

OCHRONA DANYCH OSOBOWYCH

PRZEWODNIK PO USTAWIE I RODO Z WZORAMI

redakcja Maciej Gawroński

Aleksander P. Czarnowski, Paweł Dmowski, Marcin Dominiak
Aleksandra Gawron, Maciej Gawroński, Adrianna Gnatowska
Michał Kibil, Katarzyna Kloc, Katarzyna Kunda
Patrycja Naklicka, Zuzanna Piotrowska, Paweł Punda
Tomasz Soczyński, Michał Sztąberek, Magdalena Wojtas

OCHRONA DANYCH OSOBOWYCH

PRZEWODNIK PO USTAWIE I RODO Z WZORAMI

redakcja Maciej Gawroński

Aleksander P. Czarnowski, Paweł Dmowski, Marcin Dominiak
Aleksandra Gawron, Maciej Gawroński, Adrianna Gnatowska
Michał Kibil, Katarzyna Kloc, Katarzyna Kunda
Patrycja Naklicka, Zuzanna Piotrowska, Paweł Punda
Tomasz Soczyński, Michał Sztąberek, Magdalena Wojtas

Zamów książkę w księgarni internetowej

proinfo.pl
księgarnia internetowa

Stan prawny na 1 października 2018 r.

Wydawca
Monika Pawłowska

Redaktor prowadzący
Joanna Ołówek

Opracowanie redakcyjne
Michał Dymiński

Łamanie
Fotoedytor

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegał przysługujących im praw. Książkę możesz udostępnić osobom bliskim lub osobiście znanym, 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
POLSKA IZBA KSIĄŻKI

© Copyright by
Wolters Kluwer Polska Sp. z o.o., 2018

ISBN 978-83-8160-187-0

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

Wykaz skrótów	37
---------------------	----

Wstęp	39
-------------	----

Część A

Kompedium ochrony danych osobowych

Rozdział I

Zgodność podstawowa	43
---------------------------	----

1. RODO – unijna „ustawa” o ochronie danych osobowych – <i>Katarzyna Kloc, Maciej Gawroński</i>	43
1.1. RODO – nowa „ustawa” o ochronie danych osobowych	43
1.2. Przedmiot i cel RODO	44
1.2.1. Uwagi wstępne	44
1.2.2. Ochrona osób fizycznych	45
1.2.3. Bezpośredniość	45
1.2.4. Konsekwencje dla polskich przedsiębiorców ...	46
1.3. Prywatność, prawa, bezpieczeństwo – filary RODO ...	46
1.4. Wymagania RODO	48
1.4.1. Ogólnikowość	48
1.4.2. Mierzalność	49
1.4.3. Bezpośredniość	50
1.4.4. Surowość	50
1.4.5. Domniemanie winy	51
1.5. Podział funkcjonalny RODO	52
2. Przedmiotowy i terytorialny zakres stosowania RODO – <i>Katarzyna Kloc, Maciej Gawroński</i>	56

2.1. Zakres stosowania RODO	56
2.1.1. Zakres przedmiotowy	56
2.1.2. Wyłączenia stosowania RODO	59
2.1.3. Zakres terytorialny	60
3. Rodosłowniczek, czyli omówienie podstawowych pojęć RODO wraz z przykładami – <i>Patrycja Naklicka,</i> <i>Aleksandra Gawron</i>	63
3.1. Uwagi wstępne	63
3.2. Administrator	63
3.3. Analiza ryzyka	65
3.4. Anonimizacja	65
3.5. Czynności przetwarzania danych	66
3.6. Dane osobowe	66
3.7. Kategorie danych osobowych	68
3.8. Rodzaj danych osobowych	73
3.9. Eksport danych / Transfer danych	73
3.10. GIODO i PUODO	74
3.11. Grupa Robocza Art. 29 i Europejska Rada Ochrony Danych	74
3.12. Inspektor ochrony danych	75
3.13. Naruszenie ochrony danych osobowych	75
3.14. Ocena skutków dla ochrony danych	76
3.15. Odbiorca danych	76
3.16. Ograniczenie przetwarzania	77
3.17. Operacje przetwarzania danych	78
3.18. Osoba, której dane dotyczą	80
3.19. Personel	81
3.20. Podmiot przetwarzający	81
3.21. Przetwarzanie	83
3.22. Pseudonimizacja	85
3.23. Rejestr czynności przetwarzania danych	86
3.24. Ryzyko	86
3.25. Ustawa o ochronie danych osobowych	87
3.26. Współadministrowanie	88
4. Zasady przetwarzania danych osobowych – <i>Marcin Dominiak, Maciej Gawroński</i>	90
4.1. Wprowadzenie	90
4.1.1. Zasady materialne	91

4.1.2. Zasada formalna – rozliczalność	91
4.1.3. Bliżej o zasadach ochrony danych	92
4.2. Zasada legalności, rzetelności i przejrzystości przetwarzania (zgodności z prawem)	93
4.2.1. Legalność	93
4.2.2. Rzetelność	94
4.2.3. Przejrzystość	94
4.3. Zasada celowości	95
4.4. Zasada minimalizacji danych (adekwatności, proporcjonalności)	96
4.5. Zasada prawidłowości (poprawności)	98
4.6. Zasada ograniczenia czasowego (czasowości)	99
4.7. Zasada bezpieczeństwa (integralności i poufności danych)	103
4.7.1. Poufność	103
4.7.2. Integralność	104
4.7.3. Dostępność	104
4.7.4. Odpowiedniość	105
4.8. Zasada rozliczalności	107
5. Podstawy prawne przetwarzania danych osobowych – <i>Maciej Gawroński, Michał Sztąberek</i>	107
5.1. Wstęp	107
5.2. Dane osobowe „zwykłe” – art. 6–8 RODO	108
5.2.1. Zgoda jako podstawa przetwarzania danych ...	109
5.2.1.1. Wstęp	109
5.2.1.2. Zgoda jako podstawa prawna	110
5.2.1.3. Zgoda dziecka	110
5.2.2. Zawarcie i wykonywanie umowy	111
5.2.2.1. Działania przed zawarciem umowy ...	112
5.2.2.2. Wykonywanie umowy	112
5.2.2.3. Przetwarzanie danych osoby trzeciej ...	112
5.2.3. Obowiązek prawny	113
5.2.4. Ochrona żywotnych interesów	115
5.2.5. Zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej	116
5.2.6. Uzasadniony interes administratora danych lub strony trzeciej	118
5.3. Wybór podstawy przetwarzania	121

6. Artykuły 9 i 10 RODO – dane szczególnych kategorii i dane „karne” – <i>Maciej Gawroński, Michał Sztąberek</i>	122
6.1. Przesłanka zgody	124
6.2. Przetwarzanie wynikające ze stosunku pracy jest dozwolone prawem	125
6.3. Ochrona żywotnych interesów	126
6.4. Stowarzyszenie się	126
6.5. Dane upublicznione	126
6.6. Sprawy sądowe	126
6.7. Na podstawie prawa dla ważnego interesu publicznego	127
6.8. Dane „karne”	128
7. Zgoda – cechy oraz warunki wyrażenia zgody – <i>Maciej Gawroński</i>	129
7.1. Definicja zgody	129
7.1.1. Dobrowolność zgody	129
7.1.2. Konkretność zgody	134
7.1.3. Świadomość zgody	134
7.1.4. Jednoznaczność zgody	135
7.2. Warunki wyrażenia zgody	136
7.2.1. Rozliczalność – forma udzielonej zgody	137
7.3. Retencja (okres ważności zgody)	139
7.4. Równość cofnięcia zgody	139
7.5. Ważność „starych” zgód	140
7.6. Wyrażna zgoda	140
7.7. Zgoda dziecka na usługi społeczeństwa informacyjnego (np. media społecznościowe)	141
7.8. Zgoda jako pozorna podstawa prawna	143
8. Administrator i podmiot przetwarzający – <i>Maciej Gawroński, Katarzyna Kloc, Magdalena Wojtas</i>	144
8.1. Wstęp	144
8.2. Administrator danych osobowych – definicja, cechy, obowiązki	145
8.2.1. Definicja	145
8.2.2. Każdy jest ADO	146
8.2.3. Co przesądza, że dany podmiot jest ADO?	147
8.2.4. Decydowanie o celach i środkach przetwarzania	147

