

RODO

PRZEWODNIK

ZE WZORAMI

redakcja Maciej Gawroński

Aleksander P. Czarnowski, Marcin Dominiak

Aleksandra Gawron, Maciej Gawroński

Michał Kibil, Katarzyna Kloc, Katarzyna Kunda

Patrycja Naklicka, Zuzanna Piotrowska, Paweł Punda

Michał Sztąberek, Magdalena Wojtas

RODO 2018



Wolters Kluwer

PIKTOGRAMY

wskazują ważne elementy
książki i ułatwiają
ich odnalezienie nie tylko
tuż przed egzaminem



Ważne



Przykłady



Podstawa prawna
Kontekst prawny



Pytania
Zadania



Rozwiązania
Odpowiedzi



Stanowisko stron
Pogląd



Orzecznictwo



Literatura



Historia



Nowe przepisy

RODO PRZEWODNIK ZE WZORAMI

redakcja Maciej Gawroński

Aleksander P. Czarnowski, Marcin Dominiak

Aleksandra Gawron, Maciej Gawroński

Michał Kibil, Katarzyna Kloc, Katarzyna Kunda

Patrycja Naklicka, Zuzanna Piotrowska, Paweł Punda

Michał Sztąberek, Magdalena Wojtas



Stan prawny na 10.03.2018 r. z uwzględnieniem zmian wprowadzonych rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. (ogólne rozporządzenie o ochronie danych, Dz.Urz. UE L 119, s. 1) wchodzącym w życie z dniem 25.05.2018 r.

Wydawca
Monika Pawłowska

Redaktor prowadzący
Joanna Tchorek

Opracowanie redakcyjne
Grażyna Polkowska-Nowak

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.

The logo for 'prawolubni' features the word in a stylized, lowercase font. Above the 'i' in 'lubni' is a small heart symbol. Below the text are three horizontal wavy lines.

SZANUJMY PRAWO I WŁASNOŚĆ
Więcej na www.legalnakultura.pl
POLSKA IZBA KSIĄŻKI

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

ISBN 978-83-8124-637-8

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	25
---------------------	----

Część A Kompendium RODO

Rozdział I

Zgodność podstawowa	29
1. RODO – unijna „ustawa” o ochronie danych osobowych – <i>Katarzyna Kloc, Maciej Gawroński</i>	29
1.1. RODO – nowa „ustawa” o ochronie danych osobowych	29
1.2. Przedmiot i cel RODO	30
1.2.1. Uwagi wstępne	30
1.2.2. Ochrona osób fizycznych	31
1.2.3. Bezpośredniość	31
1.2.4. Konsekwencje dla polskich przedsiębiorców ...	32
1.3. Prywatność, prawa, bezpieczeństwo – filary RODO ...	32
1.4. Wymagania RODO	34
1.4.1. Ogólnikowość	34
1.4.2. Mierzalność	35
1.4.3. Bezpośredniość	36
1.4.4. Surowość	36
1.4.5. Domniemanie winy	37
1.5. Podział funkcjonalny RODO	38
2. Przedmiotowy i terytorialny zakres stosowania RODO – <i>Katarzyna Kloc, Maciej Gawroński</i>	42
2.1. Zakres stosowania RODO	42

2.1.1. Zakres przedmiotowy	42
2.1.2. Wyłączenia stosowania RODO	43
2.1.3. Zakres terytorialny	44
3. Rodosłowniczek, czyli omówienie podstawowych pojęć RODO wraz z przykładami – <i>Patrycja Naklicka,</i> <i>Aleksandra Gawron</i>	47
3.1. Uwagi wstępne	47
3.2. Administrator	47
3.3. Analiza ryzyka	48
3.4. Anonimizacja	49
3.5. Czynności przetwarzania danych	49
3.6. Dane osobowe	50
3.7. Eksport danych	52
3.8. GIODO i PUODO	53
3.9. Grupa Robocza Art. 29 i Europejska Rada Ochrony Danych	53
3.10. Inspektor ochrony danych	54
3.11. Naruszenie ochrony danych osobowych	54
3.12. Ocena skutków dla ochrony danych	55
3.13. Odbiorca	55
3.14. Ograniczenie przetwarzania	56
3.15. Osoba, której dane dotyczą	57
3.16. Personel	57
3.17. Podmiot przetwarzający	57
3.18. Przetwarzanie	58
3.19. Pseudonimizacja	61
3.20. Rejestr czynności przetwarzania danych	61
3.21. Ryzyko	62
3.22. Ustawa o ochronie danych osobowych	63
4. Zasady przetwarzania danych osobowych – <i>Marcin Dominiak, Maciej Gawroński</i>	64
4.1. Wprowadzenie	64
4.1.1. Zasady materialne	65
4.1.2. Zasada formalna – rozliczalność	65
4.1.3. Bliżej o zasadach ochrony danych	66
4.2. Zasada legalności, rzetelności i przejrzystości przetwarzania (zgodności z prawem)	66

