
b. Rejestr czynności przetwarzania ... 504
c. Rejestr kategorii czynności przetwarzania ... 511
d. Dokumentacja analizy ryzyka ... 513
e. Dokumentacja oceny skutków dla ochrony danych ... 517
f. Dokumentacja uprzednich konsultacji ... 521
g. Dokumentacja transferów danych do państw trzecich ... 523
h. Dokumentacja naruszeń ochrony danych oraz notyfikacja naruszeń ... 526
i. Dokumentacja realizacji praw podmiotów danych ... 534
j. Dokumentacja dopuszczenia do przetwarzania i upoważnień ... 540
k. Dokumentacja powierzeń i poleceń ... 544
l. Polityka retencyjna ... 553
m. Dokumentacja spełnienia przesłanek legalizacyjnych ... 557
n. Polityki ochrony danych ... 561
E. Bezpieczeństwo przetwarzania ... 562
a. Zagadnienia ogólne ... 562
b. Definicja bezpieczeństwa przetwarzania danych osobowych ... 569
c. Ryzyko naruszenia praw lub wolności ... 574
d. Zagrożenia naruszenia praw lub wolności ... 576
e. Prawdopodobieństwo wystąpienia zagrożenia ... 583
f. Waga wpływu ... 586
g. Poziom ryzyka ... 589
h. Środki organizacyjne zapewnienia bezpieczeństwa przetwarzania ... 591
i. Środki techniczne zapewnienia bezpieczeństwa przetwarzania ... 597
j. Dobór odpowiednich środków ... 604
k. Stan wiedzy technicznej ... 611
l. Przetwarzanie danych do celów zapewnienia bezpieczeństwa ... 614
F. Ocena skutków dla ochrony danych i uprzednie konsultacje ... 616
a. Zagadnienia ogólne ... 616

b. Przypadki obligatoryjnej oceny skutków dla ochrony danych ... 620
c. Elementy i etapy oceny skutków dla ochrony danych ... 627
d. Uprzednie konsultacje z organem nadzorczym ... 632
e. Sankcje ... 641
G. Zgłoszenia naruszeń ochrony danych osobowych ... 642
a. Zagadnienia ogólne ... 642
b. Stwierdzenie i ewidencjonowanie naruszenia ochrony danych osobowych ... 645
c. Zgłaszanie naruszenia organowi nadzorczemu ... 656
d. Zawiadamianie podmiotów danych o naruszeniach ochrony danych osobowych ... 665
e. Ocena prawdopodobieństwa i wagi naruszenia ochrony danych osobowych ... 669

8. **Współadministrowanie danymi osobowymi** ... 674
A. Regulacja współadministrowania w dyrektywie 95/46 i ustawie o ochronie danych osobowych z 1997 r. ... 674
B. Definicja współadministrowania ... 676
C. Współadministrowanie w orzecznictwie TS ... 680
D. Uzgodnienia pomiędzy współadministratorami ... 687
E. Realizacja praw podmiotów danych wobec współadministratorów ... 699
F. Współadministrowanie w polskim prawie ... 700
G. Odpowiedzialność współadministratorów ... 707

9. **Powierzenie przetwarzania** ... 709
A. Wprowadzenie ... 709
B. Pojęcie powierzenia przetwarzania i podmiotu przetwarzającego ... 710
C. Kryteria wyboru podmiotu przetwarzającego ... 713
D. Umowa powierzenia przetwarzania danych osobowych ... 717
E. Dalsze powierzenie przetwarzania ... 728
F. Odpowiedzialność podmiotu przetwarzającego ... 733

10. **Inspektor ochrony danych** ... 737
A. Wprowadzenie ... 737
B. Wyznaczenie inspektora ochrony danych ... 739
C. Kwalifikacje inspektora ochrony danych ... 747
D. Status inspektora ochrony danych ... 751
E. Zadania inspektora ochrony danych ... 761

11. **Kodeksy postępowania i certyfikacja** ... 765
A. Kodeksy postępowania ... 765
a. Instytucja kodeksów postępowania ... 765
b. Definicja pojęcia kodeksu postępowania ... 766
c. Stosowanie kodeksów postępowania ... 767
d. Zakres podmiotowy ... 768
e. Zakres przedmiotowy ... 769
f. Zatwierdzanie i monitorowanie kodeksów ... 770
B. Certyfikacja ... 771
a. Funkcja mechanizmu certyfikacji ... 771
b. Definicja certyfikacji ... 772
c. Zasady certyfikacji ... 773
d. Mechanizm certyfikacji ... 774
e. Zakres podmiotowy i przedmiotowy certyfikacji ... 775
f. Warunki i tryb uzyskiwania certyfikacji ... 776

12. **Przekazywanie danych osobowych do państw trzecich i organizacji międzynarodowych** ... 777
A. Wprowadzenie ... 777
a. Zagadnienia ogólne ... 777
b. Przekazanie jako operacja przetwarzania danych osobowych ... 779
c. Pojęcie państwa trzeciego ... 780
d. Pojęcie przekazywania (transferu) danych do państwa trzeciego ... 781
e. Importer oraz eksporter danych ... 782
f. Dalsze przekazywanie danych osobowych ... 783
g. Obowiązek informacyjny ... 784
B. Decyzje w sprawie adekwatności ... 785
a. Rola decyzji Komisji w sprawie adekwatności ... 785

b. Decyzje sektorowe oraz dotyczące terytorium ... 786
c. Rezygnacja ze „specjalnych zezwoleń" ... 787
d. Decyzje o charakterze negatywnym ... 788
e. Przyjęte dotychczas oraz planowane decyzje Komisji. Zjednoczone Królestwo państwem trzecim ... 789
C. Przekazywanie danych z wykorzystaniem odpowiednich zabezpieczeń ... 792
a. Instrumenty stanowiące „odpowiednie zabezpieczenia" ... 792
b. Zatwierdzone kodeksy postępowania ... 793
c. Zatwierdzone mechanizmy certyfikacyjne ... 794
d. Instrumenty przeznaczone dla podmiotów publicznych ... 795
e. Klauzule umowne *ad hoc* ... 796
D. Standardowe klauzule ochrony danych ... 797
a. Klauzule standardowe i ich rodzaje ... 797
b. Nowe klauzule standardowe Komisji ... 798
c. Stosowanie klauzul standardowych w praktyce ... 799
d. Stosowanie klauzul standardowych po wyroku C-311/18, Schrems II ... 800
E. Wiążące reguły korporacyjne ... 801
a. Definicja i główne cechy wiążących reguł korporacyjnych ... 801
b. Elementy definicyjne BCR ... 802
c. Wiążące reguły dla podmiotów przetwarzających ... 803
d. Szczegółowe wymogi stawiane wiążącym regułom korporacyjnym ... 804
e. Zatwierdzenie wiążących reguł korporacyjnych ... 805
f. Dokumenty Grupy Roboczej ... 806
F. Wyjątki w szczególnych sytuacjach ... 807
a. Katalog wyjątków ... 807
b. Wyraźna zgoda podmiotu danych ... 808
c. Umowa zawarta z podmiotem danych lub w jego interesie ... 809
d. Interes publiczny ... 810
e. Ustalanie, dochodzenie lub ochrona roszczeń ... 811
f. Żywotne interesy podmiotów danych ... 812
g. Przekazanie danych z rejestru publicznego ... 813
h. Klauzula prawnie uzasadnionych interesów eksportera danych ... 814

13. **Organ nadzorczy** ... 815
A. Powołanie i status ... 815
a. Zasady powoływania organu ... 815
b. Wymogi dotyczące osób pełniących funkcję organu nadzorczego ... 821
c. Tajemnica służbowa ... 827
d. Zakończenie kadencji osób pełniących funkcję organu nadzorczego ... 829
e. Niezależność organu nadzorczego ... 834
B. Zadania i uprawnienia organu nadzorczego ... 849
a. Zadania organu nadzorczego ... 849
b. Uprawnienia organu nadzorczego ... 852
c. Obowiązki organu nadzorczego ... 853

14. **Współpraca i spójność** ... 856
A. Wprowadzenie ... 856
B. Współpraca między organami nadzorczymi ... 858
a. Współpraca między wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy ... 858
b. Możliwość zwrócenia się do innych organów nadzorczych o udzielenie wzajemnej pomocy ... 862
c. Wspólne operacje organów nadzorczych ... 863
d. Mechanizm spójności ... 864
e. Tryb pilny ... 868

15. **Europejska Rada Ochrony Danych** ... 869
A. Wprowadzenie ... 869
B. Skład Europejskiej Rady Ochrony Danych ... 871
a. Członkowie ... 871
b. Przewodniczący ... 872
C. Zadania ... 873
D. Sekretariat Europejskiej Rady Ochrony Danych ... 880

16. **Środki ochrony prawnej** ... 883
A. Prawo do skargi do organu nadzorczego ... 883
a. Zasady składania skargi do organu nadzorczego ... 884
b. Prawo do skargi – zakres podmiotowy ... 886
c. Właściwość miejscowa organu, do którego wnoszona jest skarga ... 887

B. Prawo do odszkodowania 889
a. Wstęp 889
b. Prawo materialne a przepisy proceduralne 893
c. Struktura zobowiązania odszkodowawczego z art. 82 ust. 1 RODO 895
Wierzyciel 895
Dłużnik 897
Roszczenie 898
C. Administracyjne kary pieniężne 899
a. Zakres podmiotowy kompetencji organu do stosowania sankcji pieniężnej 900
b. Zasady stosowania administracyjnej kary pieniężnej 901
c. Wysokość nakładanych kar 902
d. Kryteria wymiaru administracyjnej kary pieniężnej 905
17. **Podsumowanie** 906

1. Wprowadzenie

Dominik Lubasz

Podstawa prawna: rozporządzenie 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

66 Rozporządzenie 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) weszło w życie 24.05.2016 r. i po dwuletnim okresie przygotowawczym, mającym pozwolić podmiotom zobowiązanym na wdrożenie wymaganych nim rozwiązań, a państwom członkowskim na podjęcie działań legislacyjnych zapewniających możliwości stosowania rozporządzenia, jest stosowane od 25.05.2018 r.
Rozporządzenie wchodzi w skład pakietu reform aktów prawnych dotyczących problematyki ochrony danych osobowych wraz z tzw. **dyrektywą policyjną**, tj. dyrektywą 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW.

67 Rozporządzenie 2016/679 zastąpiło dotychczas obowiązującą dyrektywę 95/46, a w konsekwencji również ustawę o ochronie danych osobowych z 1997 r., wprowadzając odmienny, proaktywny model ochrony, **oparty na podejściu bazującym na ryzyku** (*risk-based approach*). Odchodzi tym samym od sztywnych ram regulacyjnych i wyabstrahowanych od kategorii administratora, zakresu jego działania, zwłaszcza jego związku z przetwarzaniem danych osobowych i skali tego przetwarzania, które były charakterystyczne dla polskiej ustawy o ochronie danych osobowych i rozporządzeń wykonawczych do niej, a zwłaszcza rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

68 Na konieczność zmiany podejścia regulacyjnego do ochrony danych osobowych zwracano uwagę od dłuższego czasu. W szczególności było to motywowane koniecznością unowocześnienia regulacji, zapewnienia jej neutralności technologicznej, zniesienia zbędnych z perspektywy ochrony obciążeń administracyjnych, zniwelowania negatywnych aspektów związanych z dotychczasowym wyborem środka legislacyjnego w postaci dyrektywy o minimalnym charakterze, a wreszcie dostrzeżeniem wartości danych osobowych w gospodarce i wpływu wykorzystania danych, zwłaszcza w aspekcie transgranicznym, w celu budowania jednolitego rynku cyfrowego w UE.

69 Zgodnie z zamierzeniami Komisji rozporządzenie 2016/679 miało zapewnić z jednej strony **wysoki poziom ochrony praw osób fizycznych**, z drugiej jednak poszerzyć możliwości biznesowe poprzez **ułatwienie swobodnego przepływu danych osobowych na jednolitym rynku cyfrowym**. W założeniach nowa regulacja miała być technologicznie neutralna i pozostawiać administratorom danych osobowych swobodę co do wyboru metod i środków, z wykorzystaniem których będą realizować cele i zadania związane z bezpieczeństwem informacji, co stało się ostatecznie jednym z najbardziej charakterystycznych elementów regulacji.

Zmieniono w związku z tym optykę rozwiązań, uelastyczniając podejścia i różnicując nakładane obowiązki zależnie od warunków przetwarzania danych, różnych podmiotów przetwarzających i różnej jego skali.

Warto podkreślić, że jedną ze znaczących zmian był także **wybór środka legislacyjnego w postaci rozporządzenia**, jako aktu prawa europejskiego stosowanego bezpośrednio we wszystkich państwach członkowskich, bez konieczności jego implementacji, jak ma to miejsce w przypadku dyrektyw. Zgodnie bowiem z art. 288 TFUE rozporządzenie ma zasięg ogólny oraz wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich (*direct effect*). Zabieg ten miał na celu usunięcie różnic w poziomie ochrony w poszczególnych państwach członkowskich, a także zapewnienie jednolitości stosowania przy równoczesnym wprowadzeniu innych mających to zagwarantować mechanizmów, jak np. mechanizmu spójności. 70

W celu zapewnienia stosowania rozporządzenia w krajowych porządkach prawnych, mimo bezpośredniego stosowania, konieczna była ingerencja ustawodawcza w poszczególnych państwach członkowskich. Wynika to przede wszystkim z przyjętej w prawie europejskim zasady **autonomii proceduralnej** państw członkowskich. Konieczne było zatem stworzenie na szczeblu krajowym odpowiednich przepisów obejmujących zagadnienia instytucjonalne i proceduralne. 71

> **WAŻNE!** Istotą zasady autonomii proceduralnej jest przyjęcie, że w razie braku regulacji w prawie unijnym państwa członkowskie korzystają ze swobody stanowienia reguł proceduralnych. Swoboda ta jednakże podlega dwóm zasadom ograniczającym, tj.:
> – zasadzie równoważności (*principle of equivalence*) oraz
> – zasadzie skuteczności (*principle of effectivness*).

Zgodnie z pierwszą z nich prawo krajowe nie może regulować uprawnień wynikających z prawa unijnego w sposób mniej korzystny niż wynikający z prawa krajowego. Druga natomiast przesądza, że procedura ustanowiona w prawie krajowym nie może prowadzić do uniemożliwienia lub znacznego utrudnienia (*excessively difficult*) realizowania praw przyznanych w prawie unijnym. W tym kontekście autonomia proceduralna podlega ograniczeniom i przepisy procedury mogą być objęte kognicją Trybunału Sprawiedliwości, zwłaszcza w sytuacji naruszania przez nie drugiej ze wskazanych zasad. Zwrócił na to uwagę Trybunał Sprawiedliwości w wyroku z 6.10.1981 r., C-246/80, Broekmeulen v. Huisarts Registratie Commissie, EU:C:1981:218. Na temat przepisów podlegających ocenie przez pryzmat zasady autonomii proceduralnej i jej ograniczeń, zwłaszcza zasady efektywności, zob. dodatkowo wyrok TS z 5.03.1996 r., C-46/93 i C-48/93, Brasserie du Pêcheur SA v. Bundesrepublik Deutschland i The Queen v. Secretary of State for Transport, EU:C:1996:79 [na temat autonomii proceduralnej zob. A. Wróbel, *Autonomia proceduralna państw członkowskich. Zasada efektywności i zasada efektywnej ochrony sądowej w prawie Unii Europejskiej*, RPEiS 2005/1, s. 35 i n.; D. Miąsik, *Zasada efektywności prawa wspólnotowego* [w:] *Stosowanie prawa Unii Europejskiej przez sądy*, red. A. Wróbel, Kraków 2005, s. 315–316; K. Kowalik-Bańczyk, *Procedural Autonomy of Member States and the EU Rights of Defence in Antitrust Proceedings,* „Yearbook of Antitrust and Regulatory Studies" 2012/5, s. 218 i n.; A. Kołyszko, P. Dyrberg, *Zasada autonomii proceduralnej w prawie Unii Europejskiej i jej ograniczenia w praktyce*, „Temidium" 2014/4, s. 57 i n.; zob. również D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 31, nt 7].

Państwa członkowskie zostały upoważnione jednak również do przyjmowania środków prawa krajowego w zakresie wprost wskazanym w RODO, tj. w przypadkach, do których rozporządzenie nie znajduje zastosowania (art. 2 ust. 2), oraz w przypadkach określonych w **klau-** 72

zulach kompetencyjnych, np. art. 6 ust. 2, art. 9 ust. 4, art. 23, 43, 84–91. Na możliwość doregulowywania niektórych zagadnień przez państwa członkowskie wskazano także w motywie 10 RODO, w którym prawodawca unijny podkreślił, że państwa członkowskie powinny móc zachować lub wprowadzić krajowe przepisy doprecyzowujące stosowanie przepisów rozporządzenia, w zakresie dotyczącym przetwarzania danych osobowych w celu wypełnienia obowiązku prawnego, w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, w tym uregulowania sektorowe, a także zachowują prawo do doprecyzowania przepisów w odniesieniu m.in. do przetwarzania szczególnych kategorii danych osobowych. Warunkiem prawidłowości regulacji krajowych jest jednak to, by przepisy wydawane na tych podstawach mieściły się w ich ramach, a ponadto by ingerencja ustawodawcy krajowego odbywała się w duchu zasad przyjętych w rozporządzeniu i zgodnie z nimi, co zatem niekoniecznie musi wpływać negatywnie *per se* na stopień harmonizacji.

73 Istotnym elementem wprowadzonych przez RODO zmian regulacyjnych jest nastawienie na unowocześnienie i **urealnienie technologiczne przepisów**. Jak podkreślono bowiem w motywie 6 RODO, szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne dysponują narzędziami pozwalającymi na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Udostępnianie danych ma charakter globalny, również bowiem narzędzia umożliwiające przetwarzanie mają taki charakter.

74 Dostrzeżono również, że to właśnie technologia zmieniła gospodarkę i życie społeczne i że powinna ona nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, jednocześnie jednak dzięki technologii właśnie powinno się zapewniać wysoki stopień ochrony danych osobowych. Uwzględniając postęp technologiczny, zrealizowano równocześnie postulat **technologicznej neutralności regulacji**. Jak podkreślono w motywie 15, ochrona danych osób fizycznych nie powinna zależeć od stosowanych technik, ponieważ w przeciwnym razie wystąpiłoby poważne ryzyko obchodzenia prawa. Założenie to w istotny sposób wpływa na zakres obowiązków podmiotów zobowiązanych do odpowiedniego zabezpieczenia danych osobowych, także już na etapie projektowania rozwiązań służących do ich przetwarzania.

