

# **RODO**

## **OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH**

**Komentarz**

**redakcja naukowa**

**Edyta Bielak-Jomaa, Dominik Lubasz**

Edyta Bielak-Jomaa, Witold Chomiczewski, Michał Czerniawski

Piotr Drobek, Urszula Góral, Magdalena Kuba

Dominik Lubasz, Joanna Łuczak, Paweł Makowski

Katarzyna Witkowska-Nowakowska, Natalia Zawadzka

---

**RODO 2018**

---

**KOMENTARZE**

# RODO

## OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH

Komentarz

redakcja naukowa

**Edyta Bielak-Jomaa, Dominik Lubasz**

Edyta Bielak-Jomaa, Witold Chomiczewski, Michał Czerniawski

Piotr Drobek, Urszula Góral, Magdalena Kuba

Dominik Lubasz, Joanna Łuczak, Paweł Makowski

Katarzyna Witkowska-Nowakowska, Natalia Zawadzka

---

---

KOMENTARZE

Zamów książkę w księgarni internetowej

**profinfo.pl**  
księgarnia internetowa

*Stan prawny na 1 października 2017 r.*

Recenzent

*Dr hab. Monika Namysłowska, prof. UŁ*

Wydawca

*Monika Pawłowska*

Redaktor prowadzący

*Adam Choiński*

Opracowanie redakcyjne

*Bartosz Stanisławski, Eliza Marks*

Łamanie

*JustLuk*

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegał przysługujących im praw. Książkę możesz udostępnić osobom bliskim lub osobiście znajomym, ale nie publikuj jej w internecie. Jeśli cytujesz fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A jeśli musisz skopiować część, rób to jedynie na użytek osobisty.

prawolubni

SZANUJMY PRAWO I WŁASNOŚĆ  
Więcej na [www.legalnakultura.pl](http://www.legalnakultura.pl)  
POLSKA IZBA KSIĄŻKI

© Copyright by  
Wolters Kluwer Polska SA, 2018

ISBN: 978-83-8124-014-7

Dział Praw Autorskich

01-208 Warszawa, ul. Przyokopowa 33

tel. 22 535 82 19

e-mail: [ksiazki@wolterskluwer.pl](mailto:ksiazki@wolterskluwer.pl)

[www.wolterskluwer.pl](http://www.wolterskluwer.pl)

księgarnia internetowa [www.profinfo.pl](http://www.profinfo.pl)

# Spis treści

Wykaz skrótów .....	13
Słowo wstępne .....	19
<b>Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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) (Tekst mający znaczenie dla EOG) (Dz.Urz. UE L 119, s. 1) .....</b>	<b>21</b>
<b>Preambuła .....</b>	<b>23</b>
<b>Rozdział I. Przepisy ogólne .....</b>	<b>105</b>
Artykuł 1. Przedmiot i cele .....	105
Artykuł 2. Materialny zakres stosowania .....	118
Artykuł 3. Terytorialny zakres stosowania .....	147
Artykuł 4. Definicje .....	156
Artykuł 4 pkt 1. Dane osobowe .....	163
Artykuł 4 pkt 2. Przetwarzanie .....	186
Artykuł 4 pkt 3. Ograniczenie przetwarzania .....	199
Artykuł 4 pkt 4. Profilowanie .....	200
Artykuł 4 pkt 5. Pseudonimizacja .....	203
Artykuł 4 pkt 6. Zbiór danych .....	208
Artykuł 4 pkt 7. Administrator .....	211
Artykuł 4 pkt 8. Podmiot przetwarzający .....	222
Artykuł 4 pkt 9. Odbiorca .....	228

Artykuł 4 pkt 10. Strona trzecia .....	236
Artykuł 4 pkt 11. Zgoda .....	242
Artykuł 4 pkt 12. Naruszenie ochrony danych osobowych ..	263
Artykuł 4 pkt 13. Dane genetyczne .....	267
Artykuł 4 pkt 14. Dane biometryczne .....	273
Artykuł 4 pkt 15. Dane dotyczące zdrowia .....	277
Artykuł 4 pkt 16. Główna jednostka organizacyjna .....	281
Artykuł 4 pkt 17. Przedstawiciel .....	285
Artykuł 4 pkt 18. Przedsiębiorca .....	288
Artykuł 4 pkt 19. Grupa przedsiębiorstw .....	295
Artykuł 4 pkt 20. Wiążące reguły korporacyjne .....	298
Artykuł 4 pkt 21. Organ nadzorczy .....	300
Artykuł 4 pkt 22. Organ nadzorczy, którego sprawa dotyczy .....	302
Artykuł 4 pkt 23. Transgraniczne przetwarzanie .....	306
Artykuł 4 pkt 24. Mający znaczenie dla sprawy i uzasadniony sprzeciw .....	309
Artykuł 4 pkt 25. Usługa społeczeństwa informacyjnego ...	311
Artykuł 4 pkt 26. Organizacja międzynarodowa .....	317
<b>Rozdział II. Zasady .....</b>	<b>322</b>
Artykuł 5. Zasady dotyczące przetwarzania danych osobowych .....	322
Artykuł 6. Zgodność przetwarzania z prawem .....	344
Artykuł 6 ust. 1 lit. a. Zgoda .....	351
Artykuł 6 ust. 1 lit. b. Niezbędność przetwarzania dla wykonania umowy lub podjęcia działań przed zawarciem umowy .....	358
Artykuł 6 ust. 1 lit. c. Niezbędność przetwarzania dla wypełnienia obowiązku prawnego ciążącego na administratorze .....	366
Artykuł 6 ust. 1 lit. d. Niezbędność przetwarzania z uwagi na ochronę żywotnych interesów osoby .....	376
Artykuł 6 ust. 1 lit. e. Niezbędność przetwarzania dla wykonania zadania realizowanego w interesie publicznym .....	380
Artykuł 6 ust. 1 lit. f. Niezbędność przetwarzania dla celów wynikających z prawnie uzasadnionych interesów .....	388