8.2.5. Praktyczny test ADO	148
8.2.6. Rola ADO	148
8.2.7. Obowiązki ADO	149
8.3. Podmiot przetwarzający – definicja, cechy, rola i obowiązki	151
8.3.1. Definicja	151
8.3.2. Rola podmiotu przetwarzającego	151
8.3.3. Wiarygodność i wystarczające gwarancje	151
8.3.4. Umowa z ADO	152
8.3.5. Obowiązki wynikające z umowy z ADO	152
8.3.6. Obowiązki wynikające z RODO	155
8.4. Porównanie roli i obowiązków ADO i podmiotu przetwarzającego	156
9. Przetwarzanie danych niewymagające identyfikacji – <i>Maciej Gawroński</i>	157
9.1. Wprowadzenie	157
9.2. Brak obowiązku identyfikacji	159
9.3. Brak obowiązku monitorowania	161
9.4. Obowiązki informacyjne	161
9.4.1. Obowiązek poinformowania osób „niezidentyfikowanych” o niemożności zidentyfikowania – jeśli to możliwe	162
9.4.2. Umożliwienie wykonania praw jednostki	164
9.4.3. Bezpieczeństwo	165
9.4.4. Minimalizacja (dostępu i czasu)	165
10. Rejestrowanie czynności przetwarzania danych – <i>Katarzyna Kloc</i>	166
10.1. Własny rejestr zamiast zgłaszania do GIODO	166
10.2. RCPD – podstawa rozliczalności	167
10.3. Czynność przetwarzania danych	167
10.4. Czynności realizowane w tym samym celu	168
10.5. Czynności klasyfikowane w inny sposób	170
10.6. RCPD dla „małych” i „dużych” – różnice	171
10.6.1. Czy każdy musi prowadzić RCPD?	172
10.6.2. Zatrudnienie 250 osób	173
10.6.3. Przetwarzanie wysokiego ryzyka	173
10.7. Zakres informacji w RCPD – administratorzy danych	174

10.8.	Zakres informacji w RCPD – podmioty przetwarzające dane	177
10.9.	Forma RCPD	178
10.10.	Osoba odpowiedzialna za prowadzenie RCPD	178
11.	Przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej (eksport danych lub transfer danych) – <i>Maciej Gawroński</i>	179
11.1.	Reglamentacja eksportu danych	179
11.2.	Praktyczne utrudnienie eksportu danych	180
11.3.	Legalność eksportu danych	181
11.4.	Podstawy eksportu danych	181
11.5.	Dodatkowe podstawy przekazania	182
11.6.	Przekazanie „naprawdę wyjątkowe”	183
11.7.	Zarejestrowanie przekazania wyjątkowego	184
11.8.	Zakaz sądowej samopomocy – ucinanie „długiej ręki”..	184
11.9.	Podsumowanie	184
12.	Przetwarzanie transgraniczne, czyli właściwość wiodącego organu nadzorczego (art. 4 pkt 16 i 23, art. 56 RODO) – <i>Maciej Gawroński</i>	186
12.1.	Wstęp	186
12.2.	<i>One-stop-shop</i>	187
12.3.	Przetwarzający	187
12.4.	Administratorzy	188
12.4.1.	Przetwarzanie lokalne	189
12.4.2.	Zasięg lokalny	190
12.5.	Tryb pilny	190
12.6.	Prawo holdingowe	190
12.7.	Wytyczne Grupy Roboczej Art. 29	190
12.8.	Wnioski	191
13.	Współadministrowanie danymi osobowymi – <i>Maciej Gawroński</i>	191
13.1.	Wstęp	191
13.2.	Przykłady współadministrowania danymi	192
13.3.	Czy unikać współadministrowania?	193
13.4.	Obowiązki współadministratorów	194
13.5.	Umowa o współadministrowanie	195
13.6.	Treść umowy, analogia do powierzenia danych	195
13.7.	Ujawnienie podmiotom danych	196

13.8. Transgraniczne współadministrowanie	196
13.9. Wnioski	196
14. Kodeksy postępowania i certyfikacja (art. 40 i n. RODO) – Paweł Punda, Aleksander P. Czarnowski, Maciej Gawroński	197
14.1. Wstęp	197
14.2. Kodeksy	198
14.2.1. Opracowanie	198
14.2.2. Zatwierdzanie	199
14.3. Certyfikacja	199
14.3.1. Schematy certyfikacyjne	199
14.3.2. Prace legislacyjne	199
14.4. Korzyści	200
14.5. Projekty kodeksów	202
14.6. Certyfikacja prywatna	202

Rozdział II

Prawa jednostki	204
1. Obsługa praw jednostki (art. 12 RODO) – Maciej Gawroński, Michał Kibil	204
1.1. Wstęp	204
1.2. Czytelność komunikowania się	205
1.2.1. Czytelnie i zwięźle	205
1.2.2. Kompletność	206
1.2.3. Niecytowanie przepisów	206
1.2.4. Dzieci	206
1.2.5. Test Kowalskiego	206
1.3. Uwierzytelnienie	207
1.3.1. Potwierdzenie tożsamości	207
1.3.2. Pogłębione uwierzytelnienie	209
1.4. Forma komunikacji	209
1.5. Ułatwianie	210
1.6. Obsługa danych niezidentyfikowanych	210
1.7. Czas reakcji i czas obsługi	211
1.8. Nieuzasadnione lub nadmierne żądania	212
1.8.1. Nieuzasadnione żądanie	214
1.8.2. Nadmierne żądanie	214
1.9. Schemat działania administratora	215

2. Prawo do informacji i obowiązek informacyjny (art. 13 i 14 RODO) – <i>Maciej Gawroński</i>	215
2.1. Uwagi wstępne	215
2.2. Zakres informacji	216
2.2.1. Pozyskiwanie od osoby	216
2.2.2. Pozyskiwanie nie od osoby	217
2.2.3. Zmiana celu	218
2.2.4. Prawo dostępu	218
2.3. Szczegóły informacji	218
2.3.1. Podstawa prawna	218
2.3.2. Kategorie odbiorców i odbiorcy	218
2.3.3. Eksport danych	219
2.3.4. Profilowanie	221
2.4. Kiedy i jak informować	221
2.4.1. Kiedy informować?	221
2.4.1.1. Podczas pozyskiwania od osoby	221
2.4.1.2. W ciągu miesiąca – z innych źródeł ..	222
2.4.1.3. Aktualizacja informacji	222
2.4.1.4. Informowanie osób niezidentyfikowanych (art. 11 ust. 2 RODO)	223
2.4.2. Jak informować?	223
2.4.2.1. Przejrzystość	223
2.4.2.2. Dostępność	224
2.4.2.3. Konkretność	225
2.5. Wyjątki od obowiązku informowania	226
3. Prawo dostępu do danych (art. 15 RODO) – <i>Maciej Gawroński, Michał Sztąberek</i>	227
3.1. Wstęp	227
3.2. Terminy	228
3.3. Informacje	228
3.4. Dostęp	229
3.5. Kopia danych	229
3.6. Prośba o sprecyzowanie	230
3.7. Odmowa	231
3.8. Prawa innych	231
3.9. Uwierzytelnienie i komunikacja	233
3.10. Regulaminy i procedury	234

3.11. Mapowanie danych, narzędzia eksploracji danych (<i>data mining</i>), narzędzia do tzw. ticketowania	234
3.12. Podsumowanie	234
4. Prawo do sprostowania danych (art. 16 RODO) – <i>Maciej Gawroński, Michał Sztąberek</i>	235
4.1. Wstęp	235
4.2. Zagadnienia ogólne – tryb uwierzytelnienia i komunikacji	235
4.2.1. Element sporu	236
4.2.2. Prawo do skargi	236
4.2.3. Styl	236
4.2.4. Wykazanie nieprawidłowości danych	237
4.2.5. Dane nieaktualne czy nieprawidłowe	237
4.2.6. Zakres korekty danych	237
4.3. Uzupełnienie danych niekompletnych	238
4.3.1. Adekwatność danych	238
4.3.2. Podstawa aktualizacji	238
4.4. Obowiązek powiadomienia	239
5. Prawo do usunięcia danych, prawo do bycia zapomnianym (art. 17 RODO) – <i>Maciej Gawroński, Katarzyna Kunda</i>	240
5.1. Historia prawa do bycia zapomnianym	240
5.2. Składniki prawa do bycia zapomnianym	242
5.3. Podstawy żądania usunięcia danych	242
5.3.1. Zbędność do celów przetwarzania	243
5.3.2. Cofnięcie zgody	243
5.3.3. Wniesienie sprzeciwu	244
5.3.4. Przetwarzanie niezgodne z prawem	245
5.3.5. Prawny obowiązek usunięcia danych	246
5.3.6. Oferowanie usług społeczeństwa informacyjnego dzieciom	246
5.4. Wyjątki	246
5.4.1. Korzystanie z prawa do wolności wypowiedzi i informacji	247
5.4.2. Wywiązanie się z obowiązku prawnego lub zadania realizowanych w interesie publicznym albo w ramach wykonywania władzy publicznej	248

5.4.3. Interes publiczny w ochronie zdrowia publicznego	248
5.4.4. Cele archiwalne, badania naukowe, historyczne, cele statystyczne	249
5.4.5. Ustalenie, dochodzenie, obrona roszczeń	250
5.5. Zakres usunięcia danych	250
5.6. Przetwarzanie w celu realizacji prawa do usunięcia danych i prawa do bycia zapomnianym	252
5.7. Przetwarzanie w celu zapewnienia bezpieczeństwa – problem kopii zapasowych i archiwalnych	253
5.7.1. Jak wszyscy, to wszyscy	253
5.7.2. Problem bezpieczeństwa i ciągłości działania	253
5.7.3. Problem rozliczalności	254
5.7.4. Problem praktyczny – zasoby i proces	254
5.7.5. Rozwiązywanie	255
5.8. Problem danych nieustrukturyzowanych	256
5.9. Obowiązek powiadomienia	258
5.10. Poinformowanie innych administratorów	258
5.11. Ograniczenie obowiązku poinformowania	259
5.12. Listy kontrolne	259
5.12.1. Przygotowanie do RODO – wprowadzenie prawa do bycia zapomnianym do organizacji	259
5.12.2. Przetworzenie żądania usunięcia danych ...	260
6. Prawo do ograniczenia przetwarzania (art. 18 RODO) – <i>Michał Sztąberek, Maciej Gawroński</i>	261
6.1. Ograniczenie przetwarzania	261
6.2. Prawo do ograniczenia przetwarzania	261
6.2.1. Ograniczenie w razie sporu co do prawidłowości danych	262
6.2.2. Ograniczenie w razie niezgodności z prawem	263
6.2.3. Ograniczenie dla potrzeb roszczeń	263
6.2.4. Ograniczenie w razie sprzeciwu ze względu na szczególną sytuację	264
6.3. Sposób zastosowania się do żądania ograniczenia przetwarzania	264

7. Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO) – <i>Aleksander P. Czarnowski, Maciej Gawroński, Paweł Punda</i>	265
7.1. Obowiązek śledzenia danych	265
7.2. Odbiorca danych na gruncie art. 19 RODO	266
7.3. Obowiązek informacyjny na żądanie	266
8. Prawo do przenoszenia danych, czyli jak przenieść dane od jednego administratora danych do drugiego (art. 20 RODO) – <i>Aleksander P. Czarnowski, Maciej Gawroński, Paweł Punda</i>	267
8.1. Wstęp	267
8.2. Na czym dokładnie polega prawo przenoszenia danych?	268
8.3. Kiedy można skorzystać z prawa do przenoszenia danych?	269
8.4. Jaki zakres danych należy przekazać?	269
8.5. W jaki sposób należy zrealizować prawo do przeniesienia danych?	271
8.5.1. Wyjątki	273
8.5.2. Prawa osób trzecich	274
8.5.3. Przenoszenie danych, które są równocześnie danymi wnioskodawcy i danymi innej osoby ...	275
8.6. Kogo przenoszenie danych dotyczy najbardziej?	276
8.6.1. Bezpieczeństwo	276
8.6.2. Kwestia techniczna	277
9. Prawo do sprzeciwu (art. 21 RODO) – <i>Maciej Gawroński, Michał Sztąberek</i>	277
9.1. Prawo do sprzeciwu	277
9.2. Sprzeciw ze względu na szczególną sytuację osoby ...	279
9.2.1. Prawnie uzasadnione interesy	280
9.2.2. Roszczenia i spory	281
9.2.3. Interes publiczny lub władza publiczna	282
9.3. Przetwarzanie danych na potrzeby marketingu bezpośredniego	283
9.3.1. Sprzeciw względem marketingu bezpośredniego a cofnięcie zgody na przetwarzanie	284

9.3.2. Sprzeciw względem marketingu bezpośredniego a zgoda na zdalną komunikację marketingową	284
9.4. Skuteczne wniesienie sprzeciwu na przetwarzanie danych	285
9.5. Jak powinien być składany sprzeciw	286
10. Profilowanie i automatyczne podejmowanie decyzji (art. 22 RODO) – <i>Michał Kibil</i>	286
10.1. Wstęp	286
10.2. Definicja profilowania z RODO	291
10.2.1. Automatyzacja	292
10.2.2. Dane osobowe	292
10.2.3. Efekt	292
10.2.4. Czynności traktowane jako profilowanie ...	293
10.3. Obowiązki administratora danych osobowych związane z profilowaniem lub automatycznym podejmowaniem decyzji, lub podejmowaniem decyzji w oparciu o profilowanie	294
10.3.1. Obowiązki ogólne administratora	295
10.3.1.1. Informowanie o decydowaniu automatycznym i w oparciu o profilowanie	295
10.3.1.2. Ile razy informować	296
10.3.1.3. Zmiana celu	296
10.3.1.4. Profilowanie danych ze „starej” ustawy o ochronie danych osobowych	296
10.3.2. Prawo sprzeciwu	296
10.4. Profilowanie a podejmowanie zautomatyzowanych decyzji	297
10.4.1. Środki bezpieczeństwa	299
10.4.2. Kiedy można stosować decyzje zautomatyzowane lub oparte wyłącznie na profilowaniu	300
10.4.2.1. Prawo do ludzkiej interwencji	302
10.4.2.2. Proces reklamacyjny	303
10.4.2.3. Automatyczne uwierzytelnienie ...	303
10.4.3. Profilowanie dzieci	304

10.4.4. Zautomatyzowane decyzje dotyczące danych wrażliwych	304
10.4.5. Wnioski	305

Rozdział III

Bezpieczeństwo	306
1. Bezpieczeństwo danych w świetle RODO – analiza ryzyka i adekwatność środków – <i>Aleksander P. Czarnowski, Maciej Gawroński</i>	306
1.1. Bezpieczeństwo odpowiednie do ryzyka	306
1.1.1. Ryzyko	307
1.1.2. Ryzyko naruszenia praw lub wolności	308
1.1.3. Analiza ryzyka	309
1.2. Elementy oceny adekwatności środków bezpieczeństwa danych	312
1.2.1. Stan wiedzy technicznej	313
1.2.2. Koszt	313
1.2.3. Cechy samego przetwarzania	314
1.2.4. Ryzyko naruszenia praw lub wolności	314
1.3. Nie trzeba wymyślać procesu samemu?	321
1.4. Środki bezpieczeństwa	323
1.5. Jak z tego wybrnąć na skrót?	325
2. Pseudonimizacja i szyfrowanie – preferowane środki zabezpieczania danych osobowych – <i>Aleksander P. Czarnowski, Maciej Gawroński, Paweł Punda</i>	326
2.1. Uwagi wstępne	326
2.2. Szyfrowanie	326
2.3. Pseudonimizacja	329
2.4. Anonimizacja	330
2.5. Pseudonimizacja czy szyfrowanie	330
2.5.1. Bezpieczeństwo	331
2.5.2. Analiza ryzyka	332
2.5.2.1. Ocena skutków dla ochrony danych ...	334
2.5.2.2. Metodyka analizy ryzyka	335
2.6. <i>Privacy by design</i>	337
2.7. Notyfikacja naruszeń ochrony danych	337

2.8. Zastosowania biznesowe pseudonimizacji	338
2.9. Podsumowanie	339
3. <i>Privacy by design</i> , czyli projektowanie prywatności – Maciej Gawroński, Katarzyna Kunda	339
3.1. <i>Privacy by design</i>	339
3.1.1. Z czego się składa projektowanie prywatności ..	341
3.1.1.1. Bezpieczeństwo	342
3.1.1.2. Pseudonimizacja	343
3.1.1.3. Minimalizacja	344
3.1.1.4. Prawa jednostki i czasowość	344
3.1.2. Jak wdrożyć <i>privacy by design</i> w organizacji? .	345
3.1.2.1. Projektowanie prywatności w konkretnym projekcie	345
3.1.2.2. Zasady projektowania prywatności ..	345
3.1.2.3. Od kiedy projektować prywatność ...	346
3.2. Certyfikacja projektowania prywatności i domyślnej prywatności	346
4. <i>Privacy by default</i> , czyli domyślna ochrona danych – minimalizacja – Maciej Gawroński, Katarzyna Kunda	347
4.1. Zasada <i>privacy by default</i>	347
4.2. <i>Privacy by default</i> , czyli minimalizacja	347
4.3. Atrybuty domyślnej prywatności	348
4.4. Wskazówki praktyczne	349
4.5. Udostępnianie nieokreślonej liczbie osób	350
4.6. Certyfikacja projektowania prywatności i domyślnej prywatności	351
5. Ocena skutków dla ochrony danych krok po kroku – Katarzyna Kloc	351
5.1. Uwagi wstępne	351
5.2. „Kwalifikowana” analiza ryzyka i rozliczalność	352
5.3. Podobne procesy, jedna DPIA	354
5.4. Analiza ryzyka do kwadratu	355
5.4.1. Analiza ryzyka	355
5.4.2. Jak w praktyce można przeprowadzić analizę ryzyka pierwszego stopnia i mieć wstępny przegląd operacji wymagających DPIA?	356
5.5. DPIA – kiedy trzeba?	357
5.5.1. Duża skala	358

5.5.2. Wytyczne Grupy Roboczej Art. 29	360
5.6. Jak określić, czy w naszej firmie należy przeprowadzić DPIA i w odniesieniu do których procesów?	363
5.6.1. Urzędowy katalog operacji DPIA	364
5.7. Kiedy nie trzeba przeprowadzać DPIA?	372
5.8. DPIA krok po kroku	373
5.8.1. Uwagi ogólne	373
5.8.2. IOD	376
5.8.3. Eksperti	376
5.8.4. Reprezentanci grup docelowych	376
5.8.5. Uprzednie konsultacje z organem nadzorczym ..	377
5.9. Wytyczne GODO	378
5.9. Podsumowanie	378