4.2.1. Legalność	66
4.2.2. Rzetelność	67
4.2.3. Przejrzystość	67
4.3. Zasada celowości	68
4.4. Zasada minimalizacji danych (adekwatności, proporcjonalności)	70
4.5. Zasada prawidłowości (poprawności)	72
4.6. Zasada ograniczenia czasowego (czasowości)	73
4.7. Zasada bezpieczeństwa (integralności i poufności danych)	76
4.7.1. Poufność	77
4.7.2. Integralność	77
4.7.3. Dostępność	77
4.7.4. Odpowiedniość	78
4.8. Zasada rozliczalności	80
5. Podstawy prawne przetwarzania danych osobowych – <i>Maciej Gawroński, Michał Sztąberek</i>	80
5.1. Wstęp	80
5.2. Dane osobowe „zwykłe” – art. 6–8 RODO	81
5.2.1. Zgoda na przetwarzanie danych osobowych ...	83
5.2.1.1. Dobrowolność zgody	83
5.2.1.2. Konkretność zgody	84
5.2.1.3. Świadomość zgody	85
5.2.1.4. Jednoznaczność zgody	85
5.2.1.5. Forma zgody	85
5.2.1.6. Zgoda dziecka na usługi społeczeństwa informacyjnego (np. media społecznościowe)	87
5.2.2. Zawarcie i wykonywanie umowy	89
5.2.2.1. Działania przed zawarciem umowy ...	90
5.2.2.2. Wykonywanie umowy	90
5.2.2.3. Przetwarzanie danych osoby trzeciej ...	90
5.2.3. Obowiązek prawny	91
5.2.4. Ochrona żywotnych interesów	93
5.2.5. Zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej	94

5.2.6. Uzasadniony interes administratora danych lub strony trzeciej	96
6. Artykuły 9 i 10 RODO – dane szczególnych kategorii i dane „karne” – <i>Maciej Gawroński, Michał Sztąberek</i>	99
6.1. Przesłanka zgody	101
6.2. Przetwarzanie wynikające ze stosunku pracy jest dozwolone prawem	102
6.3. Ochrona żywotnych interesów	102
6.4. Stowarzyszanie się	103
6.5. Dane upublicznione	103
6.6. Sprawy sądowe	103
6.7. Na podstawie prawa dla ważnego interesu publicznego	103
6.8. Dane „karne”	105
7. Zgoda jako podstawa przetwarzania danych – <i>Maciej Gawroński</i>	105
7.1. Wstęp	105
7.2. Podstawa prawna	106
7.3. Zgoda dziecka	106
7.4. Warunki wyrażenia zgody	107
7.5. Rozliczalność	112
7.6. Retencja (okres ważności zgody)	112
7.7. Równolaćwość cofnięcia zgody	113
7.8. Wybór podstawy przetwarzania	113
7.9. Ważność „starych” zgód	114
8. Administrator i podmiot przetwarzający – <i>Maciej Gawroński, Katarzyna Kloc, Magdalena Wojtas</i>	114
8.1. Wstęp	114
8.2. Administrator danych osobowych – definicja, cechy, obowiązki	116
8.2.1. Definicja	116
8.2.2. Każdy jest ADO	116
8.2.3. Co przesądza, że dany podmiot jest ADO? ...	117
8.2.4. Decydowanie o celach i środkach przetwarzania	117
8.2.5. Praktyczny test ADO	118