---

Artykuł 6 ust. 2. Uprawnienie państw członkowskich do wprowadzenia bardziej szczegółowych przepisów dotyczących warunków przetwarzania .....	400
Artykuł 6 ust. 3. Wymogi dotyczące podstawy prawnej przetwarzania .....	401
Artykuł 6 ust. 4. Zmiana celu przetwarzania danych osobowych .....	402
Artykuł 7. Warunki wyrażenia zgody .....	409
Artykuł 8. Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego .....	427
Artykuł 9. Przetwarzanie szczególnych kategorii danych osobowych .....	437
Artykuł 10. Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa .....	455
Artykuł 11. Przetwarzanie niewymagające identyfikacji .....	460
<b>Rozdział III. Prawa osoby, której dane dotyczą .....</b>	<b>464</b>
<b>Sekcja 1. Przejrzystość oraz tryb korzystania z praw .....</b>	<b>464</b>
Artykuł 12. Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą .....	464
<b>Sekcja 2. Informacje i dostęp do danych osobowych .....</b>	<b>477</b>
Artykuł 13. Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą .....	477
Artykuł 14. Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą .....	492
Artykuł 15. Prawo dostępu przysługujące osobie, której dane dotyczą .....	507
<b>Sekcja 3. Sprostowanie i usuwanie danych .....</b>	<b>517</b>
Artykuł 16. Prawo do sprostowania danych .....	517
Artykuł 17. Prawo do usunięcia danych („prawo do bycia zapomnianym”) .....	522
Artykuł 18. Prawo do ograniczenia przetwarzania .....	530
Artykuł 19. Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania .....	537
Artykuł 20. Prawo do przenoszenia danych .....	542

---

<b>Sekcja 4. Prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach</b> . . . . .	554
Artykuł 21. Prawo do sprzeciwu . . . . .	554
Artykuł 22. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie . . . . .	561
<b>Sekcja 5. Ograniczenia</b> . . . . .	573
Artykuł 23. Ograniczenia . . . . .	573
<b>Rozdział IV. Administrator i podmiot przetwarzający</b> . . . . .	585
<b>Sekcja 1. Obowiązki ogólne</b> . . . . .	585
Artykuł 24. Obowiązki administratora . . . . .	585
Artykuł 25. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych . . . . .	599
Artykuł 26. Współadministratorzy . . . . .	612
Artykuł 27. Przedstawiciele administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii . . . . .	623
Artykuł 28. Podmiot przetwarzający . . . . .	631
Artykuł 29. Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego . . . . .	654
Artykuł 30. Rejestrowanie czynności przetwarzania . . . . .	661
Artykuł 31. Współpraca z organem nadzorczym . . . . .	681
<b>Sekcja 2. Bezpieczeństwo danych osobowych</b> . . . . .	687
Artykuł 32. Bezpieczeństwo przetwarzania . . . . .	687
Artykuł 33. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu . . . . .	708
Artykuł 34. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych . . . . .	717
<b>Sekcja 3. Ocena skutków dla ochrony danych i uprzednie konsultacje</b> . . . . .	728
Artykuł 35. Ocena skutków dla ochrony danych . . . . .	728
Artykuł 36. Uprzednie konsultacje . . . . .	756
<b>Sekcja 4. Inspektor ochrony danych</b> . . . . .	765
Artykuł 37. Wyznaczenie inspektora ochrony danych . . . . .	765
Artykuł 38. Status inspektora ochrony danych . . . . .	794
Artykuł 39. Zadania inspektora ochrony danych . . . . .	807
<b>Sekcja 5. Kodeksy postępowania i certyfikacja</b> . . . . .	816
Artykuł 40. Kodeksy postępowania . . . . .	816