Rozdział IV

Przetwarzający dane	380
1. Powierzenie danych oraz elementy nowej umowy powierzenia danych – <i>Aleksander P. Czarnowski,</i> <i>Maciej Gawroński, Patrycja Naklicka</i>	380
1.1. Uwagi wstępne	380
1.2. Opis gwarancji zgodności	380
1.3. Pisemna umowa	381
1.4. Zgoda na podpowierzenie danych	381
1.5. Transfer obowiązków na podprzetwarzającego	382
1.6. Zakaz „wydmuszki”	382
1.7. Przedmiot przetwarzania	383
1.8. Pisemność poleceń ADO	383
1.9. Zobowiązania do poufności	383
1.10. Bezpieczeństwo danych	384
1.11. Obsługa praw jednostki	384
1.12. Wsparcie obowiązków bezpieczeństwa administratora	384
1.13. Notyfikacja podejrzenia naruszenia ochrony danych ..	385
1.14. Usuwanie i zwrot danych	385
1.15. Obowiązek rozliczenia się ze zgodności z umową ...	387
1.16. Podleganie audytom	387
1.17. Odpłatność	388

1.18. Informowanie o legalności poleceń	388
1.19. Procedura rozstrzygania legalności	388
1.20. Zasady odpowiedzialności	389
1.21. Wyznaczanie inspektora ochrony danych	390
2. Powierzenie danych oraz elementy nowej umowy powierzenia danych – <i>Aleksander P. Czarnowski,</i> <i>Maciej Gawroński, Patrycja Naklicka</i>	390
2.1. Umowy powierzenia a umowy SLA	390
2.1.1. Dostępność systemu SLA i czas reakcji	391
2.1.2. SLA w praktyce	391
2.1.3. Standaryzacja umów SLA a zgodność z RODO ..	391
2.2. Nowe wyzwania dla administratora i procesora	392
2.3. Rekomendacje	393

Rozdział V

Zarządzanie incydentami	394
1. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorcemu (art. 33 RODO) – <i>Maciej Gawroński, Zuzanna Piotrowska</i>	394
1.1. Przepis	394
1.2. Co to jest naruszenie ochrony danych osobowych? ...	395
1.2.1. Naruszenie ochrony danych wg Grupy Roboczej Art. 29	397
1.2.1.1. Naruszenie poufności	397
1.2.1.2. Naruszenie dostępności	398
1.2.1.3. Naruszenie integralności	398
1.3. Czy każde naruszenie trzeba zgłaszać?	398
1.3.1. Procedura zgłaszania	399
1.3.1.1. Termin dla administratora	399
1.3.1.2. Termin dla przetwarzającego	400
1.3.2. Stwierdzenie naruszenia	400
1.3.3. Zgłoszenie – treść i forma	402
1.3.4. Powiadamianie z opóźnieniem	403
1.3.5. Obowiązki podmiotu przetwarzającego	404
1.4. Kiedy mimo wystąpienia incydentu naruszenia ochrony danych nie trzeba powiadamiać organu nadzorczego?	404
1.4.1. Kwestie praktyczne	407

1.4.2. Dokumentowanie naruszeń	407
1.4.3. Sankcja administracyjna	409
1.5. Elementy systemu zgłaszania naruszeń	410
2. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych (art. 34 RODO) – <i>Katarzyna Kloc,</i> <i>Maciej Gawroński</i>	410
2.1. Wstęp	410
2.2. Wysokie ryzyko naruszenia praw lub wolności	411
2.2.1. Prawa i wolności	411
2.3. Wyjątki od obowiązku zawiadomienia	413
2.3.1. Działania prewencyjne	414
2.3.2. Działania następcze	414
2.4. Zawiadomienie	414
2.4.1. Treść zawiadomienia	414
2.4.2. Forma zawiadomienia	415
2.4.3. Ogłoszenie w miejscu zawiadomienia	416
2.4.4. Termin zawiadomienia	416
2.5. Uzgodnienia z organem nadzorczym	417

Rozdział VI

Inspektor ochrony danych (IOD)	418
1. Inspektor ochrony danych – wyznaczenie i status – <i>Michał Kibil, Maciej Gawroński</i>	418
1.1. IOD – ewolucja czy rewolucja	418
1.2. Kto ma obowiązek wyznaczenia inspektora ochrony danych?	419
1.2.1. Organ lub podmiot publiczny	420
1.2.2. Działalność wymagająca systematycznego i regularnego monitorowania oraz przetwarzanie na dużą skalę	421
1.2.2.1. Główna działalność	421
1.2.2.2. Monitorowanie osób	422
1.3. Działanie w ramach zrzeczeń i grup przedsiębiorców ..	426
1.4. Kwalifikacje IOD	427
1.5. Zatrudnienie IOD	428
1.6. Status inspektora danych	429
1.6.1. Obowiązki administratora względem IOD ...	429
1.6.2. Niezależność IOD	431

2. Zadania inspektora ochrony danych osobowych	
– <i>Michał Kibil, Maciej Gawroński</i>	432
2.1. Wstęp	432
2.2. Informacje poufne oraz unikanie konfliktu interesów ..	432
2.3. Zadania inspektora ochrony danych	434

Rozdział VII

Regulator	437
1. Organ nadzorczy – status, rola i obowiązki – <i>Katarzyna Kunda, Patrycja Naklicka, Zuzanna Piotrowska</i>	437
1.1. Niezależność	437
1.2. Cechy i gwarancje niezależności	438
1.3. Członkowie organu nadzorczego	439
1.3.1. Wybór	439
1.3.2. Okres kadencji – konflikt interesów	440
1.4. Rola organu nadzorczego	440
1.4.1. Kompetencje z art. 57 RODO	440
1.5. Bezpłatność	441
2. Uprawnienia organu nadzorczego z zakresu ochrony danych osobowych – <i>Katarzyna Kunda, Patrycja Naklicka, Zuzanna Piotrowska</i>	442
2.1. Wstęp	442
2.2. Uprawnienia kontrolne	442
2.2.1. Rodzaje i techniki kontroli	442
2.2.2. Przebieg kontroli	443
2.2.3. Zakres kontroli	443
2.2.4. Uprawnienia pokontrolne	445
2.2.5. Obowiązek zachowania tajemnicy	445
2.3. Kary przewidziane przez RODO	445
2.4. Udzielanie zezwoleń i kompetencje doradcze	446
2.5. Obowiązek rozpatrywania skarg przez PUODO	446

Rozdział VIII

Środki ochrony prawnej, odpowiedzialność i sankcje	447
1. Środki ochrony prawnej – odpowiedzialność cywilnoprawna i administracyjna – <i>Maciej Gawroński</i> ...	447
1.1. Wstęp	447
1.2. Skarga do organu nadzorczego	448

1.3. Skarga do sądu (administracyjnego) na organ nadzorczy	449
1.4. Odpowiedzialność cywilnoprawna – żądanie zaniechania lub zachowania	450
1.4.1. Prawo do sądu	450
1.4.2. Właściwość miejscowa sądu	451
1.4.3. Tryb procesowy	451
1.5. Odpowiedzialność odszkodowawcza	451
1.5.1. Szkoda majątkowa i niemajątkowa	452
1.5.2. Administrator i przetwarzający	452
1.5.3. Uwolnienie się od odpowiedzialności	452
1.5.4. Domniemanie winy	454
1.5.5. Współodpowiedzialność	454
1.5.6. Właściwość sądu	455
1.5.7. Proces cywilny	455
1.6. Reprezentacja podmiotów danych przez wyspecjalizowane podmioty	455
2. Sankcje administracyjne za naruszenie przepisów RODO – <i>Maciej Gawroński</i>	456
2.1. Wstęp	456
2.2. Komu grożą kary?	456
2.3. Jakie powinny być kary?	456
2.4. Kara większa i kara mniejsza	456
2.5. Księgowość karania	458
2.6. Konfiskata korzyści z „rodoprzestępstwa”	459
3. Odpowiedzialność podmiotu przetwarzającego – <i>Maciej Gawroński</i>	460

Rozdział IX

Nowa ustawa o ochronie danych osobowych – rola i miejsce

w porządku prawnym po 25.05.2018 r. – <i>Katarzyna Kloc</i>	462
1. Wprowadzenie	462
2. Porządek prawny przed 25.05.2018 r.	462
3. Planowane zmiany – przepisy sektorowe	464
4. Rola nowej ustawy o ochronie danych osobowych	465
5. Niewielki zakres obowiązywania ustawy o ochronie danych osobowych z 1997 r.	466
6. Podsumowanie	467

Rozdział X**Wyjątek dziennikarski (art. 2), cz. 1 – Maciej Gawroński,**

<i>Katarzyna Kunda, Katarzyna Kloc</i>	468
1. Wolność wypowiedzi i informacji a RODO	468
1.1. Wyłączenia – podstawa w RODO	469
1.2. Pogodzenie przepisów regulujących wolność wypowiedzi i informacji z RODO w polskim porządku prawnym	471
2. Wyjątek dziennikarski, działalność artystyczna i literacka a RODO	472
2.1. Wyjątek dziennikarski – wyłączenia dla dziennikarzy ..	473
2.2. Waga wyłączenia w przypadku dziennikarzy	474
2.3. Wyłączenia dla pisarzy i artystów – działalność literacka i artystyczna	475
2.4. Zakres wyłączenia stosowania RODO	476
2.5. Wyłączenia w zakresie podstawowych zasad	477