8.2.6. Rola ADO	118
8.2.7. Obowiązki ADO	119
8.3. Podmiot przetwarzający – definicja, cechy, rola i obowiązki	121
8.3.1. Definicja	121
8.3.2. Rola podmiotu przetwarzającego	121
8.3.3. Wiarygodność i wystarczające gwarancje	122
8.3.4. Umowa z ADO	122
8.3.5. Obowiązki wynikające z umowy z ADO	123
8.3.6. Obowiązki wynikające z RODO	125
8.4. Porównanie roli i obowiązków ADO i podmiotu przetwarzającego	126
9. Przetwarzanie danych niewymagające identyfikacji – <i>Maciej Gawroński</i>	127
9.1. Wprowadzenie	127
9.2. Brak obowiązku identyfikacji	129
9.3. Brak obowiązku monitorowania	130
9.4. Obowiązki informacyjne	131
9.4.1. Obowiązek poinformowania osób „niezidentyfikowanych” o niemożności zidentyfikowania – jeśli to możliwe	132
9.4.2. Umożliwienie wykonania praw jednostki	134
9.4.3. Bezpieczeństwo	134
9.4.4. Minimalizacja (dostępu i czasu)	135
10. Rejestrowanie czynności przetwarzania danych – <i>Katarzyna Kloc</i>	136
10.1. Własny rejestr zamiast zgłaszania do GIODO	136
10.2. RCPD – podstawa rozliczalności	137
10.3. Czynność przetwarzania danych	137
10.4. Czynności realizowane w tym samym celu	138
10.5. Czynności klasyfikowane w inny sposób	140
10.6. RCPD dla „małych” i „dużych” – różnice	141
10.6.1. Czy każdy musi prowadzić RCPD?	142
10.6.2. Zatrudnienie 250 osób	142
10.6.3. Przetwarzanie wysokiego ryzyka	143
10.7. Zakres informacji w RCPD – administratorzy danych	144

10.8. Zakres informacji w RCPD – podmioty przetwarzające dane	146
10.9. Forma RCPD	147
10.10. Osoba odpowiedzialna za prowadzenie RCPD ...	148
11. Przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej (eksport danych)	
– <i>Maciej Gawroński</i>	148
11.1. Reglamentacja eksportu danych	148
11.2. Praktyczne utrudnienie eksportu danych	149
11.3. Legalność eksportu danych	150
11.4. Podstawy eksportu danych	150
11.5. Dodatkowe podstawy przekazania	151
11.6. Przekazanie „naprawdę wyjątkowe”	152
11.7. Zarejestrowanie przekazania wyjątkowego	153
11.8. Zakaz sądowej samopomocy – ucinanie „długiej ręki”	153
11.9. Podsumowanie	153
12. Przetwarzanie transgraniczne, czyli właściwość wiodącego organu nadzorczego (art. 4 pkt 16 i 23, art. 56 RODO) – <i>Maciej Gawroński</i>	154
12.1. Wstęp	154
12.2. <i>One-stop-shop</i>	155
12.3. Przetwarzający	156
12.4. Administratorzy	156
12.4.1. Przetwarzanie lokalne	157
12.4.2. Zasięg lokalny	158
12.5. Prawo holdingowe	158
12.6. Wytyczne Grupy Roboczej Art. 29	158
12.7. Wnioski	159
13. Współadministrowanie danymi osobowymi	
– <i>Maciej Gawroński</i>	159
13.1. Wstęp	159
13.2. Przykłady współadministrowania danymi	160
13.3. Współadministrowania lepiej unikać	161
13.4. Obowiązki współadministratorów	162
13.5. Umowa o współadministrowanie	162
13.6. Treść umowy, analogia do powierzenia danych ...	162

13.7. Ujawnienie podmiotom danych	163
13.8. Transgraniczne współadministrowanie	163
13.9. Wnioski	164
14. Kodeksy postępowania i certyfikacja (art. 40 i n. RODO) – <i>Paweł Punda, Aleksander P. Czarnowski,</i> <i>Maciej Gawroński</i>	164
14.1. Wstęp	164
14.2. Kodeksy	165
14.2.1. Opracowanie	165
14.2.2. Zatwierdzanie	165
14.3. Certyfikacja	166
14.3.1. Schematy certyfikacyjne	166
14.3.2. Prace legislacyjne	166
14.4. Korzyści	167
14.5. Brak Urzędu	168
14.6. Projekty kodeksów	169
14.7. Certyfikacja prywatna	169