75 W koncepcji regulacyjnej rozporządzenia, jak już wspomniano, centralną rolę odgrywa **ocena ryzyka** i dokonywany na jej podstawie przez administratora dobór środków technicznych i organizacyjnych mających na celu zapewnienie zgodności z rozporządzeniem. Ocena ta ma uwzględniać z jednej strony naturę, zakres, kontekst i cel przetwarzania danych, a z drugiej – wynikające z tego ryzyka dla praw i wolności podmiotów danych. **Kluczowa jest zatem perspektywa podmiotu danych, a nie samego administratora**, o czym należy pamiętać, projektując adekwatne z punktu widzenia rozporządzenia rozwiązania.

76 Warto również zwrócić uwagę, że zgodna z RODO ochrona praw i wolności podmiotów danych w zakresie przetwarzania ich danych osobowych wymaga podjęcia odpowiednich środków nie tylko przy projektowaniu rozwiązań wymagających przetwarzania danych osobowych, lecz także podczas całego procesu przetwarzania, aż do jego zakończenia. Jest to odzwierciedleniem woli zapewnienia wysokiego standardu ochrony w toku całego życia informacji o charakterze osobowym. Jak podkreśla się bowiem w motywie 78 RODO, by zapewnić i wykazać zgodność z rozporządzeniem, administrator powinien w szczególności przyjąć wewnętrzne polityki i wdrożyć odpowiednie środki, które są zgodne m.in. z zasadą uwzględnienia **ochrony danych już w fazie projektowania** (*data protection by design*) **oraz zasadą domyślnej ochrony danych** (*data protection by default*).

77 Zakres i rozkład **obowiązków administratorów i podmiotów przetwarzających** skonstruowane zostały w rozporządzeniu z jednej strony z uwzględnieniem ochrony praw i wolności podmiotów danych, a z drugiej – kompetencji przyznawanych organom nadzorczym i środków przez nie stosowanych. W tym kontekście do podstawowych obowiązków administratora lub podmiotu przetwarzającego należy dokumentowanie operacji przetwarzania, który to obowiązek koreluje z uprawnieniami kontrolnymi organu nadzorczego, w tym w zakresie żądania udostępniania dokumentacji, tak by mogła ona służyć do monitorowania operacji przetwarzania.

78 Równocześnie wspominana elastyczność stosowanych środków ochrony danych zależnych od dokonywanej przez administratora oceny ryzyka związanego z przetwarzaniem danych w pewnym zakresie kompensowana jest nowym **obowiązkiem notyfikacyjnym w przypadku naruszenia ochrony danych osobowych**. Kolejnym nowym obowiązkiem nakładanym na administratora jest obowiązek dokonywania **oceny skutków dla ochrony danych** (*data protection impact assessment*). W szczególności jest ona niezbędna, jeśli operacje przetwarzania stwarzają konkretne prawdopodobieństwo i konkretną wagę danego zagrożenia, z uwzględnieniem charakteru, zakresu, kontekstu i celów oraz źródła zagrożenia. Ocena powinna obejmować w szczególności planowane środki, gwarancje i mechanizmy mające minimalizować zagrożenie. Z obowiązkiem dotyczącym oceny ryzyk i ich skutków dla ochrony danych osobowych związane jest też kolejne nowe zobowiązanie do przeprowadzenia **uprzedniej konsultacji** z organem nadzorczym przed przetwarzaniem danych osobowych, by zapewnić zgodność planowanego przetwarzania z rozporządzeniem, w szczególności w takim przypadku, gdy ocena ryzyka prowadzi do wniosku, że przetwarzanie danych może powodować istotne zagrożenia dla praw i wolności podmiotów danych, a ryzyko to nie zostało zminimalizowane.

79 W rozporządzeniu wprowadzono ponadto przesłanki obligatoryjnego powołania **inspektora ochrony danych**, zastępującego fakultatywną instytucję administratora bezpieczeństwa informacji. Rozstrzygnięta została także pozycja ustrojowa inspektora, jego status i obowiązki.

80 W stosunku do dotychczasowej regulacji zmianie ulegają nie tylko obowiązki administratorów, lecz także **prawa podmiotów danych**, które stanowią jeden z filarów nowego systemu ochrony danych. Poświęcono im regulację rozdziału III, kładąc nacisk na przejrzystość komunikacji i ułatwienie przez administratorów wykonywania prawa przez osoby, których dane dotyczą. Prawa ujęto w dwie grupy przepisów – pierwszą, dotyczącą obowiązków informacyjnych administratora, i drugą, dotyczącą uprawnień podmiotu danych, wśród których można wymienić prawo dostępu do danych oraz prawo do poprawiania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, do sprzeciwu oraz do niepodlegania decyzjom podejmowanym w indywidualnych przypadkach w sposób zautomatyzowany.

81 Kluczowe dla zgodnego z rozporządzeniem wykonania obowiązków, jak i zapewnienia prawidłowej realizacji praw podmiotów danych jest uwzględnienie sformułowanych w art. 5 **podstawowych zasad przetwarzania danych**. Determinują one bowiem zakres i sposób realizacji obowiązków informacyjnych, związanych z transparentnością procesów przetwarzania, ocenę legalności przetwarzania, czy też wreszcie bezpieczeństwo. Część zasad przetwarzania była już znana na gruncie dyrektywy 95/46, jednakże ich katalog ulega istotnemu rozszerzeniu, co ma być wyrazem woli zapewnienia jak najpełniejszej realizacji celów rozporządzenia, w szczególności osiągnięcia wysokiego poziomu ochrony praw osób fizycznych, zwłaszcza w zakresie ochrony ich danych osobowych oraz autonomii informacyjnej, kładąc w konsekwencji wyraźny nacisk na przejrzystość i jasność procesów związanych z przetwarzaniem danych oraz na minimalizację, a zatem zapewnienie możliwie najmniejszej ingerencji w prawa podstawowe jednostek.

82 W rozporządzeniu 2016/679 na nowo zostają ukształtowane także **przesłanki przetwarzania danych osobowych**. Zachowany zostaje wprawdzie znany z dotychczasowych przepisów podział na przesłanki przetwarzania danych osobowych zwykłych i danych osobowych szczególnych kategorii, tj. ogólnego dopuszczenia przetwarzania danych zwykłych, gdy spełniona jest co najmniej jedna z przesłanek z art. 6 ust. 1, oraz ogólnego zakazu przetwarzania danych wrażliwych, chyba że zachodzi którykolwiek z wyjątków pozwalających na takie przetwarzanie wskazanych w art. 9 ust. 2, jednakże zakresy poszczególnych przesłanek ulegają modyfikacji. Istotnie zmieniona zostaje przesłanka zgody, w szczególności poprzez dopuszczenie zgody konkludentnej, a także wprowadzenie zgody dziecka. Rozszerzony zostaje także m.in. zakres zastosowania przesłanki prawnie uzasadnionego interesu administratora.

83 Warto zwrócić uwagę, że rozpatrywanie szczegółowych przepisów rozporządzenia, zarówno nakładających obowiązki, jak i przyznających prawa, dokonywane być musi w świetle **przedmiotu i celu rozporządzenia** uregulowanego w art. 1. Zgodnie z tym przepisem z jednej strony celem rozporządzenia jest ochrona praw i wolności osób fizycznych w związku z przetwarzaniem ich danych, a nie ochrona danych osobowych *per se*, z drugiej zaś równorzędnym celem jest nieograniczanie ani niezakazywanie swobodnego przepływu danych osobowych w ramach Unii.
Taka konstelacja celów wynika z woli zbalansowania konieczności zapewnienia ochrony jednostkom i rozwoju jednolitego rynku cyfrowego w Europie. Należy podkreślić, że kwalifikacja ochrony osób fizycznych w związku z przetwarzaniem danych osobowych jako prawa podstawowego wynika wprost z art. 8 ust. 1 KPP UE oraz z art. 16 ust. 1 TFUE, stanowiących, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących, co przesądza o randze i wykładni omawianych przepisów (motyw 1 RODO). W art. 1 ust. 2 stwierdzono, że RODO ma służyć ochronie w szczególności tego prawa podstawowego, konkretyzując w zakresie swojej regulacji prawa wynikające z prawa pierwotnego. Ponadto w motywie 2 RODO wskazano, że zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą, i to niezależnie od obywatelstwa czy miejsca zamieszkania takich osób, być w kolizji z ich podstawowymi prawami i wolnościami, w szczególności prawem do ochrony danych osobowych. W motywie 4 RODO z kolei podkreślono, że prawo do ochrony danych osobowych **nie jest prawem bezwzględnym**. W konsekwencji należy je postrzegać przez pryzmat jego funkcji społecznej i ważyć względem innych praw podstawowych, stosując zasadę proporcjonalności. W takiej relacji zatem pozostawać ma rozporządzenie i jego stosowanie do pozostałych praw podstawowych, wolności i zasad uznanych w Karcie Praw Podstawowych i traktatach i wywodzących się z tradycji konstytucyjnych państw członkowskich.

> ***WAŻNE!*** Regulacja rozporządzenia ma także służyć realizacji celu natury generalnej. Ma bowiem przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, a także do postępu społeczno-gospodarczego oraz do wzmacniania i konwergencji gospodarek na rynku wewnętrznym (motyw 2 RODO).

84 **Sformułowane cele** w postaci ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu danych osobowych, jako jednego z elementów istotnych z punktu widzenia urzeczywistniania rynku wewnętrznego, należy rozpatrywać jako cele równorzędne i współzależne. **Jest to istotne z punktu widzenia wykładni przepisów rozporządzenia i zostało uwypuklone w jego motywach** (motywy 2, 7, 9, 10, 13 RODO).

2. Zakres zastosowania ogólnego rozporządzenia o ochronie danych

Dominik Lubasz

Podstawa prawna: art. 2 i 3 RODO.

Zakres zastosowania ogólnego rozporządzenia o ochronie danych osobowych wyznaczają art. 2 i 3 RODO. Odpowiednio dotyczą one problematyki zakresu przedmiotowego, czyli wskazują rodzaj przetwarzania danych osobowych podlegających regulacji, oraz zakresu terytorialnego zastosowania, tj. wyznaczają terytorium i podmioty, do których przepisy rozporządzenia mają zastosowanie. 85

A. Zakres przedmiotowy

Zgodnie z art. 2 RODO rozporządzenie znajduje zastosowanie do wszelkiego rodzaju przetwarzania danych osobowych stanowiących lub mających stanowić część zbioru danych, niezależnie od sposobu przetwarzania, a zatem tego, czy przetwarzanie następuje w sposób całkowicie lub tylko częściowo zautomatyzowany, czy też w sposób w ogóle niezautomatyzowany. 86

WAŻNE! Rozstrzygające dla wykładni zakresu przedmiotowego są przede wszystkim pojęcia danych osobowych (art. 4 pkt 1 RODO), przetwarzania (art. 4 pkt 2 RODO) oraz zbioru danych (art. 4 pkt 6 RODO).

Dla objęcia materialnym zakresem zastosowania RODO istotne znaczenie ma rozróżnienie procesów przetwarzania danych osobowych: 87

1) **zautomatyzowanego lub częściowo zautomatyzowanego** bez związku z tym, czy dane w ten sposób przetwarzane staną się lub mają (mogą) się stać częścią zbioru;
2) **innych niż zautomatyzowane**, lecz jedynie wówczas, gdy dane w ten sposób przetwarzane stanowią część zbioru danych lub mają (mogą) stanowić część zbioru danych.

Pojęcie **przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany** nie zostało zdefiniowane w rozporządzeniu, co jest wyrazem woli zachowania neutralności technologicznej regulacji. Pojęcia te należy jednak wykładać szeroko, co powoduje, że rozporządzeniem objęte będą nie tylko przetwarzanie w systemach teleinformatycznych, lecz także inne sposoby automatycznego przetwarzania na innych urządzeniach, np. wideorejestratorach samochodowych, bodycam czy kamerach na dronach, utrwalających zapis, z zastrzeżeniem wyłączeń zawartych w art. 2 ust. 2 RODO. 88

PRZYKŁAD: Nadzór polegający na rejestracji obrazu osób, przechowywanego na sprzęcie nagrywającym w sposób ciągły, a mianowicie na twardym dysku, zautomatyzowane przetwarzanie danych osobowych (wyrok TS z 11.12.2014 r., C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, EU:C:2014:2428).

89 **Częściowo zautomatyzowane przetwarzanie danych** tym się różni od całkowicie zautomatyzowanego przetwarzania, że niektóre z etapów przetwarzania mają inny niż zautomatyzowany charakter – np. samo zbieranie danych w sposób niezautomatyzowany, jednakże z przeznaczeniem do późniejszego automatycznego przetwarzania, np. w systemie teleinformatycznym.

> *WAŻNE!* Przez pojęcie częściowego **zautomatyzowanego sposobu przetwarzania danych należy także rozumieć sytuację, w której wprawdzie zestaw danych prowadzony jest w całości w formie analogowej, ale wyposażony zostaje w zautomatyzowany system indeksujący**.

90 **Przetwarzaniem innym niż zautomatyzowane** jest przetwarzanie ręczne, co wynika z semantyki motywu 15 RODO. Na żadnym etapie takiego przetwarzania i przy żadnej operacji przetwarzania nie może dochodzić do zautomatyzowania przetwarzania i nie chodzi tu o ustawienie przetwarzania analogowego w opozycji do cyfrowego czy – szerzej – elektronicznego, ale każdego automatycznego, w tym z wykorzystaniem analogowych mechanizmów automatycznych. Takie formy przetwarzania, by być objęte rozporządzeniem, muszą dotyczyć danych **stanowiących część zbioru danych lub mających stanowić część zbioru danych**.

> *WAŻNE!* Pojęcie zbioru danych zdefiniowane zostało w art. 4 pkt 6 RODO jako uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany, czy rozproszony funkcjonalnie lub geograficznie.

W tym kontekście kluczowe jest rozstrzygnięcie, czy **przeznaczenie lub możliwość włączenia w zbiór należy rozumieć abstrakcyjnie, czy konkretnie**. Należy stanąć na stanowisku, że wystarczające do objęcia regulacją będzie już, jeśli dane jedynie będą mogły znaleźć się w zbiorze danych, bez względu na to, czy się w nim ostatecznie znalazły.

91 W art. 2 ust. 2 RODO sformułowano katalog przypadków, w których **rozporządzenie nie znajdzie zastosowania**.

> *WAŻNE!* Wyłączenia zastosowania RODO:
> a) przetwarzanie w ramach działalności nieobjętej zakresem prawa Unii;
> b) przetwarzanie przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;
> c) przetwarzanie przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;
> d) przetwarzanie przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

92 Wyłączenie zastosowania rozporządzenia obejmujące **przetwarzanie w ramach działalności nieobjętej zakresem prawa Unii** związane jest z jednej strony z podstawą kompetencyj-

ną wydania rozporządzenia, tj. art. 16 ust. 2 TFUE, zgodnie z którym Parlament Europejski i Rada, w zwykłej procedurze ustawodawczej, uprawnione są do określenia zasad dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych, z drugiej zaś – z podziałem kompetencji prawodawczych między Unię a państwa członkowskie na podstawie art. 2–4 i 6 TFUE. W przepisach tych wskazano ogólne kompetencje organów unijnych wyłączne i dzielone z państwami członkowskimi, zakreślając tym samym ogólne podstawy aktywności legislacyjnej organów Unii konkretyzowane poprzez postanowienia Traktatów odnoszące się do każdej dziedziny. To one wyznaczają ramy znaczenia normatywnego art. 2 ust. 1 lit. a RODO.

> *WAŻNE!* Poszukując prawidłowej interpretacji wyłączenia z art. 2 ust. 2 lit. a RODO, można próbować znajdować argumenty w orzecznictwie Trybunału Sprawiedliwości dotyczącym pojęcia dziedzin objętych prawem Unii i jego rozszerzającej wykładni (zob. wyroki: z 27.02.2018 r., C-64/16, Associação Sindical dos Juízes Portugueses v. Tribunal de Contas, EU:C:2018:117, pkt 29–40; z 24.06.2019 r., C-619/18, Komisja Europejska v. Rzeczpospolita Polska, EU:C:2019:531, pkt 47–51, a także z 25.07.2018 r., C-216/18, Minister for Justice and Equality, EU:C:2018:586, pkt 50 i powołane tam orzecznictwo), co prowadziłoby do wniosku, że poza materialnym zakresem zastosowania rozporządzenia mieścić się będą jedynie te działalności, które nie mają łącznika z prawem Unii i nie służą realizacji praw wywodzonych z prawa Unii.

Zagadnienie to było przedmiotem analizy w opinii rzecznika generalnego M. Szpunara w sprawie C-439/19, Latvijas Republikas Saeima (Points de pénalité), EU:C:2020:1054, który wskazał, że prawidłowa wykładnia art. 2 ust. 2 lit. a RODO prowadzi do wniosku, że rozporządzenie 2016/679 ma zastosowanie do przetwarzania danych osobowych w państwie członkowskim lub przez państwo członkowskie, chyba że przetwarzanie to odbywa się w obszarze, w którym Unia Europejska nie ma kompetencji (pkt 63 opinii).
Interpretacji przepisu art. 2 ust. 2 lit. a RODO dokonał również WSA w Warszawie w wyroku z 26.08.2020 r., II SA/Wa 2826/19, LEX nr 3067899, stwierdzając, że wykładnia ww. wyłączenia musi zostać dokonana z uwzględnieniem wykładni systemowej i celowościowej. Intencją ustawodawcy nie było zawężenie stosowania ochrony danych osobowych, a wręcz przeciwnie, zwiększenie jej zakresu i stosowania, co wynika m.in. z art. 16 ust. 1 TFUE, art. 8 ust. 1 KPP UE.

Wyłączenie zastosowania rozporządzenia do przetwarzania przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze wymaga łącznego spełnienia następujących przesłanek: 93

1) przetwarzanie ma być **podejmowane przez osobę fizyczną** oraz
2) przetwarzanie ma następować **w ramach czynności o wyłącznie osobistym lub domowym charakterze**.

W motywie 18 RODO wyjaśniono, że działalność czysto osobista lub domowa to taka, która pozostaje bez związku z działalnością zawodową lub handlową. Polegać ona może na **korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych** oraz **działalności internetowej podejmowanej w ramach takiej działalności.** Rozporządzenie znajdzie jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej, np. sieci społecznościowych.

