

Spis treści

Wykaz skrótów	XV
Wykaz literatury	XXI
Wprowadzenie	XXVII
Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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	1
Rozdział 1. Przedmiot i cele oraz podsumowanie zmian, które wprowadza RODO. Tło ochrony danych osobowych w Unii Europejskiej. Komentarz do art. 1 RODO	3
Art. 1. [Przedmiot i cele]	3
I. Przedmiot i cele RODO. Konsekwencje ujednolicenia przepisów o ochronie danych osobowych w skali Unii Europejskiej i bezpośredni wpływ reformy w Polsce	4
II. Podsumowanie zmian, które wprowadza RODO – największa od 21 lat reforma ochrony danych osobowych	6
III. Tło ochrony danych osobowych w Unii Europejskiej	11
Rozdział 2. Definicje prawa do prywatności. Zakres prawa do prywatności w prawie Unii Europejskiej i w orzecznictwie europejskim	15
I. Definicje prawa do prywatności. Ochrona danych osobowych jako aspekt tego prawa	15
II. Podstawy prawne prawa do prywatności i ochrony danych osobowych w UE	18
III. Zakres prawa do prywatności i ochrony danych osobowych w orzecznictwie europejskim	21
IV. Znaczenie ochrony danych osobowych dla prawa do prywatności	26
Rozdział 3. Zakres ochrony danych osobowych oraz kluczowe definicje. Komentarz do art. 2–4 RODO	29
Art. 2. [Materialny zakres stosowania]	29
I. Zakres podmiotowy ochrony danych osobowych	30

II. Zakres przedmiotowy ochrony danych osobowych – wpływ formy przetwarzania i przetwarzania w zbiorach	30
III. Przetwarzanie danych do celów osobistych lub domowych jako wyjątek od zakresu przedmiotowego	32
Art. 3. [Terytorialny zakres stosowania]	34
Art. 4. [Definicje]	36
I. Uwagi wstępne	40
II. Definicja danych osobowych – ewolucja kategorii danych chronionych wraz z rozwojem technologii	40
III. Anonimizacja i pseudonimizacja – różnice	47
IV. Zbiór danych	48
V. Przetwarzanie danych	49
Rozdział 4. Kluczowe zasady przetwarzania danych osobowych. Komentarz do art. 5 RODO	53
Art. 5. [Zasady dotyczące przetwarzania danych osobowych]	53
I. Uwagi ogólne – nadrzędność zasad przetwarzania danych osobowych	54
II. Zasada legalności, rzetelności i przejrzystości przetwarzania (<i>lawfulness, fairness and transparency</i>)	55
III. Zasada celowości (określenia i ograniczenia celu) (<i>purpose limitation</i>). Związanie celem przetwarzania m.in. w marketingu i monitoringu pracowników	59
IV. Zasada adekwatności (proporcjonalności) danych (<i>data minimisation</i>). Niezbędność jako warunek przetwarzania. Adekwatność danych m.in. w stosunkach pracy i monitoringu	65
V. Zasada prawidłowości danych (ściśłości) (<i>accuracy</i>). Ścisłość i aktualność danych	70
VI. Zasada ograniczenia czasowego (<i>storage limitation</i>). Analiza okresów retencji danych	72
Rozdział 5. Podstawy prawne przetwarzania danych osobowych. Komentarz do art. 6–8 RODO	79
Art. 6. [Zgodność przetwarzania z prawem]	79
Art. 7. [Warunki wyrażenia zgody]	81
Art. 8. [Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego]	81
I. Uwagi ogólne. Różnica między podstawami przetwarzania danych zwykłych i wrażliwych	82
II. Przetwarzanie danych na podstawie zgody osoby, której dotyczą	83
III. Warunki ważności zgody	85
IV. Forma zgody	88
V. Wycofanie zgody	89
VI. Zgoda dziecka na świadczenie usług społeczeństwa informacyjnego	90