Rozdział II

Prawa jednostki	170
1. Obsługa praw jednostki (art. 12 RODO) – <i>Maciej Gawroński, Michał Kibil</i>	170
1.1. Wstęp	170
1.2. Czytelność komunikowania się	171
1.2.1. Czytelnie i zwięźle	171
1.2.2. Kompletność	171
1.2.3. Niecytowanie przepisów	172
1.2.4. Dzieci	172
1.2.5. Test Kowalskiego	172
1.3. Uwierzytelnienie	173
1.3.1. Potwierdzenie tożsamości	173
1.3.2. Pogłębione uwierzytelnienie	174
1.4. Forma komunikacji	174
1.5. Ułatwianie	175
1.6. Obsługa danych niezidentyfikowanych	175
1.7. Czas reakcji i czas obsługi	176
1.8. Nieuzasadnione lub nadmierne żądania	177

1.8.1. Nieuzasadnione żądanie	179
1.8.2. Nadmierne żądanie	179
1.9. Schemat działania administratora	180
2. Prawo do informacji i obowiązek informacyjny (art. 13 i 14 RODO)	
<i>Maciej Gawroński</i>	180
2.1. Uwagi wstępne	180
2.2. Zakres informacji	181
2.2.1. Pozyskiwanie od osoby	181
2.2.2. Pozyskiwanie nie od osoby	183
2.2.3. Zmiana celu	183
2.2.4. Prawo dostępu	183
2.3. Szczegóły informacji	183
2.3.1. Podstawa prawna	183
2.3.2. Kategorie odbiorców i odbiorcy	184
2.3.3. Eksport danych	185
2.3.4. Profilowanie	185
2.4. Kiedy i jak informować	185
2.4.1. Kiedy informować?	186
2.4.1.1. Podczas pozyskiwania od osoby	186
2.4.1.2. W ciągu miesiąca – z innych źródeł ...	186
2.4.1.3. Aktualizacja informacji	186
2.4.1.4. Informowanie osób niezidentyfikowanych (art. 11 ust. 2 RODO)	187
2.4.2. Jak informować?	187
2.4.2.1. Przejrzystość	187
2.4.2.2. Dostępność	188
2.4.2.3. Konkretność	189
2.5. Wyjątki od obowiązku informowania	189
3. Prawo dostępu do danych (art. 15 RODO)	
– <i>Maciej Gawroński, Michał Sztąberek</i>	190
3.1. Wstęp	190
3.2. Terminy	191
3.3. Informacje	191
3.4. Dostęp	192
3.5. Kopia danych	192

3.6.	Prośba o sprecyzowanie	193
3.7.	Odmowa	193
3.8.	Prawa innych	193
3.9.	Uwierzytelnienie i komunikacja	195
3.10.	Regulaminy i procedury	195
3.11.	Mapowanie danych, narzędzia eksploracji danych (data mining), narzędzia do tzw. ticketowania	196
3.12.	Podsumowanie	196
4.	Prawo do sprostowania danych (art. 16 RODO) – <i>Maciej Gawroński, Michał Sztąberek</i>	196
4.1.	Wstęp	196
4.2.	Zagadnienia ogólne – tryb uwierzytelnienia i komunikacji	197
4.2.1.	Element sporu	197
4.2.2.	Prawo do skargi	198
4.2.3.	Styl	198
4.2.4.	Wykazanie nieprawidłowości danych	198
4.2.5.	Dane nieaktualne czy nieprawidłowe	199
4.2.6.	Zakres korekty danych	199
4.3.	Uzupełnienie danych niekompletnych	200
4.3.1.	Adekwatność danych	200
4.3.2.	Podstawa aktualizacji	200
4.4.	Obowiązek powiadomienia	201
5.	Prawo do usunięcia danych, prawo do bycia zapomnianym (art. 17 RODO) – <i>Maciej Gawroński, Katarzyna Kunda</i>	202
5.1.	Historia prawa do bycia zapomnianym	202
5.2.	Składniki prawa do bycia zapomnianym	203
5.3.	Podstawy żądania usunięcia danych	204
5.3.1.	Zbędność do celów przetwarzania	204
5.3.2.	Cofnięcie zgody	205
5.3.3.	Wniesienie sprzeciwu	205
5.3.4.	Przetwarzanie niezgodne z prawem	206
5.3.5.	Prawny obowiązek usunięcia danych	207
5.3.6.	Oferowanie usług społeczeństwa informacyjnego dzieciom	207
5.4.	Wyjątki	207