WAŻNE! Aktualne pozostaje rozstrzygnięcie TS z 6.11.2003 r., C-101/01, Bodil Lindqvist, EU:C:2003:596, w którym Trybunał stwierdził, że wyłączenie to **nie powinno obejmować przypadków przetwarzania danych osobowych polegającego na ich opublikowaniu w Internecie w taki sposób, że staną się one dostępne dla nieograniczonej liczby osób**.
W wyroku z 11.12.2014 r., C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, EU:C:2014:2428, Trybunał podkreślił z kolei, że jeżeli przetwarzanie danych z użyciem przeznaczonych do tego narzędzi **rozciąga się choćby częściowo na przestrzeń publiczną i tym samym jest skierowane poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych**, nie powinno ono być rozumiane jako czynność o czysto „osobistym lub domowym charakterze".

W opinii Grupy Roboczej Art. 29 w sprawie portali społecznościowych, zachowującej walor aktualności również na gruncie RODO, stwierdzono, że co do zasady przetwarzanie danych osobowych przez użytkowników **portali społecznościowych** mieści się w ramach czynności o czysto osobistym lub domowym charakterze, chyba że np. dostęp do danych mają inne osoby niż samodzielnie wybrane przez użytkownika.

WAŻNE! Powyższe poglądy podzielone zostały w orzecznictwie sądów administracyjnych (zob. wyrok WSA w Warszawie z 23.11.2020 r., II SA/Wa 895/20, LEX nr 3157275, w którym stwierdzono, iż „o ile nie ulega wątpliwości, że w motywie 18 Preambuły RODO, jako objętą wyłączeniem, wskazuje się działalność internetową, w tym wykorzystanie sieci społecznościowych, o tyle jednak – zdaniem Sądu – nie należy interpretować tego jako przykład wyłączenia absolutnego, następującego w każdej sytuacji i w przypadku dowolnej aktywności niekomercyjnej użytkownika w Internecie, lecz z zawężeniem do tych stanów faktycznych, w których przetwarzanie danych, w szczególności ich udostępnianie poprzez Internet, nie następuje na rzecz nieograniczonego kręgu odbiorców").

94 Na podstawie art. 2 ust. 2 lit. d RODO nie stosuje się do zagadnień objętych regulacją ustawy o ochronie danych osobowych przetwarzanych w **związku z zapobieganiem i zwalczaniem przestępczości**, którą dokonano transpozycji tzw. dyrektywy policyjnej do krajowego porządku prawnego. Jej przepisy co do zasady weszły w życie 6.02.2019 r. i z tym dniem uchylono obowiązujące na podstawie art. 175 u.o.d.o. przepisy ustawy z 29.08.1997 r. o ochronie danych osobowych.

95 Rozporządzenia nie stosuje się także do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii. W tym zakresie znajduje zastosowanie rozporządzenie **(UE) 2018/1725** z 23.10.2018 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 (Dz.Urz. UE L 295, s. 39)**.

B. Zakres terytorialny

96 Rozporządzenie obejmie swoją regulacją następujące podmioty:
1) przetwarzające dane osobowe **w związku z działalnością prowadzoną przez jednostkę organizacyjną** w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii (art. 3 ust. 1 RODO);

2) niemające jednostek organizacyjnych w Unii, jednak przetwarzające w Unii dane, gdy przetwarzanie to **wiąże się z oferowaniem osobom przebywającym w Unii** towarów lub usług (niezależnie od tego, czy wymagają one zapłaty), a także gdy przetwarzanie wiąże się z **monitorowaniem zachowania osób**, których dane dotyczą, o ile zachowanie to ma miejsce w Unii (art. 3 ust. 2 RODO).

97 Pierwszy z powołanych przypadków objęcia zakresem terytorialnym zastosowania rozporządzenia związany jest z czynnościami przetwarzania przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium Unii Europejskiej.
Zgodnie z powołanym przepisem, by dane przetwarzanie objąć zakresem zastosowania rozporządzenia, musi ono następować w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego, co nie jest jednak równoznaczne z tym, że przetwarzania tego musi dokonywać właśnie ta jednostka organizacyjna.

> *WAŻNE!* **Do tego, aby przepisy RODO znalazły zastosowanie, wystarczy, że istnieje związek między czynnością przetwarzania danych a działalnością danej jednostki organizacyjnej znajdującej się na terytorium Unii Europejskiej.**

98 Regulacja art. 3 ust. 2 RODO stanowi natomiast *novum* w stosunku do przepisów dyrektywy 95/46. Jest ona kluczowa dla administratorów lub podmiotów przetwarzających prowadzących działalność i zlokalizowanych w państwach trzecich, tj. poza Europejskim Obszarem Gospodarczym.
W stosunku do tych podmiotów rozporządzenie będzie miało zastosowanie nie wtedy, gdy usługi tych administratorów będą dostępne w Unii, lecz wyłącznie wówczas, gdy będą oni **nakierowywali swoją działalność na odbiorców w UE**.

> *WAŻNE!* Zgodnie z motywem 23 RODO koncepcja nakierowania wymaga uwzględniania takich czynników, jak „posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii".

99 Dla wykładni regulacji art. 3 RODO kluczowe znaczenie ma pojęcie jednostki organizacyjnej, które jednak nie jest definiowane w rozporządzeniu.

> *WAŻNE!* Pojęcie jednostki organizacyjnej zakłada **skuteczne i faktyczne prowadzenie działalności poprzez stabilne struktury**, niezależnie od tego, czy chodzi o oddział, czy spółkę zależną posiadającą osobowość prawną, a zatem podmiotowość prawna nie jest czynnikiem decydującym przy kwalifikowaniu danej struktury jako „jednostki organizacyjnej" (motyw 22 RODO).
> **Zachowają także aktualność w stosunku do wykładni pojęcia jednostki organizacyjnej rozstrzygnięcia Trybunału Sprawiedliwości:** z 13.05.2014 r., C-131/12, Google Spain i Google Inc. v. Agencia Española de Protección de Datos (AEPD) i Mario Costeja González, EU:C:2014:317; z 1.10.2015 r., C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, EU:C:2015:639, oraz z 28.07.2016 r., C-191/15, Verein für Konsumenteninformation v. Amazon EU Sàrl, EU:C:2016:612.

3. Podstawowe pojęcia

Podstawa prawna: art. 4 RODO.

A. Wprowadzenie

Dominik Lubasz

100 Przepis art. 4 RODO zawiera **definicje pojęć użytych w rozporządzeniu**. Istotna część z nich nie była ujęta w katalogu pojęć zdefiniowanych w dyrektywie 95/46. Inne w większym bądź mniejszym zakresie uległy modyfikacji w stosunku do dotychczasowego stanu prawnego. Nowościami są np. pojęcia:
- ograniczenia przetwarzania (pkt 3),
- profilowania (pkt 4),
- pseudonimizacji (pkt 5),
- naruszenia ochrony danych osobowych (pkt 12),
- danych genetycznych (pkt 13) czy biometrycznych (pkt 14),
- przedstawiciela (pkt 17),
- grupy przedsiębiorstw (pkt 19) oraz
- organizacji międzynarodowej (pkt 26).

Istotnej modyfikacji uległa także definicja zgody (pkt 11). Nadal, co oczywiste, centralną pozycję zajmuje pojęcie danych osobowych (pkt 1).

101 Wiele terminów użytych w RODO nie zostało jednak zdefiniowanych, a zatem ich wykładnia musi być poprzedzana podjęciem zabiegów interpretacyjnych przez podmioty stosujące prawo. Wykładnia ta musi jednak uwzględniać, że mamy do czynienia z unijnym, a nie krajowym aktem prawnym, co ma wpływ na wybór pierwszorzędnej metody wykładni. Dominująca w prawie UE jest wykładnia celowościowa. Zgodnie z nią przepisy muszą być interpretowane w świetle ogólnego celu aktu prawnego, który realizuje. Podkreślone to zostało wyraźnie w wyroku TS z 6.10.1982 r., C-283/81, w którym Trybunał stwierdził, że prawo unijne stosuje właściwą dla siebie terminologię, a użyte pojęcia prawne niekoniecznie muszą posiadać to samo znaczenie w prawie unijnym i w różnych porządkach krajowych. Ponadto każdy przepis prawa unijnego musi być umieszczony w swoim kontekście i interpretowany w świetle prawa unijnego jako całości, biorąc pod uwagę jego cele oraz stan jego ewolucji w momencie, w którym dany przepis ma być stosowany (zob. wyrok TS z 6.10.1982 r., C-283/81, Srl CILFIT i Lanificio di Gavardo SpA v. Ministero della sanità, EU:C:1982:335, pkt 19 i 20. Szerzej na temat **autonomiczności pojęć na gruncie prawa europejskiego** zob. dotyczące tego zagadnienia wyroki TS: z 18.01.1982 r., C-327/82, Ekro BV Vee- en Vleeshandel v. Produktschap voor Vee en Vlees, EU:C:1984:11, pkt 11; z 12.09.2000 r., C-358/97, Komisja v. Irlandia, EU:C:2000:425; z 12.06.2003 r., C-275/01, Sinclair Collis Ltd v. Commissioners of Customs & Excise, EU:C:2003:341, pkt 22; z 18.11.2004 r., C-284/03, Państwo belgijskie v. Temco Europe SA, EU:C:2004:730, pkt 16; z 6.10.1982 r., C-283/81, Srl CILFIT i Lanificio di Gavardo SpA v. Ministero della sanità, EU:C:1982:335, pkt 19; z 1.12.2016 r., C-395/15, Mohamed Daouidi v. Bootes Plus SL u. a., EU:C:2016:917, pkt 50).

102 Ponadto przy wykładni pojęć użytych w RODO należy uwzględniać podstawowe zasady prawa europejskiego, w szczególności **zasadę pierwszeństwa** (zob. wyrok TS z 15.07.1964 r., C-6/64,

Flaminio Costa v. E.N.E.L., EU:C:1964:66) oraz **zasadę efektywności** (*effet utile*), zgodnie z którymi prawo europejskie jest nadrzędne w stosunku do prawa krajowego państw członkowskich, co powoduje, że sprzeczna z przepisem prawa unijnego norma krajowa nie może być zastosowana w konkretnym przypadku, a po wtóre, na państwach członkowskich spoczywa obowiązek zapewnienia efektywności prawa europejskiego i osiągania jego wyznaczonych celów. Równocześnie jednak należy zwrócić uwagę na związaną z tymi zasadami i służącą ich realizacji zasadę autonomiczności pojęć prawa europejskiego, która również realizuje potrzebę jednolitości stosowania prawa europejskiego.

B. Dane osobowe

Dominik Lubasz

Podstawa prawna: art. 4 pkt 1 RODO.

a. Znaczenie pojęcia

Zgodnie z art. 4 pkt 1 RODO **dane osobowe** oznaczają: 103

> „wszelkie 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".

WAŻNE! W definicji pojęcia danych osobowych wyróżnić należy trzy podstawowe **elementy określonej kwalifikacyjnej treści (informacji), którą można uznać za dane osobowe**:
1) muszą to być informacje – bez względu na rodzaj, a zatem wszelkie informacje;
2) informacje te muszą dotyczyć osoby fizycznej;
3) osoba ta musi być zidentyfikowana lub możliwa do zidentyfikowania.

b. Wszelkie informacje

Pojęcie danych osobowych obejmuje **wszelkiego rodzaju informacje**, bez względu na formę ich przekazywania lub udostępniania, np. w postaci pisemnej, ustnej, obrazu, dźwięku, a także utrwalenia na nośniku. Nie ma znaczenia, czy informacje te są prawdziwe, czy nie (np. wypowiedź zniesławiająca), obiektywne czy subiektywne. Nie jest to dystynktywny sposób wyrażenia – w znakach językowych czy pozajęzykowych, cechach fizjologicznych czy właściwościach biologicznych, np. sposób mówienia, pisania na klawiaturze, składania podpisu. 104
Pojęcie informacji należy interpretować w sposób **szeroki**.

PRZYKŁAD: W zakres tych informacji wchodzą dane o cechach bezpośrednio lub pośrednio identyfikujących, związane np. z użytym identyfikatorem, jak imię i nazwisko, numer identyfikacyjny, także np. datą urodzin, adresem zamieszkania (w wyroku TS z 29.01.2008 r., C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, EU:C:2008:54, Trybunał Sprawiedliwości wskazał na nazwiska i adresy osób fizycznych jako ich dane osobowe) czy też innymi czynnikami, jak płeć, kolor oczu, waga, wzrost lub inne dane biometryczne odnoszące się do właściwości biologicznych, czyli czynniki o charakterze fizycznym, fizjologicznym, ale również informacje dotyczące poglądów, przekonań, wypowiedzi czy życzeń.
Wprost w definicji pojęcia danych osobowych wskazuje się informacje dotyczące genetycznej, psychicznej, kulturowej lub społecznej oraz ekonomicznej tożsamości osoby fizycznej. Czynniki te obejmują więc informacje nie tylko o charakterze osobistym, lecz także majątkowym, dotyczące zarówno życia prywatnego i rodzinnego danej osoby (zob. wyrok ETPC z 16.02.2000 r., 27798/95, Amann v. Szwajcaria, HUDOC, pkt 65, w którym stwierdzono, że „termin «życie prywatne» nie może być interpretowany w sposób zawężający. W szczególności, poszanowanie życia prywatnego obejmuje prawo do nawiązywania i rozwijania relacji z innymi ludźmi; ponadto nic nie uzasadnia wykluczenia czynności o charakterze zawodowym lub handlowym z zakresu pojęcia «życie prywatne» (zob. wyrok ETPC w sprawie Niemietz przeciwko v. Niemcy z dnia 16 grudnia 1992 r., seria A nr 251-B, str. 33–34, pkt 29 oraz wyrok ETPC w sprawie Halford, str. 1015–16, pkt 42). Ta szeroka interpretacja jest zgodna z konwencją Rady Europy z dnia 28 stycznia 1981 r."), jak i wszelkich aktywności, relacji zawodowych (wyrok TS z 6.11.2003 r., C-101/01, Bodil Lindqvist, EU:C:2003:596, pkt 24, w którym na gruncie analizy pojęcia danych osobowych, zgodnie z definicją zawartą w art. 2 lit. a dyrektywy 95/46, Trybunał stwierdził, że termin ten obejmuje niewątpliwie nie tylko nazwisko osoby w połączeniu z jej danymi telefonicznymi, lecz także informacje o jej warunkach pracy lub zainteresowaniach; także wyrok ETPC z 28.11.2017 r., 70838/13, Antović i Mirković v. Czarnogóra, HUDOC) lub też zachowań ekonomicznych albo społecznych, niezależnie od zajmowanego stanowiska, cechy obiektywności czy prawdziwości, byleby umożliwiały spełnienie przesłanki związku i identyfikowalności danej osoby fizycznej, której dotyczą. Ponadto wymieniono informacje o danych lokalizacyjnych oraz identyfikatorach internetowych – uściślając w motywie 30 RODO, że dotyczy to adresów IP [zob. także wyrok TS z 24.11.2011 r., C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), EU:C:2011:771, w którym adres IP został uznany za dane osobowe w relacji do dostawcy dostępu do Internetu, w relacji natomiast do dostawcy usług medialnych (*content provider*) w wyroku TS z 19.10.2016 r., C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, EU:C:2016:779 – identyfikatory plików *cookie* – generowane z urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane np. przez etykiety RFID]. Danymi osobowymi będą również nagrania dźwiękowe lub obrazu (Grupa Robocza Art. 29, Opinia 4/2007 w sprawie pojęcia danych osobowych, przyjęta 20.06.2007 r., dokument WP 136, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pl.pdf, dostęp: 1.09.2021 r.), w tym monitoringu (zob. wyrok TS z 14.12.2014 r., C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, EU:C:2014:2428).

WAŻNE! **Nie jest możliwe określenie zamkniętego katalogu informacji o cechach osobowych.**

c. Informacje dotyczące osoby fizycznej

105 Zgodnie z motywem 14 RODO rozporządzenie obejmuje swoją **ochroną osoby fizyczne w związku z przetwarzaniem ich danych osobowych**. **Nie ma w tym kontekście zna-**

czenia obywatelstwo, miejsce zamieszkania ani aktywność zawodowa danej osoby, w tym związek przetwarzania np. z prowadzeniem działalności gospodarczej, jako że w definicji pojęcia danych osobowych nie zostały wprowadzone żadne dodatkowe desygnaty terminu „osoba fizyczna".

PRZYKŁAD: Z perspektywy definicji danych osobowych irrelewantne jest, czy chodzi o dane wykorzystywane przez administratora w związku z działalnością gospodarczą lub zawodową osoby, której dane dotyczą, czy też występującej np. w charakterze konsumenta. W każdym przypadku będą to dane osobowe osoby fizycznej, z perspektywy przepisów zasadniczo podlegające ochronie (wyrok TS z 20.05.2003 r., C-465/00, C-138/01 i C-139/01, Rechnungshof v. Österreichischer Rundfunk i in. oraz Christa Neukomm i Joseph Lauermann v. Österreichischer Rundfunk, EU:C:2003:294, pkt 73, a także wyroki ETPC: z 16.02.2000 r., 27798/95, Amann v. Szwajcaria, HUDOC, pkt 65, oraz z 4.05.2000 r., 28341/95, Rotaru v. Rumunia, HUDOC, pkt 43), w zakresie zastosowania przepisów chroniących prywatność również w przypadku informacji związanych z działalnością o charakterze zawodowym lub gospodarczym.

Ochrona **w zasięgu terytorialnym zastosowania rozporządzenia** (art. 3 RODO) obejmuje w konsekwencji wszystkie osoby fizyczne w związku z przetwarzaniem ich danych.

106 Pojęcie osoby fizycznej, choć niezdefiniowane w rozporządzeniu, prawodawca unijny zdaje się stawiać **w opozycji do osoby prawnej**, której dane ochronie na podstawie rozporządzenia **nie podlegają**, co podkreśla się w motywie 14, wskazując wprost, że rozporządzenie nie odnosi się do przetwarzania danych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej. Zabieg ten jest typowy dla nowoczesnych systemów prawnych, w których co do zasady występują tylko te dwa rodzaje podmiotów prawa:

– osoby fizyczne, czyli jednostki ludzkie, i
– osoby prawne, czyli twory społeczne,

w obu przypadkach wyposażone w podmiotowość prawną.

Dystynkcja kreacyjna wyznacza pośrednio zakres pojęcia osoby fizycznej.