Rozdział XI**Wyjątek dziennikarski (art. 2), cz. 2 – Maciej Gawroński,**

<i>Katarzyna Kunda, Katarzyna Kloc</i>	479
1. Wyłączenia w zakresie obsługi praw jednostki	479
2. Wyłączenia w zakresie obowiązków przy powierzeniu przetwarzania	482
3. Wyłączenia w zakresie rejestru czynności przetwarzania danych	483
4. Przepisy RODO stosowane do dziennikarzy, literatów i artystów	483
4.1. Przetwarzanie danych karnych	484
4.2. Bezpieczeństwo	484
4.3. Inspektor ochrony danych	485
4.4. Współadministrowanie	485
4.5. Transfer danych poza EOG	485
4.6. Odpowiedzialność	486
5. Wypowiedź akademicka	486
5.1. Wyłączenia stosowania przepisów RODO dla wypowiedzi akademickiej	487
5.2. Ograniczenia w zakresie realizacji praw jednostki ...	487
5.3. Powierzenie przetwarzania danych	488

- 5.4. Wyłączenie w zakresie obowiązku prowadzenia rejestru czynności przetwarzania danych 488
- 5.5. Zakres stosowania RODO w przypadku wypowiedzi akademickich 488

Rozdział XII

Prezes Urzędu Ochrony Danych – polski organ nadzorczy

- *Maciej Gawroński, Patrycja Naklicka* 490
 - 1. Prezes Urzędu 490
 - 2. GIODO a Prezes Urzędu 491
 - 2.1. Zmiana nazwy organu nadzorczego 491
 - 2.2. Kontynuacja kierownictwa 492
 - 3. Zadania oraz uprawnienia Prezesa Urzędu 493
 - 3.1. Zadania i uprawnienia Prezesa Urzędu określone w RODO 493
 - 3.2. Zadania i uprawnienia Prezesa Urzędu określone w ustawie o ochronie danych osobowych 497
 - 4. Podmioty uprawnione do wystąpienia o uprzednie konsultacje 504
 - 5. Dodatkowe uprawnienia Prezesa Urzędu i kwestia rozstrzygania sporów o właściwość 505
 - 6. Sposób powoływania, odwoływania oraz kadencja Prezesa Urzędu 506
 - 6.1. Powoływanie Prezesa Urzędu 506
 - 6.2. Wymogi względem Prezesa Urzędu 506
 - 6.3. Kadencja 506
 - 6.4. Sposób odwołania Prezesa Urzędu 507
 - 7. Niezależność Prezesa Urzędu 508
 - 8. Niezależność materialna. Zapewnienie zasobów i zaplecza administracyjnego dla Prezesa Urzędu 509
 - 8.1. Budżet 509
 - 8.2. Urząd 509
 - 8.3. Statut Urzędu 511
 - 8.4. Zachowanie poufności 511
 - 8.5. Zastępcy Prezesa Urzędu 512
 - 8.6. Zakaz zajmowania innych stanowisk 512
 - 8.7. Apolityczność 512
 - 9. Immunitet formalny Prezesa Urzędu 513

9.1. Wniosek o pociągnięcie do odpowiedzialności	513
9.2. Wymogi formalne wniosku o pociągnięcie do odpowiedzialności	514
9.3. Procedura rozpatrywania wniosku	514
9.4. Zgoda	515
9.5. Wniosek o wyrażenie zgody na zatrzymanie lub aresztowanie	515
9.6. Wymogi formalne wniosku o zatrzymanie lub aresztowanie	515
9.7. Powiadomienie i ogłoszenie uchwały	516
9.8. Odpowiedzialność karna a odpowiedzialność za wykroczenia	516
10. Rada do Spraw Ochrony Danych Osobowych	516
10.1. Kompetencje Rady	516
10.2. Skład Rady	517
10.3. Członkowie Rady	518
10.4. Zachowanie tajemnicy	518
10.5. Kadencja członka Rady	518
10.6. Funkcjonowanie Rady	519
10.7. Wynagrodzenie za udział w pracach	519

Rozdział XIII

Postępowanie przed Prezesem Urzędu Ochrony Danych – podstawowe informacje i rodzaje postępowań (akredytacja, certyfikacja, postępowania kontrolne i postępowania w sprawie naruszeń przepisów o ochronie danych)

– <i>Magdalena Wojtas</i>	520
1. Rodzaje postępowań przed Prezesem Urzędu Ochrony Danych Osobowych	520
2. Ogólny opis postępowań przed Prezesem Urzędu	521
2.1. Postępowanie certyfikacyjne	521
2.2. Postępowanie w sprawie zatwierdzenia kodeksu postępowania	522
2.3. Postępowanie w sprawie akredytacji podmiotu monitorującego	523
2.4. Postępowanie kontrolne	524
2.5. Postępowanie w sprawie naruszeń przepisów o ochronie danych	524

Rozdział XIV

Warunki i tryb certyfikacji – Maciej Gawroński, Paweł Punda	526
1. Mechanizmy certyfikacji	526
2. Podstawy certyfikacji	526
3. Cel certyfikacji	527
3.1. Certyfikacja przez Prezesa Urzędu	529
3.2. Certyfikacja przez podmiot certyfikujący	529
4. Postępowanie w sprawie certyfikacji	530
4.1. Cofnięcie certyfikacji	530
4.2. Okres certyfikacji	531
4.3. Zasięg terytorialny certyfikacji	531
5. Specyfika mikro-, małych i średnich przedsiębiorstw	531

Rozdział XV

Postępowanie w sprawach naruszenia przepisów o ochronie danych – Maciej Gawroński, Patrycja Naklicka	534
1. Prowadzenie postępowania przez Prezesa Urzędu Ochrony Danych Osobowych (art. 60 u.o.d.o.)	534
1.1. Właściwość Prezesa Urzędu	534
1.2. Naruszenie przepisów	534
1.3. Stosowanie Kodeksu postępowania administracyjnego	535
2. Jednoinstancyjność postępowania (art. 7 u.o.d.o.)	535
2.1. Zaskarżanie postanowień Prezesa Urzędu w postępowaniu w sprawie naruszenia	537
3. Kiedy Prezes Urzędu wszczyna postępowanie?	538
4. Przedstawiciel organizacji jako pełnomocnik strony (art. 61 u.o.d.o.)	539
5. Zawiadomienie strony o niezłażwieniu sprawy w terminie (art. 63 u.o.d.o.)	540
5.1. Termin na złażwienie sprawy	540
5.2. Obowiązki organu po upływie terminu	541
5.3. Dwa czy trzy miesiące na złażwienie sprawy przez Prezesa Urzędu?	541
5.4. Terminy instrukcyjne	542
5.5. Złażwienie sprawy w terminie a liczba skarg	542
6. Uprawnienia Prezesa Urzędu w zakresie prowadzenia postępowania o naruszeniu przepisów	543

6.1. Obowiązek żądania przedstawienia dokumentacji w języku polskim (art. 63 u.o.d.o.)	543
6.2. Prawo dostępu do informacji objętych tajemnicą prawnie chronioną	543
6.2.1. Tajemnica prawnie chroniona	544
6.2.2. Przepisy ustawy sektorowej	545
6.2.3. Tajemnice zawodowe określone w projekcie ustawy sektorowej	545
6.3. Honorowanie tajemnicy przedsiębiorstwa (art. 65 u.o.d.o.)	546
6.4. Uprawnienie do uchylenia tajemnicy przedsiębiorstwa (art. 65 ust. 3 u.o.d.o.)	546
6.5. Ograniczenie dostępu do akt sprawy (art. 66 u.o.d.o.)	547
6.6. Zawiadomienie poprzez publiczne obwieszczenie (art. 67 u.o.d.o.)	547
6.7. Przeprowadzenie postępowania kontrolnego (art. 68 u.o.d.o.)	548
6.8. Grzywna za naruszenie obowiązku osobistego stawiennictwa (art. 69 u.o.d.o.)	548
6.9. Ograniczenie przetwarzania danych (art. 70 u.o.d.o.)	550
6.10. Wniosek o wystąpienie z pytaniem prawnym w sprawie ważności decyzji Komisji Europejskiej (art. 71 u.o.d.o.)	552
6.10.1. Wymogi formalne wniosku	553
6.10.2. Postanowienie sądu	554
7. Zakończenie postępowania	554
8. Uzasadnienie decyzji kończącej postępowanie w sprawie (art. 72 u.o.d.o.)	555
8.1. Matryca karania z art. 83 ust. 2 RODO	556
8.2. Matryca karania	557
9. Publikacja decyzji wydanej przez Prezesa Urzędu (art. 73 u.o.d.o.)	557
9.1. Publikacja decyzji wobec podmiotów prywatnych	557
9.2. Publikacja decyzji wobec podmiotów publicznych	557
9.3. Publikacja działań w celu wykonania decyzji	558
10. Wstrzymanie wykonalności decyzji w zakresie kary pieniężnej (art. 74 u.o.d.o.)	558