---

Artykuł 41. Monitorowanie zatwierdzonych kodeksów postępowania .....	831
Artykuł 42. Certyfikacja .....	838
Artykuł 43. Podmiot certyfikujący .....	847
<b>Rozdział V. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych .....</b>	<b>857</b>
Artykuł 44. Ogólna zasada przekazywania .....	857
Artykuł 45. Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony .....	861
Artykuł 46. Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń .....	869
Artykuł 47. Wiążące reguły korporacyjne .....	876
Artykuł 48. Przekazywanie lub ujawnianie niedozwolone na mocy prawa Unii .....	887
Artykuł 49. Wyjątki w szczególnych sytuacjach .....	888
Artykuł 50. Międzynarodowa współpraca na rzecz ochrony danych osobowych .....	903
<b>Rozdział VI. Niezależne organy nadzorcze .....</b>	<b>906</b>
<b>Sekcja 1. Niezależny status .....</b>	<b>906</b>
Artykuł 51. Organ nadzorczy .....	906
Artykuł 52. Niezależność .....	910
Artykuł 53. Ogólne warunki dotyczące członków organu nadzorczego .....	918
Artykuł 54. Zasady ustanawiania organu nadzorczego .....	921
<b>Sekcja 2. Właściwość, zadania i uprawnienia .....</b>	<b>923</b>
Artykuł 55. Właściwość .....	923
Artykuł 56. Właściwość wiodącego organu nadzorczego .....	927
Artykuł 57. Zadania .....	933
Artykuł 58. Uprawnienia .....	939
Artykuł 59. Sprawozdanie z działalności .....	946
<b>Rozdział VII. Współpraca i spójność .....</b>	<b>949</b>
<b>Sekcja 1. Współpraca .....</b>	<b>949</b>
Artykuł 60. Współpraca między wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy .....	949
Artykuł 61. Wzajemna pomoc .....	964
Artykuł 62. Wspólne operacje organów nadzorczych .....	972

---



<b>Sekcja 2. Spójność</b>	976
Artykuł 63. Mechanizm spójności	976
Artykuł 64. Opinia Europejskiej Rady Ochrony Danych	979
Artykuł 65. Rozstrzygnięcie sporów przez Europejską Radę Ochrony Danych	984
Artykuł 66. Tryb pilny	989
Artykuł 67. Wymiana informacji	993
<b>Sekcja 3. Europejska rada ochrony danych</b>	994
Artykuł 68. Europejska Rada Ochrony Danych	994
Artykuł 69. Niezależność	998
Artykuł 70. Zadania Europejskiej Rady Ochrony Danych	1000
Artykuł 71. Sprawozdania	1008
Artykuł 72. Procedura	1011
Artykuł 73. Przewodniczący	1012
Artykuł 74. Zadania przewodniczącego	1014
Artykuł 75. Sekretariat	1016
Artykuł 76. Poufność	1020
<b>Rozdział VIII. Środki ochrony prawnej, odpowiedzialność i sankcje</b>	1022
Artykuł 77. Prawo do wniesienia skargi do organu nadzorczego	1022
Artykuł 78. Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorcemu	1029
Artykuł 79. Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu	1035
Artykuł 80. Reprezentowanie osób, których dane dotyczą	1040
Artykuł 81. Zawieszenie postępowania	1045
Artykuł 82. Prawo do odszkodowania i odpowiedzialność	1048
Artykuł 83. Ogólne warunki nakładania administracyjnych kar pieniężnych	1054
Artykuł 84. Sankcje	1066
<b>Rozdział IX. Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem</b>	1073
Artykuł 85. Przetwarzanie a wolność wypowiedzi i informacji	1073

---

Artykuł 86. Przetwarzanie a publiczny dostęp do dokumentów urzędowych .....	1081
Artykuł 87. Przetwarzanie krajowego numeru identyfikacyjnego .....	1085
Artykuł 88. Przetwarzanie w kontekście zatrudnienia .....	1090
Artykuł 89. Zabezpieczenia i wyjątki mające zastosowanie do przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych .....	1103
Artykuł 90. Obowiązek zachowania tajemnicy .....	1107
Artykuł 91. Istniejące zasady ochrony danych obowiązujące kościoły i związki wyznaniowe .....	1112
<b>Rozdział X. Akty delegowane i akty wykonawcze .....</b>	<b>1118</b>
Artykuł 92. Wykonywanie przekazanych uprawnień .....	1118
Artykuł 93. Procedura komitetowa .....	1121
<b>Rozdział XI. Przepisy końcowe .....</b>	<b>1124</b>
Artykuł 94. Uchylenie dyrektywy 95/46/WE .....	1124
Artykuł 95. Stosunek do dyrektywy 2002/58/WE .....	1126
Artykuł 96. Stosunek do uprzednio zawartych umów .....	1129
Artykuł 97. Sprawozdania Komisji .....	1131
Artykuł 98. Przegląd innych aktów prawnych Unii dotyczących ochrony danych .....	1133
Artykuł 99. Wejście w życie i stosowanie .....	1135
<b>Bibliografia .....</b>	<b>1145</b>
<b>O Autorach .....</b>	<b>1163</b>



# Wykaz skrótów

## 1. Akty prawne

- BDSG – Bundesdatenschutzgesetz – Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (BGBl 2004 I, S. 66)
- BGB – Bürgerliches Gesetzbuch (BGBl 2002 I, S. 42)
- dyrektywa 93/13/EWG – dyrektywa Rady 93/13/EWG z 5.04.1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz.Urz. WE L 95, s. 29, ze zm.)
- dyrektywa 95/46/WE – dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. WE L 281, s. 31, ze zm.)
- dyrektywa 2000/31/WE – 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 – 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 pry-

- watności i łączności elektronicznej) (Dz.Urz. WE L 201, s. 37, ze zm.)
- dyrektywa 2003/98/WE – dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z 17.11.2003 r. w sprawie ponownego wykorzystania informacji sektora publicznego (Dz.Urz. UE L 345, s. 90, 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 (Dz.Urz. UE L 241, s. 1)
- dyrektywa 2016/680 – 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 uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89)
- 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. poz. 284 ze zm.)
- k.c. – ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2017 r. poz. 459 ze zm.)
- k.k. – ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2016 r. poz. 1137 ze zm.)
- Konkordat – Konkordat między Stolicą Apostolską i Rzeczypospolitą Polską podpisany w Warszawie 28.07.1993 r. (Dz.U. z 1998 r. poz. 318)
- Konstytucja RP – Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. poz. 483 ze zm.)