Warto jednak również zwrócić uwagę na podmiotowość prawną osób fizycznych wyrażającą się przez atrybut, jakim jest zdolność prawna, a zatem zdolność do bycia podmiotem praw i obowiązków, którą każdy człowiek ma **od chwili urodzenia do chwili śmierci**. Wywołuje ona bezpośrednie konsekwencje w zakresie braku zastosowania regulacji do danych **osób zmarłych i nasciturusa**. Należy zwrócić uwagę na okoliczność, że dane takie mogą podlegać ochronie pośredniej, z uwagi na brak wiedzy administratora o śmierci podmiotu danych, a także na fakt, że dane o osobach nieżyjących, zwłaszcza ich schorzeniach, mogą zawierać informację dotyczącą spokrewnionych osób żyjących, czy też wreszcie na gruncie szczególnych regulacji, np. dotyczących praw pacjenta.

WAŻNE! **Osobą fizyczną jest człowiek od chwili narodzin do chwili śmierci.**

107 O ile w motywie 14 RODO przesądzono, iż co do zasady rozporządzenie **ma nie odnosić się do przetwarzania danych dotyczących osób prawnych**, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej, o tyle nie można wykluczyć takich sytuacji, w których jednak dane o charakterze osobowym będą związane z danymi dotyczącymi osób prawnych.

PRZYKŁAD: Sytuacja taka może dotyczyć danych osób fizycznych, w szczególności w przypadku, gdy w skład firmy wchodzą imię i nazwisko wspólnika, czy też w zakresie dotyczącym członków organów. Spełnienie przesłanki identyfikowalności przesądzić bowiem powinno o objęciu zakresem ochronnym rozporządzenia danych osobowych również w takich konfiguracjach.

Problematyka kwalifikacji danych dotyczących osób prawnych w powyższym zakresie była przedmiotem rozważań Trybunału Sprawiedliwości w sprawach połączonych C-92/09 oraz C-93/09 (wyrok TS z 9.11.2010 r., C-92/09 i C-93/09, Volker und Markus Schecke i Hartmut Eifert v. Land Hessen, EU:C:2010:662). W rozstrzygnięciu tym Trybunał stwierdził, że osoby prawne mogą się powoływać na ochronę z art. 7 i 8 KPP UE w odniesieniu do identyfikacji osobowej właśnie wtedy, gdy nazwa oficjalna osoby prawnej identyfikuje jedną lub więcej osób fizycznych.
Zagadnieniem danych dotyczących osób prawnych zajmowała się również Grupa Robocza Art. 29 w opinii 4/2007, podając m.in. przykład poczty elektronicznej wykorzystywanej w ramach prowadzonej działalności gospodarczej w formie spółki będącej osobą prawną. Na gruncie tego samego przykładu Grupa Robocza Art. 29 w opinii 4/2007 sformułowała konstatację, że jeżeli kryteria „treść", „cel" lub „skutek" pozwalają na uznanie informacji o osobie prawnej lub o przedsiębiorstwie za „dotyczącą" osoby fizycznej, należy uznać je za dane osobowe i stosować przepisy o ochronie danych osobowych. Stanowiska te zachowują aktualność na gruncie RODO.

108 Informacje, by być relewantnymi z punktu widzenia definicji danych osobowych, muszą **dotyczyć** osoby fizycznej. Musi zatem istnieć **związek między informacją a osobą fizyczną**. Związek ten należy badać przez pryzmat:
– **treści**,
– **celu** lub
– **skutku**.
Związek może mieć zarówno charakter **osobowy**, jak i **rzeczowy (majątkowy)**, np. przez odwołanie się do majątku danej osoby czy używanych przez nią urządzeń.

WAŻNE! **Związek pomiędzy informacją a osobą fizyczną nie może mieć wyłącznie charakteru statystycznego, ponieważ nie pozwala wtedy na identyfikację. Taka relacja zatem co do zasady nie występuje w przypadku danych zagregowanych o charakterze statystycznym. Ocena ta może jednak ulec zmianie, jeśli niewielka liczba agregowanych danych pozwala na ustalenie relacji do konkretnych osób. W omawianym zakresie nie jest rozstrzygające, czy informacja dotyczy jednej, czy wielu osób, o ile przez skonkretyzowany charakter komunikacji, przy wypowiedzi nawet kierowanej do grupy osób, możliwa jest identyfikacja poszczególnych osób fizycznych posiadających wspólną cechę.**

d. Informacje pozwalające na zidentyfikowanie osoby fizycznej

109 Na podstawie informacji dotyczących osoby fizycznej musi być ona **zidentyfikowana lub możliwa do zidentyfikowania** – tzw. **przesłanka identyfikowalności**. To administrator, dysponując określonymi informacjami, musi mieć możliwość ustalenia na ich podstawie tożsamości osoby, której dane przetwarza. Rozróżnić należy sytuacje, w których dla administratora dana **osoba jest zidentyfikowana**, i sytuacje, w których jest jedynie **możliwa do zidentyfikowania**.

Zidentyfikowaną osobą fizyczną jest osoba, której tożsamość jest ustalona – bezpośrednio i natychmiast, czyli taka, którą bezpośrednio można wskazać, wyodrębnić lub wyróżnić z określonej zbiorowości. Nie musi to natomiast polegać na podaniu jej imienia i nazwiska. Konstatacja ta jest zwłaszcza istotna w środowisku cyfrowym, w którym identyfikacja sprowadza się do oznaczenia danego użytkownika w celu wywierania na niego określonego wpływu. Aspekt ten podkreślono w dokumencie roboczym Grupy Roboczej Art. 29 WP 105 na temat kwestii z zakresu **ochrony danych związanych w technologią RFID**, wskazując, że dane dotyczą zidentyfikowanej osoby, jeżeli odnoszą się do tożsamości, cech lub zachowania danej osoby lub też jeśli informacje te determinują bądź wpływają na sposób traktowania lub ocenę danej osoby. 110

Identyfikacja dokonywana jest na podstawie poszczególnych informacji nazywanych **„czynnikami identyfikującymi"**, na które składają się informacje w szczególności wymienione przykładowo w definicji danych osobowych zawartej w art. 4 pkt 1, w tym tzw. **Identyfikatory** (zob. nr 104 – przykład).

Możliwą do zidentyfikowania jest osoba, której tożsamość dopiero administrator może ustalić, niezależnie od tego, czy to zrobi, czy nie. W procesie przetwarzania danych nie musi dochodzić zatem do identyfikacji podmiotu danych, do zakwalifikowania danej informacji wystarcza sama możliwość identyfikacji. 111

Dla oceny tej możliwości uwzględnić należy czynniki zobiektywizowane, tj. **wszelkie rozsądnie prawdopodobne sposoby**, w stosunku do których **istnieje uzasadnione prawdopodobieństwo**, że zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. W szczególności wchodzą w grę takie czynniki, jak:

- koszt i czas potrzebne do jej zidentyfikowania oraz
- technologia dostępna w momencie przetwarzania danych, a także
- postęp technologiczny.

PRZYKŁAD: W wyroku z 19.10.2016 r., C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, EU:C:2016:779, który wprawdzie zapadł w poprzednim stanie prawnym, lecz zachowuje aktualność, Trybunał Sprawiedliwości przesądził, że dynamiczny adres IP ma walor informacji o charakterze osobowym, ponieważ na jego podstawie możliwe jest zidentyfikowanie osoby fizycznej (użytkownika urządzenia, do którego przypisany został w danej sesji dynamiczny adres IP), mimo że administrator w celu ustalenia tożsamości musi wszcząć postępowanie, w którym dopiero uzyska dodatkowe informacje pozwalające na identyfikację. Zaprezentowane podejście znacznie poszerzyło zakres pojęcia danych osobowych, ponieważ już niewielka wiązka informacji, z uwagi na uzasadnioną możliwość korzystania przez administratora w celu identyfikacji osoby z pomocy lub wiedzy innych administratorów, w tym aparatu wymiaru sprawiedliwości, w wielu przypadkach pozwoli na ustalenie tożsamości.

Wobec powyższego spełnienie przesłanki identyfikacyjnej powinno być weryfikowane przez zakres aktywności administratora lub innej osoby o określonym rozsądnym prawdopodobieństwie, ograniczonym jednak przez zobiektywizowane czynniki, jak koszt i czas potrzebne do jej zidentyfikowania, technologię dostępną w momencie przetwarzania danych czy postęp technologiczny. Zobiektywizowane kryteria dają podstawę do dokonywania **analizy ryzyka uznania danej informacji za osobową**, a w konsekwencji objęcia jej zakresem zastosowania rozporządzenia.

Informacje relewantne definicyjnie, na podstawie których możliwe będzie zidentyfikowanie osoby fizycznej, **obejmują zarówno dane, które są w posiadaniu administratora, jak i takie, które musi on pozyskać od podmiotów trzecich**. 112

PRZYKŁAD: Trybunał Sprawiedliwości w sprawie C-101/01, Lindqvist wskazywał na łączenie danych znajdujących się również w zasobach administratora w celach identyfikacyjnych (pkt 27).

Fakt zatem, że informacje umożliwiające łącznie identyfikację określonej osoby fizycznej nie znajdują się częściowo w posiadaniu jednego podmiotu, nie wyklucza uznania ich za dane osobowe. Jak wskazano dalej, sięganie przez administratora do zasobów informacyjnych innych podmiotów nie ma jednak charakteru absolutnego i ograniczone jest obiektywnymi czynnikami wskazanymi w motywie 26 RODO, takimi jak koszt i czas potrzebne do jej zidentyfikowania, a także dostępną w momencie przetwarzania danych technologią, jak również postępem technologicznym. Zgodnie ze stanowiskiem wyrażonym przez Trybunał Sprawiedliwości w sprawie C-582/14, Breyer, nie wykraczają poza czynnik związany z określonym **nakładem czasu, kosztów i pracy ludzkiej** przypadki, w których administrator dysponuje środkami prawnymi umożliwiającymi mu zidentyfikowanie osoby, której dane dotyczą, dzięki dodatkowym informacjom będącym w posiadaniu innych osób, w stosunku do których wspomniane środki prawne może skierować.

e. Dane anonimowe

113 Zasady ochrony danych nie powinny więc mieć zastosowania do **informacji anonimowych**, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Rozporządzenie nie dotyczy przetwarzania anonimowych informacji, w tym przetwarzania do celów statystycznych lub naukowych. Zaznaczyć jednocześnie należy, że już spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. Pseudonimizacja jest bowiem formą zabezpieczenia przetwarzania danych osobowych, a nie pozbawiania informacji cech kwalifikacyjnych jako dane osobowe.
Ocena, czy określone dane są anonimowe, musi następować przy uwzględnieniu wytycznych sformułowanych w motywie 26, tj. z uwzględnieniem wszelkich rozsądnie prawdopodobnych sposobów, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Uwzględnić przy tym należy również określony stan wiedzy na dzień przetwarzania oraz przewidywany postęp techniczny, a także czynniki takie jak koszt i czas potrzebne do „odwrócenia" anonimizacji, czyli dokonania identyfikacji określonej osoby, której dane dotyczą.

f. Dane zwykłe i szczególne kategorie danych

114 Podział na dane zwykłe i szczególne kategorie danych ma wpływ na obowiązki administratorów, zwłaszcza przy dokonywaniu oceny ryzyka danych i związanego z tym bezpieczeństwa przetwarzania, rejestrowania czynności, obowiązkowego powołania inspektora ochrony danych, a także – a może przede wszystkim – przesłanek legalizacyjnych.

W art. 9 ust. 1 RODO sformułowany został **zamknięty katalog danych szczególnych kategorii**. Należą do nich dane osobowe ujawniające: 115
– pochodzenie rasowe lub etniczne,
– poglądy polityczne,
– przekonania religijne lub światopoglądowe,
– przynależność do związków zawodowych oraz
– dane genetyczne,
– dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby.

Dane nieobjęte art. 9 są danymi zwykłymi. *Novum* stanowi zakwalifikowanie jako danych zwykłych informacji o wyrokach skazujących i czynach zabronionych, poddanych w rozporządzeniu szczególnej regulacji w art. 10, 35 i 37.

Ponadto część danych szczególnych kategorii została przez prawodawcę unijnego potraktowana regulacyjnie w sposób szczególny nie tylko przez ich kwalifikację jako danych szczególnych kategorii, ale i zdefiniowanie ich odpowiednio w art. 4 pkt 15 (dane o stanie zdrowia), art. 4 pkt 14 (dane biometryczne), art. 4 pkt 13 (dane genetyczne).

W odróżnieniu od danych osobowych zwykłych przetwarzanie danych osobowych szczególnych kategorii jest zakazane, z zastrzeżeniem wyjątków wskazanych w art. 9 ust. 2 Należy przy tym uwzględnić, że prawo państw członkowskich może obejmować przepisy szczegółowe o ochronie danych stwarzające warunki do zastosowania przepisów niniejszego rozporządzenia, tak by można było wypełnić obowiązki prawne lub wykonać zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Oprócz wymogów szczegółowych mających zastosowanie do takiego przetwarzania zastosowanie powinny mieć zasady ogólne i inne przepisy rozporządzenia, w szczególności jeżeli chodzi o warunki zgodności przetwarzania z prawem. 116

C. Przetwarzanie

Witold Chomiczewski

Podstawa prawna: art. 4 pkt 2 RODO.

a. Znaczenie pojęcia

Pojęcie przetwarzania jest kluczowe dla właściwego stosowania RODO. To bowiem wraz **z podjęciem działań klasyfikowanych jako przetwarzanie pojawiają się po stronie administratora, a także podmiotu przetwarzającego określone przez rozporządzenie 2016/679 obowiązki**. Należy do nich w szczególności konieczność legitymowania się przez administratora spełnieniem jednej z przesłanek legalizujących przetwarzanie, o których mowa w art. 6 ust. 1 RODO, a w odniesieniu do danych osobowych szczególnej kategorii – w art. 9 ust. 2 RODO. Innym obowiązkiem jest przykładowo przekazanie podmiotom danych informacji wskazanych w art. 13 albo 14 RODO. 117

WAŻNE! Z tego względu popełnienie błędu na etapie klasyfikacji, tj. udzielenia odpowiedzi na pytanie, czy określone operacje mieszczą się w pojęciu przetwarzania w rozumieniu art. 4 pkt 2 RODO, prowadzić będzie do całego szeregu naruszeń przepisów RODO. Dlatego właściwe zrozumienie pojęcia przetwarzania jest niezmiernie istotne.

118 Przetwarzaniem zgodnie z RODO jest **każda operacja lub każdy zestaw operacji na danych osobowych**, które odbywają się w sposób zautomatyzowany lub niezautomatyzowany. Istota pojęcia sprowadza się zatem do działania podejmowanego na informacjach kwalifikowanych jako dane osobowe. Działanie takie musi być **zależne od decyzji człowieka**, czyli albo być bezpośrednio przez niego podejmowane, albo następować wprawdzie automatycznie, ale w sposób zależny od woli człowieka.

PRZYKŁAD: Z sytuacją taką możemy mieć do czynienia w przypadku napisania przez człowieka programu komputerowego w taki sposób, by dokonywał określonej operacji na danych osobowych.

WAŻNE! Definicja przetwarzania zupełnie abstrahuje od woli i świadomości człowieka. Dla zaistnienia przetwarzania **nie jest zatem istotne, czy dana osoba chce przetwarzać dane osobowe** i czy zdaje sobie sprawę z tego, że informacje, na których dokonuje działań, są danymi osobowymi.
Ocena jest zatem obiektywna.

b. Katalog przykładowych operacji na danych osobowych

119 Prawodawca unijny zdecydował się na wskazanie przykładowych operacji, które o ile będą przeprowadzane na danych osobowych, to będą klasyfikowane jako przetwarzanie w rozumieniu art. 4 pkt 2 RODO. **W treści przepisu wymieniono**: 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.

PRZYKŁAD: Do tego typu operacji, ale już skonkretyzowanych, można zaliczyć: zbieranie danych osobowych na potrzeby zawarcia umowy, segmentowanie bazy danych klientów, przechowywanie danych osobowych w tzw. chmurze obliczeniowej czy przekazanie do zniszczenia formularzy ze zgłoszeniami do zakończonego już konkursu.

120 Trzeba zwrócić uwagę, że **powyższy katalog jest otwarty**. Oznacza to, że jeżeli podjęte zostanie niewymienione w nim działanie, ale będzie ono miało za przedmiot dane osobowe, to również będzie stanowiło przetwarzanie. Nie ma znaczenia, że nie zostało ono wskazane w art. 4 pkt 2 RODO. Zresztą pokazuje to już sama treść art. 4 RODO. Prawodawca unijny definiuje w nim również inne operacje na danych osobowych stanowiące przetwarzanie, które nie są wymienione w katalogu otwartym. Przykładem mogą być **profilowanie** oraz **pseudonimizacja**.

D. Profilowanie

Witold Chomiczewski

Podstawa prawna: art. 4 pkt 4 RODO.

a. Znaczenie pojęcia

Profilowanie jest jedną z postaci przetwarzania w rozumieniu art. 4 pkt 2 RODO. Jest jednak na tyle szczególną jego postacią, że prawodawca unijny zdecydował się na osobne zdefiniowanie tego rodzaju operacji na danych osobowych. Wynikało to w szczególności z istotnych **zagrożeń**, które może wywoływać ta postać przetwarzania **dla praw podstawowych podmiotów danych**. Posłużenie się w toku profilowania nierzetelnymi danymi czy zastosowanie niesprawdzonych danych statystycznych może prowadzić do dyskryminacji. **121**
Wyszczególnienie profilowania jako osobnej czynności przetwarzania ma służyć **wzmocnieniu pozycji prawnej podmiotów danych**. Realizowane jest to w szczególności przez **przewidziane w art. 22 RODO prawo do niepodlegania zautomatyzowanym decyzjom**, w tym profilowaniu, oraz obowiązki informacyjne uregulowane w art. 13 ust. 1 lit. f i art. 14 ust. 2 lit. g RODO.