5.4.1. Korzystanie z praw do wolności wypowiedzi i informacji	208
5.4.2. Wywiązywanie się z obowiązku prawnego lub zadania realizowanych w interesie publicznym albo w ramach wykonywania władzy publicznej	208
5.4.3. Interes publiczny w ochronie zdrowia publicznego	209
5.4.4. Cele archiwalne, badania naukowe, historyczne, cele statystyczne	210
5.4.5. Ustalenie, dochodzenie, obrona roszczeń	210
5.5. Zakres usunięcia danych	211
5.6. Przetwarzanie w celu realizacji prawa do usunięcia danych i prawa do bycia zapomnianym	212
5.7. Przetwarzanie w celu zapewnienia bezpieczeństwa – problem kopii zapasowych i archiwalnych	213
5.7.1. Jak wszyscy, to wszyscy	213
5.7.2. Problem bezpieczeństwa i ciągłości działania	214
5.7.3. Problem rozliczalności	214
5.7.4. Problem praktyczny – zasoby i proces	214
5.7.5. Rozwiązanie	215
5.8. Problem danych nieustrukturyzowanych	216
5.9. Poinformowanie innych administratorów	218
5.10. Ograniczenie obowiązku poinformowania	218
5.11. Listy kontrolne	219
5.11.1. Przygotowanie do RODO – wprowadzenie prawa do bycia zapomnianym do organizacji	219
5.11.2. Przetworzenie żądania usunięcia danych ...	219
6. Prawo do ograniczenia przetwarzania (art. 18 RODO) – <i>Michał Sztąberek, Maciej Gawroński</i>	220
6.1. Ograniczenie przetwarzania	220
6.2. Prawo do ograniczenia przetwarzania	221
6.2.1. Ograniczenie w razie sporu co do prawidłowości danych	222
6.2.2. Ograniczenie w razie niezgodności z prawem ...	222

6.2.3. Ograniczenie dla potrzeb roszczeń	223
6.2.4. Ograniczenie w razie sprzeciwu ze względu na szczególną sytuację	223
6.3. Sposób zastosowania się do żądania ograniczenia przetwarzania	223
6.4. Obowiązek powiadomienia	224
7. 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>	225
7.1. Wstęp	225
7.2. Na czym dokładnie polega prawo przenoszenia danych?	226
7.3. Kiedy można skorzystać z prawa do przenoszenia danych?	226
7.4. Jaki zakres danych należy przekazać?	227
7.5. W jaki sposób należy zrealizować prawo do przeniesienia danych?	229
7.5.1. Wyjątki	231
7.5.2. Prawa osób trzecich	231
7.5.3. Przenoszenie danych, które są równocześnie danymi wnioskodawcy i danymi innej osoby ...	232
7.6. Kogo przenoszenie danych dotyczy najbardziej? ...	234
7.6.1. Bezpieczeństwo	234
7.6.2. Kwestia techniczna	234
8. Prawo do sprzeciwu (art. 21 RODO) – <i>Maciej Gawroński, Michał Sztąberek</i>	235
8.1. Prawo do sprzeciwu	235
8.2. Sprzeciw ze względu na szczególną sytuację osoby ...	236
8.2.1. Prawnie uzasadnione interesy	238
8.2.2. Roszczenia i spory	239
8.2.3. Interes publiczny lub władza publiczna	239
8.3. Przetwarzanie danych na potrzeby marketingu bezpośredniego	241
8.3.1. Sprzeciw względem marketingu bezpośredniego a cofnięcie zgody na przetwarzanie	241