- 
- Konwencja nr 108 Rady Europy – 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. poz. 25)
- k.p. – ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2016 r. poz. 1666 ze zm.)
- k.p.a. – ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2017 r. poz. 1257)
- k.p.c. – ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2016 r. poz. 1822 ze zm.)
- k.p.k. – ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2017 r. poz. 1904)
- KPP – Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 389)
- k.s.h. – ustawa z 15.09.2000 r. – Kodeks spółek handlowych (Dz.U. z 2017 r. poz. 1577)
- opinia 4/2007 – opinia Grupy Roboczej Art. 29 4/2007 w sprawie pojęcia danych osobowych z 20.06.2007 r., WP 136, [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_pl.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf), dostęp: 26.09.2017 r.
- opinia 1/2010 – opinia Grupy Roboczej Art. 29 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający” z 16.02.2010 r., WP 169, [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169\\_pl.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_pl.pdf), dostęp: 26.09.2017 r.
- opinia 15/2011 – opinia Grupy Roboczej Art. 29 15/2011 w sprawie definicji zgody z 13.07.2011 r., WP 187, [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187\\_pl.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_pl.pdf), dostęp: 26.09.2017 r.
- opinia 2/2017 – opinia Grupy Roboczej Art. 29 2/2017 w sprawie przetwarzania danych w pracy z 8.06.2017 r., WP 249, [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=45631](http://ec.europa.eu/newsroom/document.cfm?doc_id=45631), dostęp: 26.09.2017 r.
-

- p.p.s.a. – ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2017 r. poz. 1369 ze zm.)
- pr. tel. – ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2017 r. poz. 1907)
- rozporządzenie 45/2001 – 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 z 2001 r., s. 1)
- rozporządzenie 1049/2001 – rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z 30.05.2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.Urz. WE L 145, s. 43)
- rozporządzenie 765/2008 – Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z 9.07.2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.Urz. UE L 218, s. 30)
- rozporządzenie 1215/2012 – 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 – 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)
- TFUE – Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47)

---

TUE	- Traktat o Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 13)
TWE	- Traktat ustanawiający Wspólnotę Europejską (Dz.Urz. UE C 321E z 2006 r., s. 37)
u.d.i.p.	- ustawa z 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2016 r. poz. 1764 ze zm.)
u.k.r.k.	- ustawa z 24.05.2000 r. o Krajowym Rejestrze Karnym (Dz.U. z 2017 r. poz. 678 ze zm.)
u.o.d.o.1997	- ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.)
u.o.k.k.	- ustawa z 16.02.2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2017 r. poz. 229 ze zm.)
u.p.k.	- ustawa z 30.05.2014 r. o prawach konsumenta (Dz.U. 2017 r. poz. 683)
u.p.z.p.	- ustawa z 13.05.2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym (Dz.U. poz. 862 ze zm.)
u.s.d.g.	- ustawa z 2.07.2004 r. o swobodzie działalności gospodarczej (Dz.U. z 2016 r. poz. 1829 ze zm.)
u.ś.u.d.e.	- ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2017 r. poz. 1219)
Wytyczne DPIA	- Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko”, do celów rozporządzenia 2016/679, z 4.04.2017 r., 17/EN, WP 248, <a href="http://ec.europa.eu/newsroom/document.cfm?doc_id=44137">http://ec.europa.eu/newsroom/document.cfm?doc_id=44137</a> , dostęp: 26.09.2017 r., polska wersja językowa: <a href="http://giodo.gov.pl/pl/1520285/10078">http://giodo.gov.pl/pl/1520285/10078</a> , dostęp: 26.09.2017 r.
Wytyczne DPO	- Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (DPO) z 13.12.2016 r., zmienione i przyjęte 5.04.2017 r., 16/EN, WP 243, rew.01, <a href="http://ec.europa.eu/newsroom/document.cfm?doc_id=44100">http://ec.europa.eu/newsroom/document.cfm?doc_id=44100</a> , dostęp: 26.09.2017 r., polska

---



wersja językowa: <http://www.giodo.gov.pl/pl/1520296/10056>, dostęp: 26.09.2017 r.

**Uwaga: jednostki redakcyjne bez bliższego oznaczenia dotyczą rozporządzenia 2016/679 (Dz.Urz. UE L 119, s. 1).**

## 2. Czasopisma, publikatory

EPS	– Europejski Przegląd Sądowy
M. Praw.	– Monitor Prawniczy
ONSA WSA	– Orzecznictwo Naczelnego Sądu Administracyjnego i Wojewódzkich Sądów Administracyjnych
OSNC	– Orzecznictwo Sądu Najwyższego. Izba Cywilna
OTK-A	– Orzecznictwo Trybunału Konstytucyjnego – Zbiór urzędowy, Seria A
PiP	– Państwo i Prawo
Prok. i Pr.	– Prokuratura i Prawo
RPEiS	– Ruch Prawniczy, Ekonomiczny i Socjologiczny
ZNSA	– Zeszyty Naukowe Sądownictwa Administracyjnego