Przetwarzanie będzie stanowiło profilowanie, jeżeli **spełnione będą łącznie następujące przesłanki**: **122**
– przetwarzanie następuje automatycznie;
– na podstawie danych osobowych następuje ocena niektórych czynników osobowych.

b. Zautomatyzowane przetwarzanie

Do zaistnienia profilowania konieczne jest, by proces przetwarzania następował automatycznie. **Operacji na danych osobowych nie może dokonywać człowiek**, lecz musi być ona przeprowadzana przez, przykładowo, algorytm lub innego rodzaju oprogramowanie. Rola człowieka ogranicza się tu zatem do odpowiedniego zaprogramowania narzędzi służących przetwarzaniu. **123**

WAŻNE!
– Przetwarzanie będzie nadal **zautomatyzowane**, gdy człowiek będzie pełnił w nim rolę pomocniczą, a nie podejmował decyzje. Jeżeli zatem w procesie oceny zdolności kredytowej zadaniem człowieka będzie jedynie przekazanie klientowi decyzji podjętej przez algorytm, bez realnej możliwości jej zmiany, to przetwarzanie nadal pozostanie zautomatyzowane. Taki bowiem udział człowieka pozostaje bez wpływu na sam efekt przetwarzania.
– Jeżeli natomiast decyzja algorytmu będzie tylko jednym z czynników, które człowiek powinien wziąć pod uwagę w toku oceny zdolności kredytowej, i analityk będzie mógł podjąć decyzję inną niż wskazana przez algorytm, to **przesłanka zautomatyzowanego przetwarzania nie będzie spełniona**.

c. Ocena czynników człowieka

124 W ramach zautomatyzowanego przetwarzania danych osobowych **musi następować ocena niektórych czynników osobowych człowieka**. Prawodawca unijny jako przykładowe wskazał analizę lub prognozę aspektów dotyczących:
- efektów pracy człowieka,
- jego sytuacji ekonomicznej,
- zdrowia,
- osobistych preferencji,
- zainteresowań,
- wiarygodności,
- zachowania,
- lokalizacji lub przemieszczania się.

> *WAŻNE!* **Istota profilowania** sprowadza się do wnioskowania na podstawie znanych administratorowi danych osobowych konkretnego człowieka o jego cechach.

Wnioskowanie to następuje przez **zestawienie** znanych administratorowi informacji o danym człowieku **z odpowiednim modelem statystycznym**. Model taki, w uproszczeniu, wskazuje, że jeżeli statystycznie osoba posiada cechy A oraz B, to posiada również cechę C. Na tej podstawie w toku profilowania zakłada się, że cecha C wystąpi również u osoby, której dane są przetwarzane, skoro posiada cechy A oraz B.

PRZYKŁAD: Dopasowywanie treści reklamowej wyświetlanej w Internecie do przewidywanych zainteresowań użytkownika. Jeżeli z modelu statystycznego wynikałoby zatem, że osoby wykonujące zawód doradcy kredytowego, będące w wieku między 30 a 35 lat, które interesują się podróżami, najczęściej wyjeżdżają we wrześniu na wyjazdy weekendowe do innych miast, to po stwierdzeniu u danego użytkownika pierwszych trzech cech mogłaby mu zostać wyświetlona w sierpniu reklama takich wyjazdów. Byłby to efekt profilowania.

125 Należy podkreślić, że **nie stanowi profilowania zwykła segmentacja bazy danych**. Jeżeli przykładowo wprowadzane są do bazy danych klientów podziały na poszczególne segmenty z uwzględnieniem obszarów, na których ci klienci mieszkają, to nie dochodzi tu do oceny niektórych czynników osobowych człowieka w rozumieniu art. 4 pkt 4 RODO. Jest to jedynie posegregowanie bazy według znanego administratorowi kryterium. Taka segmentacja nie stanowi zatem profilowania.

d. Profilowanie a podejmowanie zautomatyzowanych decyzji

126 Zakwalifikowanie określonej czynności przetwarzania jako profilowania **nie oznacza, że należy w każdym przypadku stosować art. 22 RODO**. Ogranicza on bowiem sytuacje, w których można stosować zautomatyzowane podejmowanie decyzji, w tym profilowanie, ale jedynie wówczas, gdy prowadzi ono do podjęcia wobec człowieka decyzji wywołującej skutki prawne lub w inny podobny sposób istotnie na niego wpływającej. Nie każde profilowanie będzie spełniało ten warunek.
Konieczna zatem jest **dodatkowa ocena**, czy dany proces profilowania spełnia dodatkowe przesłanki określone w art. 22 ust. 1 RODO.

E. Administrator

Witold Chomiczewski

Podstawa prawna: art. 4 pkt 7 RODO.

a. Znaczenie pojęcia

Administrator to, obok danych osobowych oraz przetwarzania, najważniejsze pojęcie dla właściwego stosowania rozporządzenia 2016/679. **Kwalifikacja określonego podmiotu jako administratora ma bowiem bardzo szerokie konsekwencje.** Jest on adresatem zdecydowanej większości obowiązków wynikających z RODO. To również na administratora mogą być nakładane kary pieniężne przewidziane w RODO. Dlatego właściwe zrozumienie definicji określonej w art. 4 pkt 7 RODO ma tak zasadnicze znaczenie. 127

Do kwalifikacji określonej osoby fizycznej lub prawnej, organu publicznego, jednostki lub innego podmiotu jako administratora **konieczne jest, by ustalał on, samodzielnie lub wspólnie z innymi podmiotami, cele i sposoby przetwarzania danych osobowych**. 128

> ***WAŻNE!*** Ocena, czy dany podmiot jest administratorem, następuje obiektywnie i niezależnie od jego woli. Nie ma też żadnego znaczenia świadomość pełnienia tej roli przez dany podmiot, ważne jest jedynie, czy spełnione są przesłanki określone w art. 4 pkt 7 RODO.
> Nie jest dopuszczalne zrzeczenie się statusu administratora lub jego przeniesienie na inną osobę na podstawie umowy.

b. Osoba fizyczna, prawna, organ publiczny

Zgodnie z art. 4 pkt 7 RODO **administratorem może być osoba fizyczna, osoba prawna, organ publiczny, jednostka lub inny podmiot**. Administratorem będzie zatem określona osoba prawna, np. spółka z ograniczoną odpowiedzialnością, fundacja, izba gospodarcza, jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, np. spółka komandytowa, osoba fizyczna, np. przedsiębiorca prowadzący indywidualną działalność gospodarczą, organ publiczny lub inny podmiot. 129

> ***WAŻNE!*** Administratorem nie jest człowiek sprawujący funkcję kierowniczą w danej osobie prawnej czy jednostce organizacyjnej nieposiadającej osobowości prawnej ani osoba zatrudniona w ramach jednoosobowej działalności gospodarczej.

Oczywiście, by być administratorem, wskazane podmioty muszą spełniać także drugi warunek określony w art. 4 pkt 7 RODO, czyli ustalać cele i sposoby przetwarzania.

c. Ustalanie celów i sposobów przetwarzania

130 W pewnym uproszczeniu można powiedzieć, że **ustalenie celu odpowiada na pytanie: po co** przetwarzane mają być dane osobowe, **a sposobu – na pytanie: jak** dany cel ma zostać osiągnięty.

PRZYKŁAD: Podjęcie przez spółkę prowadzącą sklep decyzji o wysłaniu listem gazetek promocyjnych do potencjalnych klientów sprawi, że spółka ta stanie się administratorem. Określiła bowiem cel przetwarzania w postaci celu marketingowego, gdyż będzie chciała zachęcić tych klientów do zakupu, oraz wskazała sposób przetwarzania, czyli to, jak cel ten ma zostać osiągnięty – poprzez wysłanie listów na adresy klientów sklepu.

WAŻNE! Administrator nie musi samodzielnie przetwarzać danych osobowych, by spełnić przesłanki wskazane w art. 4 pkt 7 RODO. Wystarczające jest, że ustali cele i sposoby takiego przetwarzania.

131 Zasadniczo wymaga się, by administrator podejmował zarówno decyzję o celu, jak i o sposobach przetwarzania. W dzisiejszej gospodarce występuje jednak coraz więcej wysoko wyspecjalizowanych usług związanych z przetwarzaniem, które są oferowane przez podmioty trzecie. W konsekwencji administrator może nie mieć pełnej świadomości, jakie sposoby przetwarzania będą zastosowane przy korzystaniu z takich rozwiązań, ani nie dysponować odpowiednią wiedzą, która pozwoli mu na dokładne określenie tych sposobów. W takich przypadkach **do kwalifikacji podmiotu jako administratora wystarczające jest, że określa on jedynie cel**, w jakim dane mają być przetwarzane, oraz **zakreśla ogólnie sposoby jego osiągnięcia**. Następuje to poprzez podjęcie decyzji o skorzystaniu z konkretnej usługi, do której realizacji konieczne jest zastosowanie określonych sposobów przetwarzania. Natomiast samo dookreślenie sposobów przetwarzania poprzez wybór konkretnych rozwiązań administrator pozostawia już usługodawcy, który będzie kwalifikowany jako podmiot przetwarzający.

PRZYKŁAD: Administrator, decydując się na wykorzystanie usługi remarketingu, w której reklamy produktów administratora mają być wyświetlane jedynie internautom interesującym się takimi towarami, nie musi znać dokładnie rozwiązań technicznych stosowanych do analizy zachowań poszczególnych internautów oraz określania ich zainteresowań. Istotne jest jedynie, że decyduje się na skorzystanie z takiego działania oraz, podejmując tę decyzję, ogólnie określa sposoby przetwarzania dla realizacji tego celu.

d. Samodzielne lub wspólne podejmowanie decyzji

132 Nie jest konieczne, by administrator samodzielnie podejmował decyzję o celach i sposobach przetwarzania. Może to robić wspólnie z innymi podmiotami. Nie jest limitowana liczba takich podmiotów.

Konsekwencją możliwości wspólnego podejmowania powyższych decyzji jest art. 26 RODO, który reguluje konstrukcję **współadministrowania**. Prawodawca unijny wskazał w nim, co współadministratorzy powinni między sobą określić w umowie o współadministrowaniu.

WAŻNE! Nie jest współadministrowaniem danymi przypadek, gdy te same dane osobowe są przetwarzane przez dwa lub więcej podmiotów, ale każdy z nich robi to we własnym, odrębnym celu.

PRZYKŁAD: Założenie profilu firmowego na portalu społecznościowym oznacza przyjęcie roli administratora w odniesieniu do danych osobowych użytkowników odwiedzających taki profil. Jednak nie oznacza to bycia współadministratorem danych z właścicielem takiego portalu. Wprawdzie on również jest administratorem danych osobowych użytkowników, jednak przetwarza je m.in. w celu realizacji umowy o założenie konta na takim portalu. Mamy tu zatem do czynienia z równoległym przetwarzaniem tych samych danych osobowych, jednak w indywidualnych celach dwóch administratorów.

Trzeba jednocześnie podkreślić, że z orzecznictwa TSUE wynika, iż współadministrowanie danymi może mieć miejsce wówczas, gdy cele przetwarzania kilku administratorów są ze sobą blisko związane lub wzajemnie się uzupełniają (zob. zwłaszcza wyrok TS z 29.07.2019 r., C-40/17, Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV, EU:C:2019:629).

WAŻNE! Oceniając, czy zachodzi relacja współadministrowania, należy zbadać w pierwszej kolejności, czy przetwarzanie następuje we wspólnym celu, a jeżeli nie, to czy cele każdego z administratorów są ze sobą blisko związane lub wzajemnie się uzupełniają.

Jednoznacznym przykładem współadministrowania może być organizacja przez dwa podmioty wspólnej konferencji.

e. Sytuacja szczególna

Mogą występować sytuacje, gdy **o statusie administratora** nie decyduje podjęcie wskazanych powyżej decyzji, lecz **przepis prawa**. Prawo unijne lub prawo państwa członkowskiego mogą określać cele i sposoby przetwarzania w danych sytuacjach. Wówczas to również te przepisy mogą określić, kto jest administratorem, albo wskazać kryteria służące do określenia, kto w danej sytuacji pełni rolę określoną w art. 4 pkt 7 RODO. W tych sytuacjach źródłem uznania, że dany podmiot decyduje o celach i sposobach przetwarzania, będzie przepis prawa, a nie ocena stanu faktycznego. **133**

F. Podmiot przetwarzający

Witold Chomiczewski

Podstawa prawna: art. 4 pkt 8 RODO.

a. Znaczenie pojęcia

Podmiotem przetwarzającym jest osoba fizyczna, osoba prawna, jednostka lub inny podmiot, który **przetwarza dane osobowe w imieniu administratora**. **134**

Ocena kwalifikacji określonego podmiotu jako podmiotu przetwarzającego, podobnie jak w przypadku administratora, następuje w **sposób zobiektywizowany**. Nie ma tu znaczenia świadomość i wola określonego podmiotu. Nie można również umownie określić, kto pełni rolę podmiotu przetwarzającego.

b. Osoba fizyczna, osoba prawna, organ publiczny

135 Podobnie jak w przypadku administratora, również podmiotem przetwarzającym jest osoba prawna (np. stowarzyszenie), jednostka organizacyjna niebędąca osobą prawną (np. spółka jawna), osoba fizyczna (np. prowadząca jednoosobową działalność gospodarczą), organ publiczny lub inny podmiot.

> *WAŻNE!* Podmiotem przetwarzającym nie jest pracownik zatrudniony w danym podmiocie czy też osoba pełniąca w nim funkcję kierowniczą, lecz ten podmiot, np. fundacja, a nie członek jej zarządu.

c. Przetwarzanie w imieniu administratora

136 Administrator nie ma obowiązku samodzielnego przetwarzania. Może do tego celu wykorzystywać podmioty, którym wyznacza określone zadania związane z przetwarzaniem, a one w tych ramach wykonują czynności na danych osobowych. Dzieje się to w ramach wskazanego przez administratora celu i sposobów przetwarzania. **Podmiot przetwarzający realizuje zatem wolę administratora w zakresie przetwarzania.**

> *WAŻNE!* Podmiot przetwarzający nie może samodzielnie wykraczać poza określone przez administratora cele i sposoby przetwarzania. Jeżeli to zrobi, to stanie się administratorem ze wszystkimi tego konsekwencjami.

PRZYKŁAD: Podmiotem przetwarzającym będzie: zewnętrzne biuro księgowe, podmiot, którego zadaniem jest zniszczenie dokumentów zawierających dane osobowe, podmiot świadczący usługi chmurowe.

d. Podstawa prawna powierzenia

137 Zgodnie z art. 28 RODO podstawą prawną powierzenia przetwarzania danych osobowych jest **umowa powierzenia lub inny instrument prawny**.
Zawarcie takiej umowy daje podmiotowi przetwarzającemu **uprawnienie do wykonywania operacji na danych osobowych w granicach określonych taką umową**. Granice te wyznaczane są zarówno przez określenie celu przetwarzania przez administratora, jak i na skutek sprecyzowania rodzaju danych osobowych, które mogą być przetwarzane.

PRZYKŁAD: Jeżeli administrator korzysta z usług zewnętrznej spółki, która wykonuje dla niego czynności związane z kompletowaniem zamówień złożonych przez sklep internetowy, adresowaniem paczek oraz przekazywaniem ich kurierom, to podstawą przetwarzania danych przez tę spółkę będzie umowa powierzenia. W niej zostanie określone, że podmiot przetwarzający może jedynie wykorzystywać dane osobowe klientów sklepu internetowego w celu przygotowania zamówień do wysyłki. Wskazane będzie także, że podmiot przetwarzający może w tym celu przetwarzać imię, nazwisko, adres zamieszkania, jak również numer zamówienia.

Natomiast innym instrumentem prawnym stanowiącym podstawę prawną powierzenia przetwarzania danych osobowych mogą być przepisy prawa krajowego lub unijnego, z których będzie wynikało powierzenie przetwarzania danych osobowych innemu podmiotowi.

e. Zagadnienia szczególne

Podmiot przetwarzający jest również odbiorcą danych w rozumieniu art. 4 pkt 9 RODO. 138
Jest też adresatem nie tylko art. 28 RODO, lecz także art. 29 i 32 tego aktu prawnego. W zakresie szczegółowych obowiązków, które są nakładane na podmiot przetwarzający na mocy tych przepisów, zob. uwagi do tych przepisów.

G. Odbiorca

Witold Chomiczewski

Podstawa prawna: art. 4 pkt 9 RODO.

a. Znaczenie pojęcia

Odbiorcą jest osoba fizyczna, prawna, organ publiczny, jednostka **lub inny podmiot, któremu ujawnia się dane osobowe**, niezależnie od tego, czy jest stroną trzecią. Przy czym nie są odbiorcą organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego. 139
Dla uznania danej osoby za odbiorcę musi być ona zatem kwalifikowana jako jeden z podmiotów wymienionych w definicji, np. musi być osobą prawną oraz muszą zostać jej ujawnione dane osobowe.

Pojęcie odbiorcy ma znaczenie w szczególności **przy realizacji obowiązków informacyjnych**, gdyż na podstawie art. 13 ust. 1 lit. e oraz art. 14 ust. 1 lit. e RODO administrator jest zobowiązany do przekazania podmiotowi danych informacji o odbiorcach danych osobowych lub kategoriach tych odbiorców. 140

WAŻNE! Właściwe określenie grona odbiorców, a więc prawidłowe zidentyfikowanie tych podmiotów przez pryzmat definicji z art. 4 pkt 9 RODO, ma decydujące znaczenie dla właściwej realizacji wskazanych obowiązków informacyjnych.

b. Osoba fizyczna, osoba prawna, organ publiczny

141 **Grono podmiotów**, które mogą być odbiorcami w rozumieniu art. 4 pkt 9 RODO, zostało **określone bardzo szeroko**. Należą do niego zarówno osoby fizyczne, jak i osoby prawne, organy publiczne, jednostki lub inne podmioty. Jedynym ograniczeniem jest wyłączenie z pojęcia odbiorcy organów publicznych w zakresie, w jakim otrzymują one dane osobowe w ramach konkretnego postępowania prowadzonego na podstawie przepisów unijnych lub prawa krajowego. Przykładowo nie będzie odbiorcą naczelnik urzędu skarbowego, który otrzyma dane osobowe podatnika w ramach prowadzonego postępowania. **Odbiorcami będą natomiast inni administratorzy czy podmioty przetwarzające.**

142 Tak szeroko zakreślony zakres podmiotowy rodzi **wątpliwości**, czy **pracownicy lub współpracownicy administratora** przetwarzający dane osobowe w ramach przestrzeni, nad którą kontrolę sprawuje administrator, powinni być kwalifikowani jako odbiorcy. Literalne brzmienie przepisu nie stoi temu na przeszkodzie, natomiast taka wykładnia nie dawałaby podmiotom danych dodatkowej ochrony, natomiast bardzo utrudniałaby wykonanie przez administratora jego obowiązków związanych z występowaniem odbiorców w procesie przetwarzania.

> ***WAŻNE!*** Pracownicy i współpracownicy administratora, którzy znajdują się pod kontrolą administratora, nie powinni być uznawani za odbiorców.

c. Ujawnianie danych osobowych

143 Do kwalifikacji podmiotu mieszczącego się w omówionym powyżej zakresie jako odbiorcy danych **konieczne jest, by dane osobowe były mu ujawniane**. Pod tym pojęciem zgodnie ze słownikiem języka polskiego należy rozumieć uczynienie jawnym tego, co do tej pory było trzymane w tajemnicy. Przekładając tę definicję na grunt RODO, można powiedzieć, że ujawnieniem danych będzie zarówno ich przekazanie przez administratora osobie, która dotąd danych tych nie znała, jak i stworzenie takich warunków, by taka osoba sama mogła poznać te dane osobowe.