VII. Przetwarzanie danych w celu zawarcia lub wykonania umowy	92
VIII. Przetwarzanie danych w celu spełnienia obowiązku prawnego	95
IX. Przetwarzanie danych w celu ochrony żywotnych interesów	97
X. Przetwarzanie danych w interesie publicznym	99
XI. Przetwarzanie danych osobowych w ramach prawnie uzasadnionych interesów administratora danych. Marketing i marketing elektroniczny oraz <i>cookies</i>	101
Rozdział 6. Dane wrażliwe. Komentarz do art. 9–10 RODO	109
Art. 9. [Przetwarzanie szczególnych kategorii danych osobowych]	109
Art. 10. [Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa]	111
I. Dane wrażliwe. Zakres i podstawy przetwarzania	111
II. Dane osobowe dotyczące wyroków skazujących i naruszeń prawa	114
Rozdział 7. Obowiązek zapewnienia informacji dotyczących przetwarzania danych. Komentarz do art. 11–14 RODO	115
Art. 11. [Przetwarzanie niewymagające identyfikacji]	115
Art. 12. [Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą]	115
Art. 13. [Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą]	121
Art. 14. [Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą]	122
I. Rozszerzenie klauzul informacyjnych	124
II. Wpływ informacji o przetwarzaniu na zgodność przetwarzania z prawem	127
III. Zakres klauzul informacyjnych	128
IV. Powstanie obowiązku informacyjnego	132
V. Wyłączenia od obowiązku informacyjnego	133
Rozdział 8. Prawo dostępu do danych, poprawiania danych oraz sprzeciwu wobec ich przetwarzania. Komentarz do art. 15–23 RODO	139
Art. 15. [Prawo dostępu przysługujące osobie, której dane dotyczą]	139
Art. 16. [Prawo do sprostowania danych]	140
Art. 17. [Prawo do usunięcia danych („prawo do bycia zapomnianym”)]	140
Art. 18. [Prawo do ograniczenia przetwarzania]	141
Art. 19. [Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania]	142
Art. 20. [Prawo do przenoszenia danych]	142

Art. 21. [Prawo do sprzeciwu]	142
Art. 22. [Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie]	143
Art. 23. [Ograniczenia]	144
I. Podstawy prawne i zakresy praw podmiotów danych (SAR – <i>Subject Access Requests</i>)	145
II. Prawo dostępu do danych (uzyskania na wniosek informacji o przetwarzaniu danych)	149
III. Prawo do korekty danych	153
IV. Prawo sprzeciwu wobec przetwarzania danych w szerokim znaczeniu	155
A. Prawo do usunięcia danych („prawo do bycia zapomnianym”)	156
B. Poinformowanie kolejnych administratorów o żądaniu usunięcia danych	161
C. Wyjątki od obowiązku usunięcia danych	162
V. „Prawo do bycia zapomnianym” w Internecie. Wyrok Trybunału Sprawiedliwości UE z 13.5.2014 r. w sprawie C-131/12	163
VI. Zapewnienie rzeczywistej skuteczności „prawu do bycia zapomnianym”	168
VII. Prawo do ograniczenia przetwarzania	170
VIII. Prawo do przenoszenia danych	172
IX. Prawo do sprzeciwu wobec przetwarzania danych ze względu na szczególną sytuację podmiotu danych oraz wobec marketingu bezpośredniego i profilowania	174
X. Profilowanie w celu marketingu i ocena ryzyka oraz inne zautomatyzowane decyzje	177
XI. Ograniczenie uprawnień podmiotów danych ze względu na interes publiczny	181
Rozdział 9. Administrator i processor. Ochrona danych w fazie projektowania i domyślna ochrona danych. Bezpieczeństwo danych. Zgłaszanie naruszeń. Inspektor ochrony danych. Kodeksy postępowania i certyfikacja. Komentarz do art. 24–43 RODO	183
Art. 24. [Obowiązki administratora]	183
Art. 25. [Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych]	184
Art. 26. [Współadministratorzy]	184
Art. 27. [Przedstawiciele administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii]	185
Art. 28. [Podmiot przetwarzający]	185
Art. 29. [Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego]	187
Art. 30. [Rejestrowanie czynności przetwarzania]	188
Art. 31. [Współpraca z organem nadzorczym]	189