## 3. Inne

ETPC	– Europejski Trybunał Praw Człowieka
GIODO	– Generalny Inspektor Ochrony Danych Osobowych
Grupa Robocza Art. 29	– Grupa Robocza ds. Ochrony Osób Fizycznych w Zakresie Przetwarzania Danych Osobowych, powołana na mocy art. 29 dyrektywy 95/46/WE
ICO	– Information Commissioner
IOD	– inspektor ochrony danych
KRK	– Krajowy Rejestr Karny
NSA	– Naczelnny Sąd Administracyjny
SN	– Sąd Najwyższy
TS	– Trybunał Sprawiedliwości

## Słowo wstępne

Ogólne rozporządzenie o ochronie danych weszło w życie 25.05.2016 r. i zacznie być stosowane od 25.05.2018 r. Wraz z rozpoczęciem stosowania rozporządzenia 2016/679 usunięta zostanie z porządku prawnego, po ponad 20 latach obowiązywania, dyrektywa 95/46/WE, a tym samym obraz ram prawnych ochrony danych osobowych w Europie ulegnie radykalnej zmianie. Data ta stanowi swoistą cezurę w rozwoju prawa ochrony danych osobowych i jest to związane nie tylko z materią regulacyjną, ale także z wyborem środka legislacyjnego dla realizacji celów regulacji. Rozporządzenie jako akt prawa unijnego będzie obowiązywało we wszystkich państwach członkowskich w sposób bezpośredni, co ma w istotny sposób ograniczyć negatywny efekt harmonizacji minimalnej dokonywanej dyrektywą 95/46/WE. Na rzeczywiste osiągnięcie projektowanego ujednoczenia poziomu ochrony danych osobowych wpływać będzie jednak nie tylko stosowanie nowego prawa przez administratorów, organy nadzorcze i sądy, ale również zakres aktywności prawodawców krajowych, których w rozporządzeniu wyposażono w szerokie kompetencje regulacyjne zarówno o charakterze obligatoryjnym, tj. zmierzających do zapewnienia stosowalności komentowanego unijnego aktu prawnego, jak i o charakterze fakultatywnym, upoważniającym m.in. do wprowadzania ograniczeń stosowania regulacji unijnej.

W komentarzu uwzględniliśmy nie tylko regulację rozporządzenia, ale także przedstawione do konsultacji społecznych przez Ministra Cyfryzacji projekty ustawy o ochronie danych osobowych z 12.09.2017 r.

oraz ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych z 12.09.2017 r., jak również opracowane przez Grupę Roboczą Art. 29 wytyczne dotyczące stosowania rozporządzenia. Wskazaliśmy i skomentowaliśmy wypowiedzi doktryny polskiej i międzynarodowej, w szczególności angielskiej, niemieckiej i francuskiej.

Opracowanie niniejszej publikacji stało się możliwe przede wszystkim dzięki jedenastu autorom o rozległych kompetencjach merytorycznych z zakresu problematyki ochrony danych osobowych, będących przedstawicielami praktyki, nauki prawa oraz administracji. To ich zaangażowaniu zawdzięczamy to, że jeszcze przed rozpoczęciem stosowania rozporządzenia, w okresie przejściowym, możliwe było oddanie tak obszernej publikacji do druku. Skala nadchodzących zmian jest bowiem na tyle rozległa, że zarówno ustawodawca krajowy, jak i administratorzy powinni jak najszybciej przeanalizować nowe mechanizmy ochrony danych i rozpocząć przygotowania do zapewnienia zgodności z unijnym aktem prawnym, w czym komentarz niniejszy będzie mógł, mamy nadzieję, im pomóc.

Liczymy, że niniejszy komentarz stanie się głosem w dyskusji na temat wykładni rozporządzenia 2016/679, ale i ułatwi jego praktyczne zastosowanie.

Łódź, Warszawa, 1.10.2017 r.

*Edyta Bielak-Jomaa, Dominik Lubasz*

**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)**

(Tekst mający znaczenie dla EOG)

(Dz.Urz. UE L 119, s. 1)



**PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,**  
uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,  
uwzględniając wniosek Komisji Europejskiej,  
po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,  
uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego<sup>1</sup>,  
uwzględniając opinię Komitetu Regionów<sup>2</sup>,  
stanowiąc zgodnie ze zwykłą procedurą ustawodawczą<sup>3</sup>,  
a także mając na uwadze, co następuje:

- (1) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą praw podstawowych”) oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.
- (2) Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą – niezależnie od obywatelstwa czy miejsca zamieszkania takich osób – naruszać ich podstawowych praw i wolności, w szczególności

---

<sup>1</sup> Dz.Urz. UE C 229 z 2012 r., s. 90.

<sup>2</sup> Dz.Urz. UE C 391 z 2012 r., s. 127.

<sup>3</sup> Stanowisko Parlamentu Europejskiego z 12.03.2014 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz stanowisko Rady w pierwszym czytaniu z 8.04.2016 r. (dotychczas nieopublikowane w Dzienniku Urzędowym). Stanowisko Parlamentu Europejskiego z 14.04.2016 r.

prawa do ochrony danych osobowych. Niniejsze rozporządzenie ma na celu przyczynić się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmocnienia i konwergencji gospodarek na rynku wewnętrznym, a także do pomyślności ludzi.