> ***PRZYKŁAD:*** Ujawnieniem będzie przyznanie danej osobie dostępu do systemu teleinformatycznego, w którym przechowywane są dane osobowe, czy przekazanie jej dokumentów lub nośnika elektronicznego z danymi osobowymi.

H. Osoba, której dane dotyczą (podmiot danych)

Dominik Lubasz

Podstawa prawna: art. 4 pkt 1, art. 12–22 RODO.

144 Osoba, której dane dotyczą, określana również jako podmiot danych, jest podmiotem ochrony przepisów rozporządzenia 2016/679. To jej prawa podstawowego do ochrony danych dotyczy regulacja RODO.

Pojęcie to nie jest samodzielnie zdefiniowane w rozporządzeniu. Stanowi natomiast element definicji pojęcia danych osobowych. W jej świetle należy stwierdzić, że osobą, której dane dotyczą, jest **zidentyfikowana** lub **możliwa do zidentyfikowania osoba fizyczna**.

> *WAŻNE!* **Osobą, której dane dotyczą, jest zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna.**

I. Przedsiębiorca

Witold Chomiczewski

Podstawa prawna: art. 4 pkt 18 RODO.

a. Znaczenie pojęcia

145 Przedsiębiorcą jest osoba fizyczna lub prawna prowadząca działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą.
Kwalifikacja określonej osoby jako przedsiębiorcy **nie ma wpływu na uznanie jej za administratora czy też podmiot przetwarzający**. Na gruncie tych pojęć nie ma żadnego znaczenia, czy jest się przedsiębiorcą, czy też nie posiada się tego statusu. Pojęcie to pojawia się natomiast w art. 30 ust. 5, art. 47 oraz 88 ust. 2 RODO. Na ich podstawie:

- przedsiębiorca zatrudniający mniej niż 250 osób jest zwolniony, z wyjątkami wynikającymi z art. 30 ust. 5 RODO, z prowadzenia rejestru czynności przetwarzania lub rejestru kategorii czynności przetwarzania;
- grupa przedsiębiorców może korzystać z wiążących reguł korporacyjnych po ich zatwierdzeniu przez organ nadzorczy;
- określono wymogi dotyczące korzystania przez państwa członkowskie z klauzuli kompetencyjnej, która przewiduje możliwość wprowadzenia przepisów krajowych odnoszących się do przetwarzania danych osobowych pracowników.

b. Rozbieżności pomiędzy wersjami językowymi RODO

146 **W niemieckiej, angielskiej, francuskiej oraz hiszpańskiej wersji językowej** rozporządzenia 2016/679 nie posłużono się terminem „przedsiębiorca", lecz **„przedsiębiorstwo"**. Przyczyną odmiennego brzmienia polskiej wersji językowej może być to, że polski ustawodawca w przepisach krajowych posługuje się pojęciem przedsiębiorcy, natomiast dla prawa unijnego charakterystyczne jest ujęcie przedmiotowe, czyli używanie pojęcia przedsiębiorstwa. Jest zatem prawdopodobne, że pojawił się **błąd w tłumaczeniu** art. 4 pkt 18 RODO.

> *WAŻNE!* Prowadzi to do komplikacji w stosowaniu art. 83 ust. 4–6 RODO, dotyczących wysokości kar pieniężnych. W polskiej wersji językowej RODO używa w nich pojęcia przedsiębiorstwa. Doprowadza to do wątpliwości, czy pojęcie to powinno być rozumiane zgodnie z art. 4 pkt 18 RODO.

Rozwiązanie powyższego problemu nie jest prostym zadaniem. Z jednej bowiem strony istnieje ugruntowane orzecznictwo TSUE wskazujące na **konieczność uwzględniania** w procesie wykładni rozporządzeń unijnych **wszystkich** ich **wersji językowych**. W przypadku wystąpienia sprzeczności między nimi należy uwzględniać ogólną systematykę i cel uregulowania, by dokonać wykładni przepisów. Nie można jednak zapominać, że art. 83 ust. 4–6 RODO to **przepisy sankcyjne**. W takich przypadkach TSUE wskazywał, że **nie można na podstawie innych wersji językowych pogarszać sytuacji podmiotu krajowego**, który opierał się na swojej wersji językowej. Można jednak zgłosić pewne wątpliwości co do możliwości przeniesienia tego orzecznictwa na art. 83 ust. 4–6 RODO. Nie określają one bowiem przesłanek zaistnienia podstaw do nałożenia sankcji, lecz wskazują wysokość tej sankcji. Kwestia ta być może znajdzie swoje rozstrzygnięcie w przyszłości właśnie w wyroku TSUE.

c. Osoba fizyczna, osoba prawna, spółki osobowe i zrzeszenia

147 Definicja przedsiębiorcy obejmuje osoby fizyczne, osoby prawne, spółki osobowe oraz zrzeszenia. Pod pojęciem **osoby fizycznej** należy rozumieć człowieka, przez **osoby prawne** – wszystkie podmioty, które zgodnie z prawem krajowym mają taki status. Przykładowo będą to: izby gospodarcze, spółki akcyjne, spółki z ograniczoną odpowiedzialnością, fundacje czy stowarzyszenia. Spółkami osobowymi będą natomiast spółka jawna, partnerska, komandytowa oraz komandytowo-akcyjna.
Większe problemy występują z określeniem znaczenia pojęcia zrzeszeń. Z uwagi na potrzebę takiego ujęcia art. 4 pkt 18 RODO, by obejmowało ono wszystkie podmioty, które zgodnie z prawem krajowym poszczególnych państw członkowskich mogą wykonywać działalność gospodarczą, **„zrzeszenia" należy rozumieć szeroko**.

> ***WAŻNE!*** Zrzeszeniami będą wszystkie inne podmioty uprawnione do prowadzenia działalności gospodarczej, a niebędące osobami fizycznymi, osobami prawnymi lub spółkami osobowymi.

W Polsce będą to:
– stowarzyszenia zwykłe oraz
– wspólnoty mieszkaniowe.

d. Prowadzenie działalności gospodarczej

148 Znaczenia tego pojęcia na gruncie RODO nie można poszukiwać w przepisach krajowych. Prawo unijne nie definiuje działalności gospodarczej. Natomiast TSUE w swoim orzecznictwie uznał za taką każdą **działalność sprowadzającą się do oferowania towarów lub usług na określonym rynku**.

e. Wymóg regularności

149 Z art. 4 pkt 18 RODO wynika, że prawodawca unijny zdecydował się, by w odniesieniu do **spółek osobowych oraz zrzeszeń** do ich kwalifikacji jako przedsiębiorcy **nie wystarczało samo prowadzenie działalności gospodarczej**. **Musi być ona regularna.** Zgodnie ze słownikowym znaczeniem tego pojęcia, regularny to taki, który powtarza się w jednakowych lub ściśle określonych odstępach. Takie ścisłe rozumienie analizowanego pojęcia nie byłoby jednak traf-

ne. Pozwalałoby ono bowiem na samodzielne decydowanie przez tę grupę podmiotów, czy chcą być kwalifikowane jako przedsiębiorcy. Wystarczałoby bowiem, aby zmieniały trochę odstępy czasu, w których prowadzą działalność gospodarczą.

WAŻNE! Wymóg regularności należy rozumieć jako wymóg powtarzalności działań, ale niekoniecznie podejmowanych w jednakowych lub ściśle określonych odstępach czasu.

PRZYKŁAD: Regularną działalnością gospodarczą będzie działalność prowadzona jedynie w wakacje przez spółkę osobową zajmującą się sprzedażą lodów w nadmorskiej miejscowości. Podobnie będzie w sytuacji, gdy spółka osobowa będzie sprzedawała jedzenie na festiwalu, który odbywa się raz w roku.

J. Grupa przedsiębiorstw

Witold Chomiczewski

Podstawa prawna: art. 4 pkt 19 RODO.

a. Znaczenie pojęcia

Grupa przedsiębiorstw to przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane. **150**

WAŻNE! Grupa przedsiębiorstw ma możliwość powołania jednego inspektora ochrony danych (art. 37 ust. 2 RODO), może uzyskać zatwierdzenie wiążących reguł korporacyjnych (art. 47 RODO), przekazywanie sobie danych osobowych do wewnętrznych celów administracyjnych może być prawnie usprawiedliwionym interesem przedsiębiorstw wchodzących w skład grupy (art. 6 ust. 1 lit. f w zw. z motywem 48 RODO). Grupa przedsiębiorstw może zatem korzystać z pewnych ułatwień w procesie stosowania RODO.

b. Sprawowanie kontroli

Sprawowanie kontroli jest elementem tworzącym grupę przedsiębiorstw. W motywie 37 RODO wyjaśniono, że chodzi o **wywieranie dominującego wpływu** na pozostałe przedsiębiorstwa. Może mieć to miejsce na skutek: **151**

– struktury właścicielskiej,
– udziału finansowego,
– przepisów regulujących działalność,
– uprawnień do nakazywania wdrożenia przepisów o ochronie danych osobowych.

Powyższe przyczyny zapewniające wywieranie dominującego wpływu są jedynie przykładowe.

WAŻNE! Wobec tego każda relacja między przedsiębiorstwami, która pozwala na sprawowanie kontroli jednemu nad innymi, będzie prowadziła do powstania grupy przedsiębiorstw w rozumieniu art. 4 pkt 19 RODO.

PRZYKŁAD: Może to być umowa, która zapewnia jednemu przedsiębiorstwu możliwość wywierania dominującego wpływu na inne przedsiębiorstwo czy też prawo do powoływania przeważającej liczby członków zarządu.

c. Ważna rola zasady rozliczalności

152 Z uwagi na opisane powyżej korzyści wynikające z bycia grupą przedsiębiorstw jej członkowie muszą pamiętać o przewidzianej w art. 5 ust. 2 RODO **zasadzie rozliczalności**. Zobowiązuje ona każdego administratora do zapewnienia sobie możliwości wykazania zgodności jego działań z RODO.

WAŻNE! To zatem członkowie grupy przedsiębiorstw będą musieli wykazać spełnienie warunku do takiej ich kwalifikacji na gruncie art. 4 pkt 19 RODO.

K. Usługa społeczeństwa informacyjnego

Dominik Lubasz

Podstawa prawna: art. 4 pkt 25 RODO.

a. Znaczenie pojęcia

153 Rozporządzenie nie definiuje pojęcia **usługi społeczeństwa informacyjnego** (*information society service*). Odsyła natomiast w art. 4 pkt 25 RODO do **dyrektywy 2015/1535 ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego**. Zgodnie z art. 1 ust. 1 lit. b dyrektywy 2015/1535 usługa społeczeństwa informacyjnego obejmuje każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie usługobiorcy.

WAŻNE! **Usługa społeczeństwa informacyjnego** to **każda usługa** (przesłanki łączne z art. 1 ust. 1 lit. b dyrektywy 2015/1535):
– **normalnie świadczona za wynagrodzeniem**,
– **na odległość**,
– **drogą elektroniczną i**
– **na indywidualne żądanie usługobiorcy**.

b. Odpłatność

Pierwszym elementem kwalifikacyjnym danej usługi jako usługi społeczeństwa informacyjnego jest **odpłatność**, co nie oznacza jednak wymogu opłacenia usługi przez jej odbiorcę. Wynagrodzenie związane ze świadczeniem usług społeczeństwa informacyjnego nie musi ponadto w każdym przypadku występować, przesłanka ta nie ma bowiem charakteru bezwzględnego, co wynika z zawartego w art. 1 ust. 1 lit. b dyrektywy **2015/1535** słowa *normally*. 154
Przesłanka odpłatności była przedmiotem analizy Trybunału Sprawiedliwości w kolejnych sprawach w zakresie dotyczącym różnych przepisów unijnych, w których formułowana była ta przesłanka. Z wypowiedzi Trybunału można jednak wyciągnąć uogólniające wnioski, że dla spełnienia omawianej przesłanki wystarczy, że dane świadczenie ma charakter ekonomiczny szeroko rozumiany i nie ma znaczenia źródło finansowania, np. czy środki pokrywające koszt usługi pochodzą z reklamy, dotacji lub innych źródeł publicznych itp. W konsekwencji stanowisko Trybunału Sprawiedliwości istotnie ogranicza znaczenie prawne przesłanki odpłatności. Takie podejście jest też koherentne z przyjętą przez prawodawcę unijnego koncepcją odpłatności za treści cyfrowe w dyrektywie 2019/770, w której cena definiowana jest jako pieniądz lub cyfrowe odwzorowanie wartości, mogące obejmować bony elektroniczne, e-kupony czy waluty wirtualne oraz zgodnie z którą dopuszczona została płatność danymi osobowymi jako świadczeniem wzajemnym.

> ***WAŻNE!*** Stanowisko Trybunału Sprawiedliwości istotnie ogranicza znaczenie prawne przesłanki odpłatności, kwalifikując jako usługę społeczeństwa informacyjnego usługę spełniającą pozostałe przesłanki kwalifikacyjne, jeśli tylko jej świadczenie przynosi korzyść ekonomiczną usługodawcy, przy czym korzyść ta nie musi być bezpośrednio związana z usługą i pochodzić od użytkownika (tak m.in. wyrok TS z 26.04.1988 r., 352/85, Bond van Adverteerders i in. v. Państwo Niderlandzkie, EU:C:1988:196; wyrok TS z 7.12.1993 r., C-109/92, Stephan Max Wirth v. Landeshauptstadt Hannover, EU:C:1993:916; wyrok TS z 12.07.2001 r., C-157/99, B.S.M. Geraets-Smits v. Stichting Ziekenfonds VGZ oraz H.T.M. Peerbooms v. Stichting CZ Groep Zorgverzekeringen, EU:C:2001:404, oraz wyrok TS z 26.06.2003 r., C-422/01, Försäkringsaktiebolaget Skandia (publ) i Ola Ramstedt v. Riksskatteverket, EU:C:2003:380).

c. Świadczenie na odległość

Wymóg świadczenia usługi **na odległość** oznacza świadczenie usługi bez równoczesnej obecności stron (art. 1 ust. 1 lit. b ppkt i dyrektywy **2015/1535**). Wymóg braku jednoczesnej obecności stron powinien być rozumiany jako brak ich jednoczesnej fizycznej obecności zapewniającej bezpośredni kontakt w danym miejscu w chwili wykonania usługi. Decydujący jest tu **moment wykonania usługi**, a nie jej zamówienia (zawarcia umowy), jak w wypadku umów zawieranych na odległość w rozumieniu art. 2 pkt 8 dyrektywy 2011/83. Z tego względu usługa polegająca np. na zapewnieniu dostępu do Internetu, nawet jeżeli będzie zamówiona w punkcie sprzedaży usługodawcy osobiście przez usługobiorcę, zachowa status usługi świadczonej drogą elektroniczną. Jej wykonywanie będzie odbywało się bowiem bez jednoczesnej obecności stron. Pojawia się pytanie, czy omawiana przesłanka będzie spełniona w sytuacji, gdy usługodawca oraz usługobiorca znajdują się wprawdzie fizycznie w jednym miejscu, ale usługobiorca skorzysta wyłącznie z udostępnianego w danym miejscu przez usługodawcę komputera z dostępem do Internetu w celu wykonania usługi. W takim przypadku rozstrzygający powinien być nie tyle związek miejscowy, ile osobowy, a zatem bezpośredni kontakt 155

pomiędzy stronami w celu wykonania usługi bądź jego brak. Znajdowanie się w tym samym miejscu bez nawiązania bezpośredniego kontaktu między stronami w celu wykonania usługi nie powinno wykluczać takiego sposobu świadczenia usługi z zakresu zastosowania ustawy o świadczeniu usług drogą elektroniczną. W przykładowym wykazie usług, które nie spełniają tej przesłanki, zawartym w załączniku I do dyrektywy 2015/1535, wskazano m.in. na rezerwację biletu lotniczego w biurze podróży przy fizycznej obecności klienta za pomocą sieci komputerowej czy też udostępnienie gier elektronicznych w salonie przy fizycznej obecności użytkownika.

d. Świadczenie drogą elektroniczną

156 Usługa będzie świadczona **drogą elektroniczną**, zgodnie z art. 1 ust. 1 lit. b ppkt ii dyrektywy **2015/1535**, jeżeli jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania (włącznie z kompresją cyfrową) oraz przechowywania danych i jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych. Przesłanka ta kreuje wymóg braku substratu materialnego usługi, co ma daleko idące konsekwencje dla zakresu zastosowania analizowanego pojęcia. O ile bowiem pojęciem świadczenia usługi drogą elektroniczną objęte będą działania polegające na zawieraniu umów *on-line*, w tym umów dotyczących sprzedaży towarów, o tyle sama dostawa towarów, a także wymagania odnoszące się do towarów definicji tej podlegać nie będą. W powołanym w załączniku I do dyrektywy 2015/1535 jako **nieświadczone drogą elektroniczną** wymieniono usługi o charakterze materialnym, nawet jeżeli świadczone są z wykorzystaniem urządzeń elektronicznych, jak dystrybucja banknotów i biletów przez automaty (banknoty, bilety kolejowe), czy usługi *off-line*, jak dystrybucja CD-ROM lub oprogramowania na dyskietkach, a także usługi, które nie są świadczone z wykorzystaniem elektronicznego systemu przetwarzania i przechowywania danych, w szczególności usługi telefonii głosowej, usługi telefaksowe/teleksowe czy telefoniczne/telefaksowe porady prawne lub telefoniczny/telefaksowy marketing bezpośredni.