Rozdział XVI

Kontrola organu nadzorczego – Magdalena Wojtas	559
1. Zakres kontroli	559
2. Podmioty kontrolujące	561
2.1. Kontrolujący	561
2.2. Wyłączenie kontrolującego	561
2.3. Specjalista	562
3. Termin przeprowadzenia kontroli	563
3.1. Podstawa wszczęcia kontroli	563
3.2. Brak obowiązku wcześniejszego zawiadomienia	563
4. Cel kontroli	564
5. Sposób przeprowadzania kontroli	565
5.1. Upoważnienie	565
5.2. Rodzaje kontroli	567
5.3. Zasady kontroli	567
5.4. Udział Policji w kontroli	568
5.5. Protokół	570
5.6. Czas trwania kontroli	571
6. Podejście do kontroli	572

Rozdział XVII**Wyznaczanie IOD, cz. 1 – Maciej Gawroński,**

<i>Adrianna Gnatowska</i>	573
1. Wstęp	573
2. Obowiązek powołania IOD	574
2.1. Uwagi ogólne	574
2.2. Powołanie fakultatywnego IOD	575
2.3. Organy i podmioty publiczne	575
2.4. Główna działalność	576
2.5. Przetwarzanie danych na dużą skalę	576
2.6. Duża skala według estońskiego DPA	576
2.7. Monitoring wizyjny	578
3. Procedura zawiadomienia o wyznaczeniu IOD według ustawy o ochronie danych osobowych	578
3.1. Uwagi ogólne	578
3.2. Zawiadomienie o wyznaczeniu IOD	580
3.3. Zastępca IOD	581
3.4. Zawiadomienie o zmianach	581
3.5. Forma zawiadomienia	582

3.6. Zawiadomienie przez pełnomocnika	582
3.7. IOD dla grupy przedsiębiorstw	583
3.8. Udostępnienie danych IOD	583
4. Charakter przepisów przejściowych	584
4.1. Przepisy przejściowe	584
4.2. ABI jako „prowizoryczny” IOD	585
4.3. Termin wyznaczenia IOD w sytuacji niepowołania ABI przed 24.05.2018 r.	586
4.4. Wyznaczenie IOD przez podmiot przetwarzający ...	586

Rozdział XVIII

Wyznaczanie IOD, cz. 2 – Maciej Gawroński,

<i>Adrianna Gnatowska</i>	587
1. Praktyczne aspekty wyznaczania inspektora ochrony danych	587
1.1. Zawiadomienie w formie elektronicznej	587
1.1.1. Kwalifikowany podpis elektroniczny	587
1.1.2. Profil zaufany ePUAP	588
1.1.3. Profil zaufany ePUAP dla organizacji	588
1.1.4. Zawiadomienie przez pełnomocnika	589
1.2. Wyznaczenie IOD dla oddziału	589
1.3. Konflikt interesów	592
1.3.1. Funkcja <i>compliance</i> a stanowisko IOD	592
1.3.2. Prawnik jako IOD	593
1.3.3. Osoba reprezentująca związek zawodowy („ZZ”) a IOD	595

Rozdział XIX

Postępowania przed sądem w przypadku naruszenia przepisów o ochronie danych – Maciej Gawroński,

<i>Patrycja Naklicka</i>	598
1. Właściwość sądu okręgowego	598
2. Synchronizacja między Urzędem a sądami	598
3. Wzajemne informowanie	600
4. Sprzeczne z RODO zamrożenie prawa do sądu	600
5. Gravamen	601
6. Związanie sądu decyzją Prezesa	601
7. Udział Prezesa w postępowaniu sądowym	601
8. Rozkład ciężaru dowodu	602

9. Ogólny ciężar udowodnienia okoliczności	602
10. Ciężar udowodnienia zgodności zdarzenia z prawem	603
11. Pojęcie szkody	603
12. Odpowiedzialność solidarna	604
13. Odpowiedzialność podmiotu przetwarzającego	605
14. Odesłanie do przepisów Kodeksu postępowania cywilnego	606

Rozdział XX

Kary pieniężne za naruszenie przepisów o ochronie danych

– Paweł Dmowski, Maciej Gawroński	607
1. Wstęp	607
2. Kto?	607
3. Komu i ile?	608
4. Za co?	609
4.1. Kara mniejsza	609
4.2. Kara większa	610
5. Ustalenie wysokości kary	612
6. Różnica w odpowiedzialności podmiotu przetwarzającego ..	615
7. Odwołanie od decyzji wymierzającej karę	616
8. Wykonanie kary (egzekucja)	616
9. Odroczenie płatności	617
10. Pozostałe ulgi w przedmiocie wykonania kary	618
11. Podsumowanie	619

Rozdział XXI

Europejska współpraca – Maciej Gawroński, Patrycja Naklicka ...

1. Wstęp	620
2. Przepisy o wzajemnej współpracy europejskiej	621
3. Cel mechanizmu wzajemnej współpracy	621
3.1. Swoboda przetwarzania danych w całej Unii	621
3.2. Regulacje wzajemnej współpracy	622
4. Wyjątek od stosowania mechanizmu wzajemnej współpracy	622
5. Co to jest wzajemna współpraca?	623
5.1. Zakres wzajemnej współpracy	623
5.2. Formy wzajemnej współpracy	623
6. Przepisy proceduralne w ustawie o ochronie danych osobowych	624

Rozdział XXII

Kodeksy postępowañ – Aleksander P. Czarnowski	626
1. Wprowadzenie	626
2. ISO 9001 a RODO	628
3. Inne ważne normy ISO z perspektywy RODO	629
4. ISO a kodeksy postępowañ	629
5. Kodeksy postępowañ	630
6. Rola kodeksów w praktyce	631
7. Zakres kodeksu	632

Rozdział XXIII**Odpowiedzialność cywilna za naruszenie przepisów**

– <i>Maciej Gawroński, Patrycja Naklicka</i>	633
1. Wstęp	633
2. Tryb dochodzenia roszczeń na gruncie poprzedniej ustawy o ochronie danych osobowych a RODO	634
3. Odesłanie do przepisów Kodeksu cywilnego	635
4. Roszczenia z art. 79 RODO – żądanie wykonania uprawnień lub zaprzestania naruszeń	635
5. Brak przedawnienia i zakaz zbywania	636
6. Roszczenie o odszkodowanie z art. 82 RODO	637

Rozdział XXIV**Akredytacja podmiotów monitorujących przestrzeganie zatwierdzonych kodeksów postępowañ**

– <i>Aleksander P. Czarnowski</i>	639
1. Wstęp	639
2. Przebieg procesu akredytacyjnego	640

Rozdział XXV**Monitoring jako jedna z kluczowych zmian wprowadzonych przez ustawę o ochronie danych osobowych.****Część I – monitoring pracowniczy – *Maciej Gawroński,***

<i>Katarzyna Kloc</i>	643
1. Wstęp	643
2. Monitoring pracowników	644
3. Monitoring wizyjny	646
4. Cele	646

5. Przykład naruszenia zasad korzystania z monitoringu wizyjnego	647
6. Rejestracja obrazu	647
7. Monitorowany obszar	648
8. Monitoring wizyjny a RODO	648
9. Podstawa przetwarzania danych z monitoringu	649
10. Prawnie uzasadniony interes jako podstawa stosowania monitoringu wizyjnego przez podmioty publiczne	649
11. Obowiązki pracodawcy związane z monitoringiem	651
12. Monitoring wizyjny a dane szczególnych kategorii	653
13. Monitoring poczty elektronicznej i inne formy monitoringu	654

Rozdział XXVI

Monitoring jako jedna z kluczowych zmian wprowadzonych przez ustawę o ochronie danych osobowych.

Część 2 – monitoring w przypadku jednostek samorządu terytorialnego oraz monitoring w szkołach

– <i>Maciej Gawroński, Katarzyna Kloc</i>	657
1. Monitoring w przypadku jednostek samorządu terytorialnego	657
2. Cele monitoringu	660
3. Monitorowany obszar	661
4. Okres przechowywania danych z nagrań	661
5. Informowanie o monitoringu	662
6. Bezpieczeństwo	662
7. Monitoring w szkołach	662
8. Bezpieczeństwo lub ochrona mienia – cele monitoringu w oświacie	664
9. Wprowadzenie monitoringu – konsultacje	665
10. Podstawa prawna przetwarzania danych z monitoringu ..	666
11. Obszar monitorowany	667
12. Warunki stosowania monitoringu	668
13. Okres przechowania danych z nagrań	669

Rozdział XXVII

Odpowiedzialność karna – *Maciej Gawroński, Katarzyna Kloc* ...