- (3) Celem dyrektywy Parlamentu Europejskiego i Rady 95/46/WE<sup>4</sup> jest zharmonizowanie ochrony podstawowych praw i wolności osób fizycznych w związku z czynnościami przetwarzania oraz zapewnienie swobodnego przepływu danych osobowych między państwami członkowskimi.
- (4) Przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości. Prawo do ochrony danych osobowych nie jest prawem bezwzględny; należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności. Niniejsze rozporządzenie nie narusza praw podstawowych, wolności i zasad uznanych w Karcie praw podstawowych – zapisanych w Traktatach – w szczególności prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, ochrony danych osobowych, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej.
- (5) Integracja społeczno-gospodarcza wynikająca z funkcjonowania rynku wewnętrznego doprowadziła do znacznego zwiększenia transgranicznych przepływów danych osobowych. Wzrosła wymiana danych osobowych między podmiotami publicznymi i prywatnymi, w tym między osobami fizycznymi, zrzeszeniami i przedsiębiorstwami w Unii. Od organów krajowych państw członkowskich prawo Unii coraz częściej

---

<sup>4</sup> Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L 281, s. 31).

wymaga, by w celu wykonania swoich obowiązków lub w celu realizacji zadań w imieniu organu innego państwa członkowskiego współpracowały ze sobą i wymieniały się danymi osobowymi.

- (6) 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 mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych.
- (7) Przemiany te wymagają stabilnych, spójniejszych ram ochrony danych w Unii oraz zdecydowanego ich egzekwowania, gdyż ważna jest budowa zaufania, które pozwoli na rozwój gospodarki cyfrowej na rynku wewnętrznym. Osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi. Osoby fizyczne, podmioty gospodarcze i organy publiczne powinny zyskać większe poczucie pewności prawa i jego stosowania w praktyce.
- (8) W zakresie, w jakim niniejsze rozporządzenie dopuszcza doprecyzowanie lub zawężenie jego przepisów przez prawo państw członkowskich, mogą one – o ile jest to niezbędne, by krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie – włączyć elementy niniejszego rozporządzenia do swego prawa krajowego.
- (9) Cele i zasady dyrektywy 95/46/WE pozostają aktualne, jednak wdrażając ochronę danych w Unii, nie uniknięto fragmentaryzacji, niepewności prawnej oraz upowszechnienia się poglądu, że ochrona osób fizycznych jest znacznie zagrożona, w szczególności w związku z działaniami w internecie. Różnice w stopniu ochrony praw i wolności osób fizycznych



obowiązujących, że administratorzy będą musieli z pewnością zmodyfikować klauzule informacyjne, a w stosunku do procesów przetwarzania w toku uzupełnić informacje o dane dotychczas niewymagane<sup>373</sup>.

### Artykuł 4 pkt 12 Naruszenie ochrony danych osobowych

12) „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

1. W art. 4 pkt 12 prawodawca unijny zdefiniował **pojęcie naruszenia ochrony danych osobowych**. W dotychczasowym stanie prawnym nie miało ono swojej legalnej definicji. Ustawa o ochronie danych osobowych z 1997 r. posługiwała się pojęciem naruszenia przepisów o ochronie danych osobowych (art. 17 i 18), jednak nie było ono analogiczne do naruszenia ochrony danych osobowych na gruncie rozporządzenia 2016/679.

Zgodnie z omawianym przepisem przez naruszenie ochrony danych osobowych należy rozumieć 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.

2. Prezentowana definicja ma **istotne znaczenie dla stosowania przepisów art. 33 i 34**. Regulują one obowiązki administratora związane odpowiednio ze zgłoszeniem naruszenia ochrony danych osobowych organowi nadzorcemu oraz zawiadomienia osoby, której dane dotyczą, o takim naruszeniu<sup>374</sup>.

<sup>373</sup> Zob. komentarz do art. 13.

<sup>374</sup> Zob. komentarz do art. 33 oraz 34.

3. Dla zaistnienia naruszenia danych osobowych muszą być spełnione **kumulatywnie** następujące **przesłanki**. Po pierwsze, musi **zaistnieć naruszenie bezpieczeństwa**. Po drugie, **skutkiem** tego naruszenia musi być **przypadkowe lub niezgodne z prawem** zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do przetwarzanych danych osobowych.
4. **Poprzez naruszenie bezpieczeństwa należy rozumieć** każde zdarzenie, w którym organizacyjne lub techniczne środki zabezpieczenia danych osobowych zawodzą<sup>375</sup>. Takimi **środkami** są te, które powinny być **wdrożone** przez danego administratora **zgodnie** z zasadami określonymi w przepisach **art. 32**. Naruszenia bezpieczeństwa w rozumieniu przepisu art. 4 pkt 12 nie można bowiem odnosić jedynie do środków rzeczywiście wdrożonych przez danego administratora. Prowadziłoby to do wyłączenia z zakresu tej przesłanki sytuacji, gdy administrator nie wdrożył odpowiednich środków technicznych i organizacyjnych zgodnie z wymogami przepisów art. 32. Taka wykładnia byłaby błędna. Prowadziłaby ona do istotnego zawężenia pojęcia naruszenia ochrony danych osobowych. W konsekwencji ograniczałaby możliwości stosowania art. 33 i 34. Byłoby to sprzeczne z wyrażoną w art. 5 ust. 1 lit. a **zasadą zgodności z prawem, rzetelności i przejrzystości przetwarzania**. Przejrzystości przetwarzania służą bowiem m.in. instytucje zgłaszania naruszenia ochrony danych osobowych organowi nadzorcemu oraz zawiadamiania osoby, której dane dotyczą, o takim naruszeniu.