> *WAŻNE!* Usługa społeczeństwa informacyjnego **nie ma substratu materialnego** i w całości **musi być świadczona drogą elektroniczną** (zob. wyrok TS z 7.12.2010 r., C-108/09, Ker-Optika bt v. ÀNTSZ Dél-dunántúli Regionális Intézete, EU:C:2010:725).

e. Świadczenie na indywidualne żądanie

157 Świadczenie usługi na indywidualne żądanie oznacza, że przesyłanie danych powinno być poprzedzone zindywidualizowanym żądaniem (zgodnie z art. 1 ust. 1 lit. b ppkt iii dyrektywy **2015/1535)**. Zindywidualizowane żądanie formułowane jest przez usługobiorcę i znajduje się w jego sferze wolicjonalnej. To usługobiorca bowiem podejmuje decyzję (obejmuje żądaniem), m.in. kiedy, gdzie oraz o jakiej konkretnej treści lub zawartości usługa ma być świadczona. Omawiana przesłanka będzie spełniona w odniesieniu do takich usług, jak np. *video on demand*, wysłanie wiadomości e-mail i korzystanie z portalu społecznościowego. Usługa nie jest natomiast świadczona na indywidualne żądanie w przypadku przesyłania danych bez indywidualnego zamówienia i przeznaczonych do równoczesnego odbioru przez nieograniczoną liczbę odbiorców (transmisja „z punktu do wielu punktów"), charakterystycznego dla przekazów telewizyjnych lub radiowych oraz wysyłania niezamówionej informacji handlowej.

L. Podejście oparte na ryzyku

Dominik Lubasz

Podstawa prawna: art. 24, 25, 30, 32, 33–36 RODO.

a. Znaczenie pojęcia

158 **Podejście oparte na ryzyku** (*risk-based approach*) jest podstawą dla przyjętej w rozporządzeniu 2016/679 konstrukcji obowiązków, które są nakładane na administratorów i podmioty przetwarzające. Pojęcie to nie zostało jednak zamieszczone w słowniku zawartym w art. 4 RODO. Prawodawca unijny, odchodząc od sztywnych, nierelatywizowanych co do zakresu, potrzeb i zagrożeń ram ochrony, zdecydował się zrelatywizować i uelastycznić regulację przez uwzględnienie perspektywy podmiotów zobowiązanych, podkreślając jednocześnie jej **neutralny technologicznie charakter**. W konsekwencji to charakter, kontekst, cel i zakres przetwarzania danych osobowych przez konkretny podmiot są podstawą oceny zgodności z przepisami RODO podjętej przez ten podmiot decyzji co do prawidłowego wdrożenia środków organizacyjnych i prawnych w celu zabezpieczenia praw i wolności osób, których dane są przetwarzane. Decyzja ta oparta jest na wykonanej przez te podmioty **ocenie ryzyka związanego z przetwarzaniem danych** (motyw 74 RODO).
Wskazane podejście stanowi klucz do zrozumienia i wyznaczenia zakresu obowiązków tychże podmiotów nakładanych mocą rozporządzenia 2016/679 i podstawową odmienność od dotychczasowego stanu prawnego narzucającego jednolite rozwiązania w zakresie dokumentacji i zabezpieczeń, niezależne od wielkości samego administratora czy też zakresu przetwarzania przez niego danych osobowych oraz infrastruktury teleinformatycznej.

b. Pojęcie ryzyka

159 Pojęcie ryzyka nie zostało zdefiniowane w przepisach rozporządzenia 2016/679.

> *WAŻNE!* Według ogólnych definicji **ryzyko** należy rozumieć jako zagrożenie lub szansę wystąpienia zdarzenia, które może pociągnąć za sobą możliwość wystąpienia zarówno negatywnych, jak i pozytywnych konsekwencji.

160 W obrocie występują również definicje szczegółowe, np. zawarta w normach ISO. Dla przykładu w normie ISO/IEC 31000 *Zarządzanie ryzykiem. Zasady i wytyczne* **ryzyko jest definiowane jako wpływ niepewności na cele, który powoduje pozytywne lub negatywne odchylenie od oczekiwań**. Cele zaś mogą dotyczyć różnych aspektów, np. finansowych lub biznesowych. W doktrynie z kolei definiuje się **ryzyko jako scenariusz opisujący konkretne zdarzenie i jego konsekwencje (dla praw i wolności osób, których dane są przetwarzane), oszacowane pod kątem ich dotkliwości oraz prawdopodobieństwa**.

161 Należy jednak zwrócić uwagę, że w rozporządzeniu 2016/679 ryzyko, rozumiane jako zagrożenie wystąpienia konsekwencji, **musi być nakierowane na ocenę możliwości powstania**

negatywnych skutków dla praw i wolności osób, których dane dotyczą (zob. nr 167), i na to powinna być ukierunkowana każdorazowo dokonywana przez podmioty zobowiązane analiza ryzyka.

c. Szacowanie i analiza ryzyka

162 Zgodnie z rozporządzeniem 2016/679 decyzja co do wyboru środków organizacyjnych i technicznych mających na celu zapewnienie zgodności z rozporządzeniem, a także bezpieczeństwo przetwarzania powinna uwzględniać w sposób adekwatny i proporcjonalny naturę, zakres, kontekst i cel przetwarzania danych oraz wynikające z tego ryzyka dla praw i wolności podmiotów danych. W niektórych przypadkach powinien on również brać pod uwagę koszty wdrożenia oraz stan wiedzy technicznej w zakresie możliwych do wdrożenia rozwiązań technicznych czy organizacyjnych.

> *WAŻNE!* **Zakres obowiązków administratora zależy od dokonanej oceny ryzyka związanego z przetwarzaniem danych osobowych.**

Dobór konkretnych środków i zakresu zabezpieczeń wdrażanych przez administratorów nie powinien mieć charakteru jednolitego, niezależnego od zakresu, formy, celu i ilości przetwarzanych danych.

163 Prawodawca unijny nie tylko nie narzuca w przepisach rozporządzenia 2016/679, ale także nie proponuje metod analizy ryzyka. Tym samym wybór metody należy do administratora i zależny jest m.in. od jego możliwości organizacyjnych i finansowych, kontekstu przetwarzania danych, ekspozycji organizacji na ryzyka oraz związku głównego przedmiotu działalności z przetwarzaniem danych osobowych, a wreszcie osobistych preferencji.
Metody analizy ryzyka można podzielić na:
– jakościowe,
– ilościowe i
– mieszane.

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

Metoda jakościowa jest prostsza, tańsza i mniej sformalizowana, jednak także mniej precyzyjna. **Metody ilościowe** charakteryzują się większą szczegółowością i precyzją, dlatego częściej stosuje się je w przypadku poważnych typów ryzyka.

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

> *WAŻNE!* Na szacowanie ryzyka składają się:
> 1) identyfikowanie ryzyka,
> 2) analiza ryzyka,
> 3) ocena poziomu ryzyka.

165 Zasadniczymi celami szacowania są określenie wartości aktywów informacyjnych, zidentyfikowanie zagrożeń, podatności, a także zabezpieczeń i ich wpływu na zidentyfikowane ryzyko, jak również możliwe następstwa, priorytety i kolejność uzyskanych typów ryzyka [Polska norma PN-ISO/EIC 27005. *Technika informatyczna. Technika bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji*, s. 20]. Szacowanie ryzyka powinno być przeprowadzone z zastosowaniem **jednej, z góry przyjętej przez administratora metody, uwzględniającej wszystkie kryteria**, które powinny zostać wzięte pod uwagę przy ocenie ryzyka, oraz perspektywę podmiotów danych, jako wymóg wyraźnie wynikający z przepisów rozporządzenia 2016/679. Szacowanie ryzyka powinno mieć charakter **obiektywny**. Co więcej, zastosowana metoda analizy ryzyka i jej szacunkowe wyniki powinny zostać udokumentowane w taki sposób, aby podmiot niezależny, w szczególności organ nadzoru, mógł odtworzyć proces analityczny administratora oraz ocenić, czy dokonując analizy, administrator wziął pod uwagę niezbędne kryteria i okoliczności, w jaki sposób je ocenił i z jakiej przyczyny doszedł do określonych wniosków. **Dokumentowanie lub raportowanie** przeprowadzanej analizy powinno obejmować każdy jej etap, co umożliwia ocenę przeprowadzonej analizy pod kątem jej rzetelności i miarodajności. Tego rodzaju dokumentowanie pozwala także na wykazanie zgodności działania administratora z obowiązującą na gruncie RODO zasadą rozliczalności.

166 Podpowiedzi dotyczących wyboru metody analitycznej można szukać m.in. w:
1) wytycznych Grupy Roboczej Art. 29 (obecnie Europejskiej Rady Ochrony Danych) dotyczących oceny skutków dla ochrony danych oraz pomagających ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, przyjętych 4.04.2017 r., dokument WP 248 rev.1, https://uodo.gov.pl/pl/10/9 (dostęp: 1.09.2021 r.);
2) opracowaniach polskiego organu nadzorczego – Poradnik – *Jak rozumieć podejście oparte na ryzyku i Jak stosować podejście oparte na ryzyku* (https://uodo.gov.pl/pl/123/208, dostęp: 1.09.2021 r);
3) normach ISO z rzędu 27000, w szczególności normie ISO/IEC 27005. *Technika informatyczna. Technika bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji* stanowiącej rozszerzenie normy ISO/IEC 27001 – w zakresie dotyczącym bezpieczeństwa opartego na analizie ryzyka, z tym zastrzeżeniem, że na podstawie tych norm badane jest ryzyko związane z zapewnieniem bezpieczeństwa informacji, a nie ryzyko przetwarzania dla praw i wolności podmiotów danych;
4) normie ISO/IEC 27701:2019. *Techniki bezpieczeństwa – Rozszerzenie do ISO/IEC 27001 i ISO/IEC 27002 – Zarządzanie informacjami o prywatności – wytyczne i wymagania*;
5) normie ISO/IEC 29134:2017. *Technika informatyczna. Techniki bezpieczeństwa. Wytyczne dotyczące oceny skutków dla prywatności wraz z normami skorelowanymi 27000 – systemy zarządzania bezpieczeństwem informacji, 29100 – ramy prywatności*;
6) opracowaniach ENISA – np. *Reinforcing trust and security in the area of electronic communications and on-line services Sketching the notion of "state-of-the-art" for SMEs in security of personal data processings*, https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-in-the-area-of-electronic-communications-and-online-services (dostęp: 20.07.2021 r.).

PRZYKŁAD: Możliwe jest także wykorzystanie metodologii, na których oparte jest działanie aplikacji analitycznych PIA (*privacy impact assessment*), np. opracowanej przez francuski organ nadzorczy CNIL – https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment (dostęp: 20.07.2021 r.) – lub opartej na normie ISO/IEC 29134:2017. *Technika informatyczna. Technika Bezpieczeństwa. Wytyczne dotyczące oceny skutków dla prywatności* – aplikacji GDPR Risk Tracker – https://app.gdprrisktracker.pl (dostęp: 20.07.2021 r.).

d. Obowiązki oparte na analizie ryzyka

167 Większość obowiązków wynikających z rozporządzenia 2016/679, opartych na analizie ryzyka, **adresowana jest do administratorów**.

> WAŻNE! Z w tym kontekście **podejście oparte na ryzyku jest przede wszystkim istotnym elementem**:
> – ogólnego obowiązku zapewnienia zgodności z rozporządzeniem, o którym mowa w art. 24 RODO (zob. nr 468);
> – uwzględniania ochrony danych już w fazie projektowania (*data protection by design*) w myśl art. 25 ust. 1 RODO oraz realizacji zasady domyślnej ochrony danych (*data protection by default*) zgodnie z art. 25 ust. 2 RODO (zob. nr 476 i n., 489);
> – oceny skutków planowanych operacji przetwarzania dla ochrony danych (*data protection impact assessment*) oraz uprzednich konsultacji z organem nadzoru, o których mowa odpowiednio w art. 35 i 36 RODO (zob. nr 465, 517 i n.).

Prawodawca unijny sformułował jednak również obowiązki bazujące na analizie ryzyka, których adresatem są zarówno administratorzy, jak i podmioty przetwarzające. Należą do nich:
– sporządzanie określonej przepisami dokumentacji przetwarzania ujętej w ramy art. 30 RODO (zob. nr 507);
– zapewnienie bezpieczeństwa przetwarzania, w szczególności wskazanego w art. 32 RODO (zob. nr 582, 721).

> WAŻNE! Znaczenie podejścia opartego na ryzyku we wdrożeniu podkreśla Prezes UODO w kolejnych decyzjach nakładających administracyjne kary pieniężne. Wskazuje w nich na kluczowe aspekty, tj. kompletność analizy ryzyka, ocenę adekwatności wdrażanych środków technicznych i organizacyjnych zarówno w stosunku do ryzyk o niskim poziomie, jak i do wysokopoziomowych, regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, rolę inspektora ochrony danych w kontekście przeprowadzania analizy ryzyka i ocenę skutków dla ochrony danych, a wreszcie powtarzające się uchybienia w zakresie prawidłowego dokumentowania analizy ryzyka (zob. decyzje: z 10.09.2019 r., ZSPR.421.2.2019; z 18.10.2019 r., ZSPU.421.3.2019; z 21.08.2020 r., ZSOŚS.421.25.2019; z 3.12.2020 r., DKN.5112.1.2020; z 11.02.2021 r., DKN.5130.2024.2020, https://uodo.gov.pl/decyzje, dostęp: 20.07.2021 r.).
> Znaczenie wymogu analizy ryzyka było również przedmiotem wykładni w orzecznictwie sądów administracyjnych. Zob. przykładowo wyrok WSA w Warszawie z 26.08.2020 r., II SA/Wa 2826/19, LEX nr 3067899, w którym w kontekście art. 32 RODO wskazane zostało, że „nie wymaga od administratora danych wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych. Taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różną wysokością", a także że „[p]rzyjęte środki mają mieć charakter skuteczny, w konkretnych przypadkach niektóre środki będą musiały być środkami o charakterze niwelującym niskie ryzyko, inne – muszą niwelować ryzyko wysokie, ważne jednak jest, aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka".

Wskazówki interpretacyjne zawarte zostały także w wyroku WSA w Warszawie z 3.09.2020 r., II SA/Wa 2559/19, LEX nr 3077973, w którym stwierdzono, że „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**. Administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych **i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka**".

e. Uwzględnienie praw i wolności podmiotów danych

Analiza ryzyka wymagana przepisami rozporządzenia 2016/679 musi być przeprowadzana w kontekście praw i wolności osób, których dane dotyczą, oraz potencjału naruszenia tychże praw i wolności (zob. motyw 75 RODO). Niemożliwe jest oderwanie oceny ryzyka od ustalenia potencjalnych skutków **wystąpienia ryzyka dla praw i wolności podmiotów danych**. Co więcej, na ryzyko o różnym prawdopodobieństwie i wadze wpływać może wiele okoliczności. W szczególności należy tu wskazać na: 168

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

Do wzrostu ryzyka przyczynia się przetwarzanie szczególnych kategorii, zwanych danymi wrażliwymi, oraz danych dotyczących wyroków skazujących i czynów zabronionych, tj. danych, o których mowa w art. 9 ust. 1 i art. 10 RODO. Istotna wartość tych danych, wynikająca z faktu dotykania sfer o podwyższonej wrażliwości z perspektywy prywatności, wpływać będzie na wynikowy poziom ryzyka poprzez zwiększenie wagi danych. Podobna sytuacja zachodzi, gdy administrator przetwarza dane osób, które wymagają szczególnej opieki, np. dzieci. Wykonywane na danych operacje, takie jak profilowanie podmiotów danych w oparciu o z góry przyjęte kryteria, również może powodować zwiększenie ryzyka naruszenia praw i wolności tychże podmiotów.

PRZYKŁAD: Ryzyko naruszenia praw lub wolności osób może wynikać z przetwarzania danych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności:

a) jeżeli przetwarzanie może poskutkować:
   – dyskryminacją,
   – kradzieżą tożsamości lub oszustwem dotyczącym tożsamości,
   – stratą finansową,
   – naruszeniem dobrego imienia,
   – naruszeniem poufności danych osobowych chronionych tajemnicą zawodową,
   – nieuprawnionym odwróceniem pseudonimizacji,
   – wszelką inną znaczną szkodą gospodarczą lub społeczną;
b) jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;

c) jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa;
d) jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych;
e) jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, zwłaszcza dzieci;
f) jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

M. Naruszenie ochrony danych osobowych

Dominik Lubasz

Podstawa prawna: art. 4 pkt 12 RODO.

a. Pojęcie naruszenia ochrony danych osobowych

169 W art. 4 pkt 12 RODO prawodawca unijny zdefiniował **pojęcie naruszenia ochrony danych osobowych**. Zgodnie z powołanym przepisem **naruszenie ochrony danych osobowych** to naruszenie bezpieczeństwa, którego efektem jest przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

b. Znaczenie pojęcia

170 Prezentowana definicja ma **istotne znaczenie dla stosowania przepisów art. 33 i 34** (zob. szerzej w punkcie dotyczącym naruszeń – nr 526 i n.). W związku z naruszeniem ochrony danych nałożone zostają bowiem na administratorów obowiązki, m.in. wprowadzenia procedur umożliwiających stwierdzanie i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych, a w przypadku zaistnienia okoliczności wskazanych w powołanych przepisach – zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienia osoby, której dane dotyczą, o takim naruszeniu, a także przeciwdziałania skutkom naruszenia i zapobiegania im w przyszłości. Również podmioty przetwarzające stają się adresatami związanych z naruszeniem ochrony danych osobowych obowiązków, w szczególności obowiązku powiadomienia adekwatnych administratorów o naruszeniu ochrony danych osobowych przetwarzanych na ich zlecenie. Należy jednak zwrócić uwagę, że podmioty przetwarzające nie mają obowiązku bezpośredniej notyfikacji naruszenia ani do organu nadzorczego, ani do podmiotu danych.

c. Przesłanki determinujące zaistnienie naruszenia

171 Dla zaistnienia naruszenia danych osobowych muszą być spełnione **kumulatywnie** następujące **przesłanki**:
- po pierwsze, musi **zaistnieć naruszenie bezpieczeństwa**;
- po drugie, naruszenie musi dotyczyć danych osobowych podmiotu przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- po trzecie, **skutkiem** tego naruszenia muszą być **przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do przetwarzanych danych osobowych**.

172 **Naruszenie bezpieczeństwa** to każde zdarzenie, w którym organizacyjne lub techniczne środki zabezpieczenia danych osobowych zawodzą. Chodzi o środki, do których wdrożenia zgodnie z art. 32 RODO zarówno administrator, jak i podmiot przetwarzający są zobowiązani, a których celem ma być w szczególności ochrona przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Przy doborze odpowiednich środków organizacyjnych i technicznych adresaci normy powinni uwzględnić stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.
Naruszenia bezpieczeństwa można odnosić jedynie do środków rzeczywiście wdrożonych przez danego administratora, a nie tych, które powinien był wdrożyć. Ocena naruszenia musi się bowiem odnosić do stanu rzeczywistego, a nie hipotetycznego.