1. Przepisy karne w ustawie o ochronie danych osobowych	670
---	-----

2. Przepisy karne a RODO	671
3. Nowe przepisy karne a ustawa z 1997 r.	672
4. Niedopuszczalne i nieuprawnione przetwarzanie danych	673
5. Przepięstwo niedopuszczalnego przetwarzania danych	674
6. Przepięstwo nieuprawnionego przetwarzania danych ...	676
7. Udaremnianie lub utrudnianie kontroli	677
8. Odpowiedzialnoř karna wedłóg ustawy o ochronie danych osobowych a inne przepięstwa z Kodeksu karnego	678
9. Odpowiedzialnoř karna a zasada rozliczalnořci i rozkład ciężaru dowodu	679
10. Nie ma osób niewinnych, sę tylko źle przesłuchane? RODO – absurd	681

Rozdział XXVIII

Ograniczenie obowiązków RODO dla podmiotów

wykonywujących zadania publiczne – Maciej Gawroński	684
1. Wstępiep	684
1.1. Zakres ułatwień	684
1.2. Wyłączenia informowania	685
1.3. Wyłączenie wyszukiwania	686
2. Uzasadnienie ułatwień dla administracji	686
3. Analiza przesłanek wyłączenia obowiązku informacyjnego	688
4. Informacja niejawna i bezpieczeñstwo narodowe	690

Rozdział XXIX

Akredytacja podmiotu uprawnionego do certyfikacji

w zakresie ochrony danych osobowych – Paweł Punda	691
1. Podstawy akredytacji	691
2. Pojęcie akredytacji	692
3. Podmiot akredytujący	693
4. Kryteria akredytacji	693
4.1. Niezależnoř i brak konfliktu interesów	694
4.2. Wiedza fachowa	696
4.3. Przestrzeganie kryteriów, procedury, obsługa procesu skarg	697

5. Postępowanie w sprawie akredytacji	697
6. Cofnięcie akredytacji	699

Część B

Wzory dokumentów

Wzór nr 1a.	Klauzula zgody na przetwarzanie danych osobowych zwykłych – <i>Michał Sztąberek</i>	703
Wzór nr 1b.	Klauzula zgody na przetwarzanie danych osobowych „szczególnych kategorii” – <i>Michał Sztąberek</i>	704
Wzór nr 2.	Klauzula informacyjna o prawie do cofnięcia zgody – <i>Paweł Punda</i>	706
Wzór nr 3.	Klauzula informacyjna o przetwarzaniu danych – <i>Michał Sztąberek</i>	707
Wzór nr 4.	Klauzula informacyjna w przypadku współadministrowania danymi – <i>Michał Kibil</i>	715
Wzór nr 5.	Klauzula o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu – element klauzuli informacyjnej – <i>Paweł Punda</i>	717
Wzór nr 6.	Umowa powierzenia przetwarzania danych osobowych – <i>Paweł Punda</i>	719
Wzór nr 7.	Szczegółowa klauzula zgody na podpowierzenie – <i>Paweł Punda</i>	730
Wzór nr 8.	Sprzeciw administratora danych osobowych wobec podpowierzenia – <i>Patrycja Naklicka</i>	731
Wzór nr 9.	Upoważnienie do przetwarzania danych osobowych – <i>Katarzyna Kloc</i>	732
Wzór nr 10.	Klauzula informacyjna dla osoby, której dane dotyczą, o przekazaniu jej danych do państwa trzeciego – <i>Maciej Gawroński</i>	734
Wzór nr 11.	Polityka ochrony danych osobowych – <i>Maciej Gawroński</i>	737
Wzór nr 12a.	Wytyczne dotyczące klasyfikacji naruszeń i procedura zgłaszania naruszenia ochrony danych do organu nadzorczego (UODO) (art. 33 ust. 3 RODO) – <i>Tomasz Soczyński</i>	756

Wzór nr 12b.	Analiza wystąpienia ryzyka naruszenia praw lub wolności w związku z incydem ochrony danych osobowych – <i>Patrycja Naklicka</i>	768
Wzór nr 13.	Wytyczne na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób w zakresie ich informowania o działaniach, jakie powinni wykonać w celu ograniczenia ryzyka – <i>Tomasz Soczyński</i>	769
Wzór nr 14.	Raport z przeprowadzonej ogólnej analizy ryzyka – <i>Tomasz Soczyński</i>	773
Wzór nr 15a.	Formularz z ogólnej analizy ryzyka – <i>Patrycja Naklicka</i>	777
Wzór nr 15b.	Instrukcja przeprowadzania ogólnej analizy ryzyka dla danych osobowych – <i>Patrycja Naklicka</i>	778
Wzór nr 15c.	Uproszczona metodyka analizy ryzyka – <i>Maciej Gawroński</i>	801
Wzór nr 16.	Proces oceny DPIA – <i>Patrycja Naklicka</i>	811
Wzór nr 17a.	Plan Ciągłości Działania (art. 32 ust. 1 lit. b RODO) – <i>Tomasz Soczyński</i>	812
Wzór nr 17b.	Plan Ciągłości Działania – <i>Aleksander P. Czarnowski</i>	814
Wzór nr 18a.	Procedura odtwarzania systemu po awarii oraz testowania (art. 32 ust. 1 lit. c RODO) – <i>Tomasz Soczyński</i>	824
Wzór nr 18b.	Procedura odtwarzania systemu po awarii oraz testowania – <i>Aleksander P. Czarnowski</i>	828
Wzór nr 19.	Umowa o współadministrowanie – <i>Maciej Gawroński, Adrianna Gnatowska</i>	831

Wzory rejestrów

Wzór Rejestru Czynności Przetwarzania Danych – <i>Katarzyna Kloc</i>	851
Wzór Rejestru Naruszeń Ochrony Danych Osobowych – <i>Paweł Punda</i>	854

WYKAZ SKRÓTÓW

- 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.) – uchylona
- 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, ze sprost.)
- EKPC** – Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie 4.11.1950 r. (Dz.U. z 1993 r. poz. 284 ze zm.)
- GDPR** – EU General Data Protection Regulation
- k.c.** – ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2018 r. poz. 1025 ze zm.)
- k.k.** – ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2018 r. poz. 1600)
- Konstytucja RP** – ustawa z 2.04.1997 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. poz. 483 ze zm.)
- k.p.** – ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2018 r. poz. 917 ze zm.)
- k.p.a.** – ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2017 r. poz. 1257 ze zm.)
- k.p.c.** – ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2018 r. poz. 1360 ze zm.) – dalej k.p.c.

- KPP** – Karta praw podstawowych UE (Dz.Urz. UE C 202 z 2016 r., s. 389)
- pr. bank.** – ustawa z 29.09.1997 r. – Prawo bankowe (Dz.U. z 2017 r. poz. 1876 ze zm.)
- pr. pras.** – ustawa z 26.01.1984 r. – Prawo prasowe (Dz.U. poz. 24 ze zm.)
- p.p.s.a.** – ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2018 r. poz. 1302 ze zm.)
- pr. przed.** – ustawa z 6.03.2018 r. – Prawo przedsiębiorców (Dz.U. z 2018 r. poz. 646 ze zm.)
- PUODO** – Prezes Urzędu Ochrony Danych Osobowych
- 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)
- 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)
- u.o.d.o.** – ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. poz. 1000 ze zm.)
- u.r.** – ustawa z 29.09.1994 r. o rachunkowości (Dz.U. z 2018 r. poz. 395 ze zm.)
- u.p.o.** – u.p.o. – ustawa z 14.12.2016 r. – Prawo oświatowe (Dz.U. z 2018 r. poz. 996 ze zm.)
- u.s.g.** – ustawa z 8.03.1990 r. o samorządzie gminnym (Dz.U. z 2018 r. poz. 994 ze zm.)
- u.s.i.o.z.** – ustawa z 28.04.2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2017 r. poz. 1845 ze zm.)
- u.z.z.** – ustawa z 23.05.1991 r. o związkach zawodowych (Dz.U. z 2015 r. poz. 1881 ze zm.)
- wyrok C-131/12 Google Spain** – wyrok z 13.05.2014 r., C-131/12, Google Spain SL i Google Inc. v. Agencia Española de Protección de Datos (AEPD) i Mario Costeja González, EU:C:2014:317

WSTĘP

Oddajemy czytelnikom zaktualizowany przewodnik po RODO wraz z przewodnikiem po nowej polskiej ustawie o ochronie danych osobowych. Całość pisaliśmy z punktu widzenia administratorów danych, koncentrując się, z racji doświadczenia, na rynku prywatnym.

Ochroną danych osobowych zajmuję się od stycznia 1999 r., gdy na stażu we Francji w paryskim oddziale pewnej kancelarii zlecono mi rozpoznanie tego zagadnienia. Następnie we wczesnych latach dwutyśniętnych doradzałem bankom w grupowych transferach danych i klauzulach informacyjnych, i zgodach, od 2007 r. zaś doradzałem w międzynarodowych przepływach danych osobowych, ustalając i wybierając role administratorów i podmiotów przetwarzających, określając zasady przekazywania danych osobowych poza teren Unii Europejskiej (na podstawie tzw. standardowych klauzul umownych), określając dopuszczalność przekazania danych osobowych do USA w ramach amerykańskiej sądowej procedury, tzw. *disclosure*, wdrażając i wyjaśniając w Polsce wiążące reguły korporacyjne (instrument o dość dziwnej naturze), określając możliwości współwłasności danych (zwanej współadministrowaniem lub równoległym administrowaniem) pomiędzy różnymi podmiotami, dyskutując w UE o zasadach podpowierzenia danych osobowych przy przekazaniu ich poza UE, o zasadach kontroli nad danymi i przenoszenia danych w modelu cloud computingu, wreszcie omawiając nowe zasady ochrony danych osobowych wynikające z RODO.