Dla zaistnienia tak rozumianego naruszenia bezpieczeństwa **nie ma żadnego znaczenia**, czy dojdzie do niego w wyniku **umyślnego, czy nieumyślnego działania**<sup>376</sup>. Istotne jest jedynie **obiektywne wystąpienie naruszenia**.

5. **Efektom naruszenia bezpieczeństwa** musi stać się: przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nie-

<sup>375</sup> L. Schreiber [w:]: *Kommentar zur BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG*, red. K.U. Plath, O. Schmidt, 2016, s. 983.

<sup>376</sup> S. Ernst [w:]: *Datenschutz-Grundverordnung...*, red. B. Paal, D. Pauly, s. 51.

uprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Wymienione skutki można podzielić na **dwie osobne kategorie: naruszenie integralności danych osobowych oraz nieuprawnione zapoznanie się z danymi**<sup>377</sup>.

6. Do **kategorii naruszenia integralności danych osobowych** zaliczyć można ich zniszczenie, utracenie oraz zmodyfikowanie<sup>378</sup>. **Utracenie danych osobowych oznacza** natomiast ich usunięcie<sup>379</sup>.

Tak rozumiane zniszczenie, utracenie lub zmodyfikowanie danych osobowych musi być **przypadkowe lub niezgodne z prawem**. Oceniając niezgodność z prawem, trzeba analizować **zgodność** takiego przetwarzania danych **z ogółem przepisów o ochronie danych osobowych**. Jeżeli operacja na danych w postaci ich zniszczenia, utracenia lub zmodyfikowania danych nastąpiła niezgodnie z zasadami wyrażonymi w tych przepisach, omawiana przesłanka będzie spełniona.

Z **przypadkowym** zniszczeniem, utraceniem lub zmodyfikowaniem danych osobowych będziemy mieli natomiast do czynienia w sytuacjach, gdy taka operacja na danych była **niezamierzonym efektem naruszenia bezpieczeństwa**.

Dla spełnienia omawianej przesłanki wystarczy, by zniszczenie, utracenie lub zmodyfikowanie danych było tylko niezgodne z prawem albo przypadkowe. Oczywiście te operacje na danych mogą być zarówno niezgodne z prawem, jak i przypadkowe.

7. Do **kategorii nieuprawnionego zapoznania się z danymi** zaliczają się ich nieuprawnione ujawnienie lub nieuprawniony dostęp do nich. Pojęcie ujawnienia zostało omówione przy definicji przetwarzania i oznacza ono przesłanie, rozpowszechnianie lub udostępnienie da-

<sup>377</sup> S. Jandt [w:] *DS-GVO...*, red. J. Kühling, B. Buchner, s. 165.

<sup>378</sup> W odniesieniu do znaczenia pojęć niszczenia oraz modyfikowania zob. uwagi 12 i 20 komentarza do art. 4 pkt 2.

<sup>379</sup> Zob. uwaga 20 komentarza do art. 4 pkt 2.

nych<sup>380</sup>. Poprzez dostęp należy natomiast rozumieć wszelkie sytuacje, gdy osoba trzecia uzyskuje dostęp do danych osobowych w wyniku swojego własnego działania, a nie w wyniku działania osoby realizującej przetwarzanie<sup>381</sup>.

Na gruncie przepisu art. 4 pkt 12 ujawnienie danych osobowych lub dostęp do nich będą istotne dopiero w sytuacji, jeżeli dojdzie do nich **w sposób nieuprawniony**. Oceny spełnienia tego warunku trzeba dokonywać przez pryzmat przepisów samego rozporządzenia ogólnego, jak również wdrożonych zgodnie z jego art. 32 zabezpieczeń organizacyjnych. Dopiero wówczas będzie można dokonać pełnej oceny, czy w danym przypadku ujawnienie lub dostęp do danych osobowych były nieuprawnione.

Badając, czy ujawnienie lub udostępnienie danych osobowych jest uprawnione, trzeba zweryfikować, czy dla takiej operacji na danych osobowych spełniona jest jedna z przesłanek legalizujących przetwarzanie, o których mowa w przepisach art. 6 ust. 1 dla danych „zwykłych”, a dla szczególnych kategorii danych osobowych w art. 9 ust. 2. Jeżeli warunki te nie będą spełnione, wówczas ujawnienie lub udostępnienie danych osobowych będzie nieuprawnione.

Jeżeli u danego administratora dostęp do danych uzyska osoba, która zgodnie z wdrożonymi u niego organizacyjnymi zabezpieczeniami nie powinna uzyskać takiego dostępu, np. administrator wymaga do tego upoważnienia, a osoba ta się nim nie legitymowała, wówczas warunek nieuprawnionego dostępu będzie zrealizowany.

- 8. Wszystkie postaci operacji**, które zostały wymienione w komentowanym przepisie, **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 rozporządzenia ogólnego

<sup>380</sup> Zob. uwaga 16 komentarza do art. 4 pkt 2.