Art. 32. [Bezpieczeństwo przetwarzania]	189
Art. 33. [Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu]	190
Art. 34. [Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych]	190
Art. 35. [Ocena skutków dla ochrony danych]	191
Art. 36. [Uprzednie konsultacje]	193
Art. 37. [Wyznaczenie inspektora ochrony danych]	194
Art. 38. [Status inspektora ochrony danych]	195
Art. 39. [Zadania inspektora ochrony danych]	195
Art. 40. [Kodeksy postępowania]	196
Art. 41. [Monitorowanie zatwierdzonych kodeksów postępowania]	198
Art. 42. [Certyfikacja]	199
Art. 43. [Podmiot certyfikujący]	200
I. Uwagi ogólne	201
II. Administrator. Kryteria uznania za administratora i relacje z innymi uczestnikami procesu przetwarzania	203
III. Współadministratorzy	205
IV. Podmiot przetwarzający (<i>processor</i>). Warunki wyboru processora i powierzenie przetwarzania	206
V. Ochrona danych w fazie projektowania i domyślna ochrona danych. Metody wdrożenia	208
VI. Adekwatność środków bezpieczeństwa danych w kontekście <i>risk-based approach</i> oraz technologii	210
VII. Rejestr czynności przetwarzania danych osobowych i <i>privacy impact assessment</i>	213
VIII. Upoważnienie do przetwarzania danych	215
IX. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu i podmiotowi danych	215
X. Inspektor ochrony danych	218
XI. Korzyści wynikające z wdrożenia branżowego kodeksu postępowania lub uzyskania certyfikatu	219
XII. Branżowe kodeksy postępowania	220
XIII. Certyfikacja	221
Rozdział 10. Transfery danych osobowych poza UE i EOG. Komentarz do art. 44–50 RODO	223
Art. 44. [Ogólna zasada przekazywania]	223
I. Definicja państw trzecich	223

II. Definicja przekazywania danych osobowych	226
III. Definicja odbiorcy danych	226
IV. Wyłączenie stosowania przepisów UE do zwrotu danych ich administratorowi w państwie trzecim	227
V. Umieszczenie danych osobowych na stronie internetowej jako wyjątek od przekazywania danych do państw trzecich	228
Art. 45. [Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony]	229
I. Odpowiedni stopień ochrony jako warunek transferu danych osobowych z UE	231
A. Definicja odpowiedniego stopnia ochrony danych osobowych	231
B. Kryteria oceny stopnia ochrony danych w państwie trzecim	234
II. Przekazywanie danych osobowych z UE do USA	238
A. Decyzje Komisji w sprawie adekwatności ochrony jako podstawy prawne transferów danych z UE do USA	238
B. Wyrok TSUE z 6.10.2015 r. w sprawie <i>Maximilian Schrems v. Data Protection Commissioner</i> (C-362/14) unieważniający <i>Safe Harbor</i> . Pozostałe zastrzeżenia do <i>Safe Harbor</i>	240
C. Zmiana podstawy prawnej transferów danych z UE do USA – unieważnienie EU-US <i>Safe Harbor</i> , przyjęcie EU-US <i>Privacy Shield</i>	243
D. Umowa między UE a USA o przekazywaniu danych z komunikatów finansowych w systemie SWIFT	247
E. Amerykańska ustawa o ujawnianiu informacji o rachunkach zagranicznych do celów podatkowych (FATCA)	251
F. Dane o pasażerach samolotów (<i>Passenger Name Record data</i> – PNR)	253
Art. 46. [Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń]	254
I. Wyjątki od zakazu transferu danych do państw trzecich niezapewniających odpowiedniego stopnia ochrony	255
II. Charakterystyka standardowych klauzul ochrony danych (standardowych klauzul umownych, <i>Standard Contractual Clauses</i> – SCCs)	258
III. Zezwolenie organu nadzorczego na transfer danych do państw trzecich niezapewniających adekwatnej ochrony (art. 46 ust. 3 RODO)	262
Art. 47. [Wiążące reguły korporacyjne]	265
I. Charakterystyka BCR	267
II. Zapewnienie skuteczności BCR	269
III. Procedura zatwierdzania BCR przez organy ochrony danych	271
Art. 48. [Przekazywanie lub ujawnianie niedozwolone na mocy prawa Unii]	276
Art. 49. [Wyjątki w szczególnych sytuacjach]	277
I. Odstępstwa od zakazu transferu danych do państw trzecich niezapewniających adekwatnej ochrony	279
II. Zgoda podmiotu danych	280
III. Realizacja umowy lub działania poprzedzające zawarcie umowy	282
IV. Ważne względy interesu publicznego	284
V. Ustalenie, dochodzenie lub ochrona roszczeń	285

VI. Ochrona żywotnych interesów w przypadku niezdolności do wyrażenia zgody	285
VII. Rejestry publiczne	286
Art. 50. [Międzynarodowa współpraca na rzecz ochrony danych osobowych]	286
Rozdział 11. Zakończenie. Prywatność w epoce Internetu, technologie a zagrożenia dla prywatności	289
I. Wyzwania dla ochrony prywatności wynikające z technologii	289
II. Ingerencja w prywatność jako cena za bezpieczeństwo i dostęp do usług	303
III. Konkluzja	309