Równolegle zajmowałem się kwestiami wdrożeń informatycznych (odpowiadałem za prawne aspekty kilkuset z nich, w tym za największe, najbardziej referencyjne wdrożenie IT w Polsce), bezpieczeństwa informacji, ciągłości działania, cyberbezpieczeństwa, gdzie kwestie

prawne miały onegdaj mniejsze znaczenie. Zajmowałem się też prawem konsumenckim (jak też wieloma innymi kwestiami, takimi jak reprezentowanie Polski w sporach o wartości powyżej 10 mld zł, do szczegółów których nie ma potrzeby tu nawiązywać).

W konsekwencji wydaje się, że dysponuję rozległym układem odniesienia pozwalającym na praktyczne ukazanie nowych przepisów, ich konsekwencji praktycznych, jak i ich oceny. Zrobiłem też co w mojej mocy, biorąc pod uwagę ten krótki czas, który mieliśmy na opracowanie niniejszego materiału, aby był on dla Państwa maksymalnie użyteczny. Zdaję sobie sprawę, że niekiedy poszliśmy na skróty i uniknęliśmy zmierzenia się z konkretnymi problemami. Jednak ilość wyzwań i niewiadomych związanych z RODO jest tak duża, że nigdy nie wyszlibyśmy z fazy pisania, gdyby nie te kompromisy.

W ciągu ostatnich 10 miesięcy poświęciłem tej książce tak dużo czasu, jak nigdy jeszcze niczemu czasu nie poświęciłem. Wytrzymała to moja Rodzina (moja żona i moja dwuletnia córka). Książce tej mnóstwo czasu, serca i zaangażowania poświęciło też kilkunastu autorów, którzy włożyli w nią „krew, pot i łzy”. Za to wszystkim serdecznie dziękuję.

Szanowni Państwo, jeżeli czują się Państwo zagubieni, wydaje się Państwu, że nic z tego nie rozumieją, a cała ochrona danych to jakieś tortury, to mają Państwo rację. Rzeczywiście jest to trudny system prawny, wymagający skupienia, żeby go jakoś zrozumieć. Ale czy to oznacza, że jest on bez sensu? Niekoniecznie. Po pierwsze, wymaga on od nas zabezpieczenia swoich danych. I to jest bardzo ważne. Po drugie, zwraca uwagę na ryzyko kontroli nad ludźmi przez wiedzę o ich zachowaniach. I to też może być bardzo ważne, choć kto z nas pojedynczo będzie się tym przejmował. Po trzecie, kompasem w ochronie danych osobowych powinien być ZDROWY ROZSĄDEK. Jeśli coś jest rozsądne, to zapewne jest zgodne z prawem. A po czwarte wreszcie, jeżeli mają Państwo pytania, proszę pisać do nas na Facebooku, Linked In, Twitterze, e-mailem, na Instagramie (nie, na Instagramie lepiej nie), na Quora, gdziekolwiek. Zawsze staramy się odpowiadać.

Część A

**KOMPENDIUM
OCHRONY DANYCH OSOBOWYCH**

Rozdział I

ZGODNOŚĆ PODSTAWOWA

1. RODO – unijna „ustawa” o ochronie danych osobowych

1.1. RODO – nowa „ustawa” o ochronie danych osobowych

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) – RODO – to w dużym skrócie **nowa „ustawa” o ochronie danych osobowych**.

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych w Unii Europejskiej (motyw 1 RODO). Stanowią o tym: art. 8 ust. 1 Karty praw podstawowych UE (Dz.Urz. UE C 202 z 2016 r., s. 389) oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47), zgodnie z którymi każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

Unia Europejska uznała, że w celu realizacji i gwarancji prawa do prywatności i ochrony danych na terenie Unii konieczne jest określenie stabilnych, spójnych ram ochrony danych osobowych oraz zdecydowanego ich **egzekwowania**. Dotychczas problemem było właśnie egzekwowanie (wymuszanie) stosowania przepisów o ochronie danych osobowych.

1.2. Przedmiot i cel RODO

1.2.1. Uwagi wstępne

Formalnie RODO utrzymuje dotychczasowe zasady ochrony danych osobowych obowiązujące na terenie Unii Europejskiej (w tym w Polsce na podstawie „starej” ustawy z 29.08.1997 r. o ochronie danych osobowych, Dz.U. z 2016 r. poz. 922 ze zm.), natomiast nieco je uszczegóławia, dodaje uprawnienia osobom fizycznym i wprowadza surowe kary.

Mimo uspokajających wypowiedzi organów nadzorczych, w praktyce RODO stanowi rewolucję w ochronie danych właśnie ze względu na kary, nowe obowiązki firm i innych podmiotów przetwarzających dane osobowe ze względu na tzw. podejście oparte na ryzyku, czyli spoczywający na wszystkich obowiązek oceny ryzyka związane go z przetwarzaniem danych osobowych i dostosowania sposobów ochrony danych do tego ryzyka, ze względu na wprowadzenie zasady rozliczalności – obowiązku wykazania zgodności przez obowiązane go, a także wobec wprowadzenia bezpośrednich podstaw odpowiedzialności cywilnej za naruszenie RODO, umożliwiającej w niektórych krajach (np. we Francji) nawet pozwy zbiorowe. Co więcej, bezpośrednią odpowiedzialność administracyjną i cywilną w myśl RODO ponoszą wszystkie podmioty, które uczestniczą w przetwarzaniu danych, a więc i podmioty przetwarzające (podwykonawcy).

§ Zgodnie z art. 1 RODO:

1. W niniejszym rozporządzeniu ustanowione zostają **przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych**.
2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich **prawo do ochrony danych osobowych**.
3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

1.2.2. Ochrona osób fizycznych

RODO jest aktem kompleksowym, który szeroko reguluje kwestię ochrony prywatności i danych osobowych (osób fizycznych), a także dotyka materii swobodnego przepływu danych osobowych w Unii Europejskiej. RODO nie dotyczy przetwarzania danych dotyczących osób prawnych, w szczególności przedsiębiorstw, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej (motyw 14). Tym zajmie się jednak 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), zwane „Rozporządzeniem ePrivacy”. Rozporządzenie ePrivacy miało wejść w życie wraz z RODO, jednak prace legislacyjne nad nim jeszcze trwają w dacie aktualizacji naszego tekstu (sierpień 2018).

RODO nie stosuje się też do danych osobowych osób zmarłych.

1.2.3. Bezpośredniość

RODO jest aktem prawnym przyjętym na poziomie unijnym, ma jednak bezpośrednio zastosowanie do każdej organizacji przetwarzającej dane osobowe jako administrator danych lub podmiot przetwarzający cy państwie członkowskim Unii Europejskiej.

Bezpośredniość stosowania i w konsekwencji rola „ustawy” o ochronie danych osobowych to cechy odróżniające RODO od dyrektywy 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.), która utraciła moc wraz z wejściem w życie RODO i w założeniu miała harmonizować przepisy o ochronie danych osobowych w Unii Europejskiej, ale ze względu na spore różnice w implementujących ją przepisach krajowych w praktyce poziom ochrony danych osobowych i podejście do tego obszaru były dość mocno zróżnicowane.

Maciej Gawroński – radca prawny od dwudziestu lat zajmujący się prawnymi aspektami technologii; konsultant Grupy Roboczej Art. 29 (obecnie Europejska Rada Ochrony Danych) ds. przekazywania danych przez przetwarzającego w UE do podprzetwarzającego spoza UE; ekspert Komisji Europejskiej ds. kontraktów cloud computingowych, ostatnio członek Grupy Roboczej ds. Ochrony Danych Osobowych przy Ministerstwie Cyfryzacji. Zaproponował zasadę odpowiedzialności pozaunijnych podprocesorów, która stała się ogólną zasadą odpowiedzialności podmiotów przetwarzających, zasadę przenoszalności danych osobowych, konsultował zasady powierzenia; ekspert prawa technologii mediów i telekomunikacji rekomendowany przez Ranking Kancelarii Prawnych dziennika „Rzeczpospolita” i rankingi międzynarodowe. Jest też jednym z twórców treści serwisu prawnego LEX Ochrona Danych Osobowych.

Publikacja to przewodnik po nowej polskiej ustawie o ochronie danych osobowych oraz unijnym ogólnym rozporządzeniu o ochronie danych osobowych.

Autorzy szczegółowo omawiają m.in.:

- zakres kontroli organu nadzorczego,
- postępowanie przed Prezesem Urzędu Ochrony Danych,
- dopuszczalność monitoringu zgodnie z nową ustawą o ochronie danych osobowych,
- kary pieniężne grożące za naruszenie przepisów o ochronie danych.

Publikacja zawiera również praktyczne wzory dokumentów, w tym:

- umowę o współadministrowanie,
- zgłoszenie naruszenia ochrony danych osobowych,
- procedurę odtwarzania systemu po awarii.

Opracowanie jest przeznaczone dla prawników, a także administratorów, podmiotów przetwarzających i inspektorów ochrony danych. Będzie przydatne pracownikom administracji oraz przedsiębiorcom przetwarzającym dane osobowe.



ZAMÓWIENIA:

INFOLINIA 801 04 45 45, FAX 22 535 80 01

ZAMOWIENIA@WOLTERSKLUPER.PL

WWW.PROFINFO.PL

ISBN 978-83-8160-187-0