<sup>381</sup> Zob. szerzej uwaga 16 komentarza do art. 4 pkt 2.

nego, jednak w jego konsekwencji zostaną utracone dane, które nie są danymi osobowymi, wówczas nie dojdzie do spełnienia przesłanek omawianego tu pojęcia.

### Artykuł 4 pkt 13 Dane genetyczne

**13) „dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;**

1. Prawodawca unijny wprowadza **pojęcia legalne różnych kategorii danych osobowych**, m.in. niedefiniowanych dotąd danych genetycznych, danych biometrycznych<sup>382</sup> oraz danych dotyczących zdrowia<sup>383</sup>. Podkreślić w szczególności wypada, iż uchylona na mocy przepisów rozporządzenia ogólnego dyrektywa 95/46/WE nie nawiązywała nawet do danych genetycznych (podobnie do danych biometrycznych), w przeciwieństwie do polskiej regulacji prawnej. Zgodnie bowiem z art. 27 ust. 1 u.o.d.o.1997 polski ustawodawca uwzględnił w katalogu szczególnie chronionych danych osobowych dane o kodzie genetycznym<sup>384</sup>. W tym kontekście można stwierdzić, że polska ustawa normowała obszerniejszy zakres tzw. danych wrażliwych (sensytywnych) w porównaniu z regulacją unijną<sup>385</sup>, chyba żeby przyjąć, iż dane te mieszczą

<sup>382</sup> Zob. komentarz do art. 4 pkt 14.

<sup>383</sup> Zob. komentarz do art. 4 pkt 15.

<sup>384</sup> Na temat różnic pomiędzy kategoriami danych o kodzie genetycznym oraz danych genetycznych zob. A. Dmochowska, *Przetwarzanie danych szczególnych kategorii* [w:] A. Dmochowska, M. Zadrozny, *Unijna reforma ochrony danych osobowych. Analiza zmian*, Warszawa 2016, s. 29. Zob. również K. Kaźmierczak, P. Litwiński, *Elementarz z zakresu ochrony danych osobowych* [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, red. D. Dörre-Kolasa, Warszawa 2017, s. 9.

<sup>385</sup> Zob. T.A.J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków*, Warszawa 2016, s. 66; T.A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych*, Wrocław 2014, s. 29.

**Edyta Bielak-Jomaa** – doktor nauk prawnych; od kwietnia 2015 r. Generalny Inspektor Ochrony Danych Osobowych; od 2003 r. adiunkt w Katedrze Prawa Pracy Wydziału Prawa i Administracji Uniwersytetu Łódzkiego; w latach 2012–2015 kierownik Podyplomowych Studiów Ochrony Danych Osobowych WPiA UŁ, a od 2013 r. kierownik Centrum Ochrony Danych Osobowych i Zarządzania Informacją; wykładowca i autorka ponad 40 opracowań z zakresu prawa pracy, problematyki rynku pracy oraz ochrony danych osobowych; jej zainteresowania naukowe obejmują przede wszystkim problematykę ochrony dóbr osobistych pracowników i ochrony danych osobowych w zatrudnieniu.

**Dominik Lubasz** – doktor nauk prawnych; radca prawny, partner zarządzający w Lubasz i Wspólnicy – Kancelaria Radców Prawnych; specjalizuje się w prawie nowych technologii, e-commerce, własności intelektualnej, ochronie danych osobowych oraz w polskim i europejskim prawie gospodarczym; autor wielu publikacji z zakresu ochrony danych osobowych oraz handlu elektronicznego, w tym komentarzy do ustaw: o prawach konsumenta, o świadczeniu usług drogą elektroniczną, o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym, o ochronie baz danych; ekspert Stowarzyszenia Konsumentów Polskich ds. handlu elektronicznego, ekspert legislacyjny Izby Gospodarki Elektronicznej E-commerce Polska.

Publikacja stanowi pierwsze kompleksowe omówienie nowych przepisów kształtujących ochronę danych osobowych. Komentowane rozporządzenie dotyczy wszystkich uczestników obrotu gospodarczego oraz innych podmiotów, takich jak stowarzyszenia i fundacje, a także jednostki publiczne.

Autorzy szczegółowo omawiają nowe obowiązki administratorów wprowadzane przez rozporządzenie, w tym m.in.:

- zasady opracowania i wdrożenia nowych procedur oraz środków zapewniających bezpieczeństwo przetwarzanych danych osobowych,
- prowadzenie wewnętrznego rejestru czynności przetwarzania danych,
- przeprowadzenie analizy ryzyka,
- powołanie inspektora ochrony danych,
- obowiązek zgłaszania naruszeń w ciągu 72 godzin od wystąpienia nieprawidłowości.

Książka jest przeznaczona dla adwokatów, radców prawnych, jak również podmiotów publicznych, przedsiębiorców (w szczególności pracowników działów kadr, księgowości, marketingu i informatycznych) oraz fundacji i stowarzyszeń.



9788381240147 W01P01

ISBN 978-83-8124-014-7



9 788381 240147

#### **ZAMÓWIENIA:**

INFOLINIA 801 04 45 45, FAX 22 535 80 01

ZAMOWIENIA@WOLTERSKLUWER.PL

WWW.PROFINFO.PL