> *WAŻNE!* Dla zaistnienia tak rozumianego naruszenia bezpieczeństwa **nie ma znaczenia**, czy dojdzie do niego w wyniku **umyślnego, czy nieumyślnego działania**. Istotne jest jedynie **obiektywne wystąpienie naruszenia**.

Warto również podkreślić, że Prezes Urzędu Ochrony Danych Osobowych w decyzji z 9.12.2020 r., DKN.5131.5.2020, https://uodo.gov.pl/decyzje (dostęp: 20.07.2021 r.), uznał, że z naruszeniem bezpieczeństwa w rozumieniu art. 4 pkt 12 RODO w zakresie poufności będziemy mieli do czynienia również wtedy, gdy do naruszenia ochrony danych osobowych doszło, ponieważ to sam podmiot danych podał administratorowi błędne dane (w sprawie adres poczty elektronicznej) do komunikacji.

d. Kategorie skutków naruszenia bezpieczeństwa

173 **Efektem naruszenia bezpieczeństwa** musi być przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Wymienione skutki można podzielić na **trzy osobne kategorie:**
1) **naruszenie poufności danych**,
2) **naruszenie integralności** danych oraz
3) **naruszenie dostępności** danych.

W zależności od naruszenia może ono obejmować jedną lub łącznie kilka powyższych kategorii.

174 Przez pojęcie **naruszenia poufności danych** należy rozumieć takie naruszenie, które prowadzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych.

Pojęcie **ujawnienia** oznacza przesłanie, rozpowszechnienie lub udostępnienie danych. **„Dostęp"** to z kolei wszelkie sytuacje, w których osoba trzecia uzyskuje dostęp do danych osobowych w wyniku swojego własnego działania, a nie w wyniku działania osoby realizującej przetwarzanie.

PRZYKŁAD: Naruszeniem poufności danych może być przypadkowe wysłanie danych klienta do niewłaściwego działu bądź uzyskanie dostępu do danych przez osobę nieupoważnioną wskutek ataku hakerskiego.

Ujawnienie danych osobowych lub dostęp do nich będą relewantne prawnie dopiero w sytuacji, gdy dojdzie do nich **w sposób nieuprawniony**. Kluczowe jest zatem zbadanie zarówno tego, czy administrator mógł ujawnić dane osobie trzeciej (posiadał stosowną przesłankę legalizacyjną z art. 6 ust. 1 lub art. 9 ust. 2 RODO lub też podpisaną umowę powierzenia przetwarzania, lub też nastąpiło to w obszarze, nad którym sprawuje kontrolę, osobie, której ujawnienie może nastąpić i za którą odpowiada, np. pracownikowi), jak i tego, czy osoba, która uzyskała dostęp do danych, miała do tego uprawnienia (np. na podstawie art. 32 ust. 4 RODO).

175 Do **kategorii naruszenia integralności danych osobowych** należą naruszenia, w rezultacie których dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych.

PRZYKŁAD: Naruszeniem integralności danych będzie modyfikacja danych, która nastąpiła celowo i sprzecznie z prawem lub przypadkowo, ale sprzecznie z przeznaczeniem.

176 Do **kategorii naruszenia dostępności danych** zalicza się **przypadkowy lub nieuprawniony dostęp do nich**. Pojęcie dostępu zawiera się w pojęciu dostępności. Grupa Robocza Art. 29 w wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, przyjętych 3.10.2017 r., dokument WP 250 rev. 01, https://www.uodo.gov.pl/pl/3/1345 (dostęp: 1.09.2021 r.) wskazuje z kolei, że dostępność to zapewnienie możliwości uzyskania terminowego i niezawodnego dostępu do informacji oraz możliwości terminowego i niezawodnego korzystania z informacji. Za naruszenie utraty dostępności należy uznać sytuację, w której np. doszło do przypadkowego usunięcia danych bądź ich usunięcia przez nieuprawnioną osobę, jak również awarię systemu zasilania skutkującą utratą dostępu do danych osobowych. Naruszenie dostępności danych może wystąpić zarówno wtedy, gdy skutkuje tymczasową utratą dostępu, jak i wtedy, gdy skutkuje trwałą utratą lub zniszczeniem danych osobowych.

WAŻNE! Nie każda tymczasowa niedostępność danych będzie stanowiła naruszenie dostępności. Do naruszenia dochodzi w sytuacji, gdy czasowa utrata danych może stanowić ryzyko dla praw lub wolności osób fizycznych.

PRZYKŁAD: Przypadkiem tymczasowej utraty danych, który stanowić będzie naruszenie ich dostępności, jest utrata przez szpital dostępu do kluczowych danych medycznych pacjentów, np. na skutek ataku DDoS lub przerwy w dostawie prądu.

Do kategorii naruszenia dostępności danych zaliczyć można również ich zniszczenie lub utracenie, zarówno przypadkowe, jak i sprzeczne z prawem. Do **zniszczenia danych osobowych** dochodzi w sytuacji, gdy dane już nie istnieją lub przestały istnieć w takiej postaci, w jakiej mogłyby zostać w jakikolwiek sposób wykorzystane. **Utracenie danych osobowych** może

oznaczać ich usunięcie lub utratę kontroli nad nimi przez administratora, w sytuacji gdy stracił on do nich dostęp bądź nie znajdują się one już w jego posiadaniu. Zmodyfikowane dane osobowe zaś to takie, które zostały zniekształcone lub stały się niekompletne.

PRZYKŁAD: Do utraty danych osobowych dochodzi w przypadku kradzieży urządzenia, na którym znajduje się kopia bazy danych klientów administratora.

PRZYKŁAD: Do utraty danych osobowych dochodzi w przypadku zagubienia urządzenia zawierającego dane, których nie da się odzyskać z kopii zapasowej.

PRZYKŁAD: Do utraty danych osobowych dochodzi w przypadku intencjonalnego usunięcia danych przez osobę uzyskującą dostęp do bazy danych w sposób nieuprawniony.

e. Przesłanka danych osobowych

177 **Wszystkie postaci operacji muszą dotyczyć danych osobowych.** Jest to oczywisty i wprost wynikający z przepisu element pojęcia naruszenia ochrony danych osobowych. Jeżeli zatem dojdzie do naruszenia zasad bezpieczeństwa w rozumieniu przepisu art. 4 pkt 12 RODO, jednak w jego konsekwencji zostaną utracone dane, które nie są danymi osobowymi, wówczas nie dojdzie do spełnienia przesłanek pozwalających uznać, że mamy do czynienia z naruszeniem ochrony danych osobowych.

N. Organ nadzorczy

Witold Chomiczewski

Podstawa prawna: art. 4 pkt 21 RODO.

a. Znaczenie pojęcia

178 Organem nadzorczym jest niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO.
Powołanie organu nadzorczego jest obowiązkiem każdego z państw członkowskich. Jego zadaniem jest monitorowanie stosowania rozporządzenia 2016/679. W Polsce takim organem jest **Prezes Urzędu Ochrony Danych Osobowych**.

b. Niezależność

179 Organ nadzorczy musi być **niezależny**. Sposób rozumienia przez prawodawcę unijnego niezależności wyjaśnia art. 52 RODO. Jest to przede wszystkim **wolność od jakichkolwiek wpły-**

wów z zewnątrz, czy to bezpośrednich, czy to pośrednich. Organ nadzorczy nie może również otrzymywać od nikogo instrukcji. Poza tym, piastun organu nadzorczego nie może wykonywać zajęć zarobkowych ani niezarobkowych sprzecznych ze swoimi obowiązkami. Dodatkowo państwa członkowskie są zobowiązane zapewnić organowi nadzorczemu odpowiednie zasoby kadrowe, techniczne i finansowe oraz pomieszczenia i infrastrukturę niezbędne do skutecznego działania. Organ nadzorczy musi mieć również swobodę w doborze swojego personelu, a kontrola finansowa organu nadzorczego nie może naruszać jego niezależności.

180 **Polski ustawodawca przewidział rozwiązania zmierzające do zapewnienia niezależności Prezesa UODO.** Z art. 34 ust. 5 u.o.d.o. wynika, że organ nadzorczy **podlega jedynie ustawie**, czyli nie jest związany żadnymi zewnętrznymi decyzjami, sugestiami czy poleceniami dotyczącymi sposobu wykonywania swoich zadań. **Gwarancją niezależności** jest również:
- powoływanie i odwoływanie Prezesa UODO przez Sejm za zgodą Senatu,
- czteroletnia kadencja i
- określone w ustawie przypadki dające możliwość odwołania ze stanowiska przed upływem kadencji.

Niezależność jest też zapewniana przez przewidziany w art. 37 u.o.d.o. **zakaz**:
- zajmowania innego stanowiska,
- wykonywania innych zajęć zarobkowych lub niezarobkowych sprzecznych z obowiązkami organu nadzorczego.

Dodatkowo zakazano: przynależności do partii politycznej, związku zawodowego, jak i prowadzenia działalności publicznej, której nie można pogodzić z godnością urzędu Prezesa UODO. Kolejną z gwarancji niezależności w sprawowaniu swojej funkcji jest **immunitet formalny** przewidziany w art. 38 u.o.d.o.

c. Wymogi powołania na stanowisko Prezesa UODO

181 Warunki, które musi spełniać kandydat na stanowisko Prezesa UODO, zostały określone przez polskiego ustawodawcę w art. 34 ust. 4 u.o.d.o. Zgodnie z tym przepisem przyszły piastun tego organu musi:
- być obywatelem polskim,
- posiadać wyższe wykształcenie,
- wyróżniać się wiedzą prawniczą i doświadczeniem z zakresu ochrony danych osobowych,
- korzystać z pełni praw publicznych,
- nie być skazany prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe oraz
- posiadać nieposzlakowaną opinię.

Wszystkie te **warunki muszą być spełnione łącznie**.

d. Właściwość

182 Organ nadzorczy jest właściwy do **wypełniania zadań i wykonywania uprawnień powierzonych mu zgodnie z RODO**. Zadania te zostały określone w art. 57 RODO i należą do nich m.in.:
- monitorowanie i egzekwowanie stosowania rozporządzenia 2016/679,
- upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o spoczywających na nich obowiązkach czy
- zatwierdzanie wiążących reguł korporacyjnych.

4. Zasady dotyczące przetwarzania danych osobowych

Dominik Lubasz

Podstawa prawna: art. 5 RODO.

A. Wprowadzenie

W art. 5 RODO sformułowano podstawowe zasady dotyczące przetwarzania danych osobowych. 183

WAŻNE! Katalog zasad dotyczących przetwarzania danych osobowych:
1) zasada legalności i rzetelności,
2) zasada przejrzystości,
3) zasada ograniczenia celu,
4) zasada minimalizacji danych,
5) zasada prawidłowości,
6) zasada ograniczenia przechowywania,
7) zasada integralności i poufności,
8) zasada rozliczalności.

Określone w art. 5 zasady mają **charakter nadrzędny** w stosunku do pozostałych przepisów rozporządzenia, w tym kształtujących zarówno prawa podmiotów danych, jak i obowiązki administratorów i podmiotów przetwarzających, oraz stanowią **trzon dla ich wykładni**. Determinują one bowiem zakres i sposób realizacji obowiązków informacyjnych, związanych z transparentnością procesów przetwarzania, ocenę legalności przetwarzania czy też wreszcie bezpieczeństwo przetwarzania. Część z zasad przetwarzania była już znana na gruncie dyrektywy 95/46, jednakże ich katalog ulega istotnemu rozszerzeniu, co ma być wyrazem woli zapewnienia jak najpełniejszej realizacji celów rozporządzenia, w szczególności osiągnięcia wysokiego poziomu ochrony praw osób fizycznych, zwłaszcza w zakresie ochrony ich danych osobowych oraz autonomii informacyjnej, kładąc w konsekwencji wyraźny nacisk na przejrzystość i jasność procesów związanych z przetwarzaniem danych oraz na minimalizację, a zatem zapewnienie możliwie najmniejszej ingerencji w prawa podstawowe jednostek. 184

B. Zasada zgodności z prawem i rzetelności

W art. 5 ust. 1 lit. a RODO prawodawca unijny sformułował wymóg, aby **dane były przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą**. W przepisie tym inkorporowane zostały zatem dwie zasady przetwarzania, tj. legalność – zgodność przetwarzania z prawem, obejmująca także uczciwość i rzetelność przetwarzania, oraz przejrzystość, która zostanie omówiona w kolejnym punkcie. 185

186 Zgodność z prawem nie oznacza wyłącznie spełnienia jednej z przesłanek legalizacyjnych wskazanych w art. 6 lub 9 RODO, na co mogłaby wskazywać literalna wykładnia uwzględniająca brzmienie tytułów poszczególnych jednostek redakcyjnych. W tym sensie zasada legalności ma charakter nadrzędny wobec pozostałych zasad.

> ***WAŻNE!*** Spełnienie zasady legalności konstruującej wymóg zapewnienia zgodności obejmuje całościowo regulację rozporządzenia, w tym m.in. wdrożenie pozostałych zasad przetwarzania danych, czyli zapewnienie przejrzystości przetwarzania, prawidłowości, poufności i integralności danych osobowych, spełnienie kryterium proporcjonalności czasu i zakresu przetwarzanych danych do realizowanego celu oraz zapewnienie możliwości wykazania przez administratora wykonania poszczególnych obowiązków, a szczegółowo także np. zapewnienie zgodnego z prawem przekazywania danych podmiotom przetwarzającym, prawidłowość transferów danych do państw trzecich.

187 **Aspekt rzetelności przetwarzania** nakierowany jest natomiast na zobowiązanie administratora do **uwzględniania w planowanych procesach przetwarzania interesów osoby, której dane dotyczą**, w tym oczekiwania, aby ingerencja w prywatność spowodowana przetwarzaniem danych nie była nadmierna w kontekście realizowanego celu przetwarzania. Zapewnić zatem należy, aby dane przetwarzane były z poszanowaniem interesów osób, których dane dotyczą, co więcej – by dane były przetwarzane w sposób i w celu, którego podmiot danych może się rozsądnie spodziewać. Kluczowe jest w konsekwencji zapewnienie respektowania podstawowych praw i wolności podmiotu danych oraz znalezienie kompromisu między prawem do ochrony danych osobowych a interesami administratora. Zasada ta znajduje uszczegółowienie zwłaszcza w uregulowanym w art. 25 RODO zobowiązaniu do uwzględniania ochrony danych osobowych w fazie projektowania (*data protection by design*).

188 Zasada ta wymaga równocześnie od administratora **wprowadzenia środków zapobiegających arbitralnemu, dyskryminującemu traktowaniu podmiotów danych** – z uwagi np. na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny, zdrowotny lub orientację seksualną – lub przetwarzaniu skutkującemu środkami mającymi taki efekt. W konsekwencji omawiana zasada wymaga implementacji rozwiązań i mechanizmów pozwalających wykluczyć z przetwarzania dane niepoprawne, przetwarzane bezpodstawnie czy w zakresie nieadekwatnym lub w inny sposób wywołujące powyższe skutki.

> ***WAŻNE!*** Aby zapewnić rzetelność i przejrzystość przetwarzania wobec osoby, której dane dotyczą, mając na uwadze konkretne okoliczności i kontekst przetwarzania danych osobowych, administrator powinien wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę czynników powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą, oraz zapobiec m.in. skutkom w postaci dyskryminacji osób fizycznych (motyw 71 RODO).

189 Ponadto z omawianej zasady wynika zobowiązanie do wdrożenia takich środków technicznych i organizacyjnych, które zapewniają w szczególności **korektę czynników powodujących nieprawidłowości** w danych osobowych i nakierowane będą na maksymalne zmniejszenie ryzyka błędów oraz zabezpieczenie danych osobowych w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą.

C. Zasada przejrzystości

Z zasady przejrzystości wynikają wymogi związane z zapewnieniem podmiotom danych jak najpełniejszej wiedzy na temat celu, zakresu i kontekstu przetwarzania danych, a także możliwości sprawowania kontroli nad własnymi danymi, co nie ogranicza się tylko do spełnienia obowiązków informacyjnych z art. 13 i 14 RODO, ale też zapewnienia świadomości w trakcie całego procesu przetwarzania. W konsekwencji zasada ta będzie stanowiła podstawę dla utrzymywania świadomości procesów przetwarzania po stronie podmiotów danych, aktualizacji informacji, formułowania zgód, instrukcji, procedur i polityk, a wreszcie realizacji praw podmiotów danych oraz wykonywania obowiązków notyfikacyjnych. 190

> **WAŻNE!** W motywie 39 RODO sprecyzowane zostaje, że dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Administrator zobowiązany jest zatem do przedstawienia podmiotowi danych wszystkich niezbędnych informacji dotyczących istotnych aspektów przetwarzania.

Istotą komunikacji z podmiotem danych **ma być transparentność procesu przetwarzania** z punktu widzenia tego podmiotu, tak by osoba, której dane dotyczą, rozumiała, jakie są ryzyka związane z przetwarzaniem, z czym ono się wiąże i jakie są skutki przekazania przez nią danych administratorowi oraz jakie w tej relacji ma uprawnienia. W tym zakresie warto mieć też na uwadze motyw 71 RODO, zgodnie z którym realizacja prawa do informacji jest jednym ze sposobów zabezpieczenia przetwarzania, zaś osoba, której dane są przetwarzane, powinna mieć prawo nie tylko do uzyskania informacji, lecz także do wyrażania własnego stanowiska co do podjętej decyzji, żądania interwencji człowieka i wyjaśnień, na jakiej podstawie decyzja została podjęta, oraz kwestionowania tej decyzji. 191

W świetle zasady przejrzystości niezbędne jest, by **wszelkie informacje i komunikaty** związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz **sformułowane jasnym i prostym językiem**. Uszczegółowienie tej zasady zawiera regulacja art. 12 ust. 1 RODO, konkretyzująca wymogi przejrzystości. 192
Wobec powyższego administrator, uwzględniając wymaganie zrozumiałej formy oraz jasnego i prostego języka, powinien formułować zapytania lub oświadczenia w sposób prosty semantycznie i jednoznaczny, a użycie pojęć technicznych ograniczyć do sytuacji, w których jest to niezbędne, tak aby komunikat został zrozumiany przez odbiorcę zgodnie z wolą administratora.

> **WAŻNE!** Wszelka komunikacja związana z przetwarzaniem danych skierowana do podmiotu danych – bez względu na jej zakres – powinna być sformułowana w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

Rozporządzenie 2016/679 nie wprowadza ograniczeń w zakresie formy komunikatów kierowanych do podmiotów danych. Szczątkową regulację zawiera art. 12 ust. 1 zdanie drugie RODO, wskazując, że informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą (zob. szerzej nr 283, 288). 193