8.3.2. Sprzeciw względem marketingu bezpośredniego a zgoda na zdalną komunikację marketingową	242
8.4. Skuteczne wniesienie sprzeciwu na przetwarzanie danych	242
8.5. Jak powinien być składany sprzeciw	243
9. Profilowanie i automatyczne podejmowanie decyzji (art. 22 RODO) – <i>Michał Kibil</i>	244
9.1. Wstęp	244
9.2. Definicja profilowania z RODO	248
9.2.1. Automatyzacja	249
9.2.2. Dane osobowe	249
9.2.3. Efekt	250
9.2.4. Czynności traktowane jako profilowanie	250
9.3. Obowiązki administratora danych osobowych związane z profilowaniem lub automatycznym podejmowaniem decyzji, lub podejmowaniem decyzji w oparciu o profilowanie	251
9.3.1. Obowiązki ogólne administratora	252
9.3.1.1. Informowanie o decydowaniu automatycznym i w oparciu o profilowanie	252
9.3.1.2. Ile razy informować	253
9.3.1.3. Zmiana celu	253
9.3.1.4. Profilowanie danych ze „starej” ustawy o ochronie danych osobowych	253
9.3.2. Prawo sprzeciwu	254
9.4. Profilowanie a podejmowanie zautomatyzowanych decyzji	254
9.4.1. Środki bezpieczeństwa	256
9.4.2. Kiedy można stosować decyzje zautomatyzowane lub oparte wyłącznie na profilowaniu	257
9.4.2.1. Prawo do ludzkiej interwencji	260
9.4.2.2. Proces reklamacyjny	260
9.4.2.3. Automatyczne uwierzytelnienie	260
9.4.3. Profilowanie dzieci	261

9.4.4. Zautomatyzowane decyzje dotyczące danych wrażliwych	262
9.4.5. Wnioski	262

Rozdział III

Bezpieczeństwo	263
1. Bezpieczeństwo danych w świetle RODO – analiza ryzyka i adekwatność środków – <i>Aleksander P. Czarnowski, Maciej Gawroński</i>	263
1.1. Bezpieczeństwo odpowiednie do ryzyka	263
1.1.1. Ryzyko	264
1.1.2. Ryzyko naruszenia praw lub wolności	265
1.1.3. Analiza ryzyka	266
1.2. Elementy oceny adekwatności środków bezpieczeństwa danych	268
1.2.1. Stan wiedzy technicznej	268
1.2.2. Koszt	268
1.2.3. Cechy samego przetwarzania	269
1.2.4. Ryzyko naruszenia praw lub wolności	269
1.3. Nie trzeba wymyślać procesu samemu?	276
1.4. Środki bezpieczeństwa	277
1.5. Jak z tego wybrnąć na skróty?	280
2. Pseudonimizacja i szyfrowanie – preferowane środki zabezpieczania danych osobowych – <i>Aleksander P. Czarnowski, Maciej Gawroński, Paweł Punda</i>	280
2.1. Uwagi wstępne	280
2.2. Szyfrowanie	281
2.3. Pseudonimizacja	282
2.4. Anonimizacja	283
2.5. Pseudonimizacja czy szyfrowanie	283
2.5.1. Bezpieczeństwo	284
2.5.2. Analiza ryzyka	284
2.5.2.1. Ocena skutków dla ochrony danych ...	287
2.5.2.2. Metodyka analizy ryzyka	287
2.6. <i>Privacy by design</i>	290
2.7. Notyfikacja naruszeń ochrony danych	290
2.8. Zastosowania biznesowe pseudonimizacji	290

2.9. Podsumowanie	291
3. <i>Privacy by design</i> , czyli projektowanie prywatności – Maciej Gawroński, Katarzyna Kunda	292
3.1. <i>Privacy by design</i>	292
3.1.1. Z czego się składa projektowanie prywatności	294
3.1.1.1. Bezpieczeństwo	294
3.1.1.2. Pseudonimizacja	295
3.1.1.3. Minimalizacja	296
3.1.2. Jak wdrożyć <i>privacy by design</i> w organizacji? ...	296
3.1.2.1. Projektowanie prywatności w konkretnym projekcie	296
3.1.2.2. Zasady projektowania prywatności ...	296
3.1.2.3. Od kiedy projektować prywatność ...	297
3.2. Certyfikacja projektowania prywatności i domyślnej prywatności	298
4. <i>Privacy by default</i> , czyli domyślna ochrona danych – minimalizacja – Maciej Gawroński, Katarzyna Kunda	298
4.1. Zasada <i>privacy by default</i>	298
4.2. <i>Privacy by default</i> , czyli minimalizacja	299
4.3. Atrybuty domyślnej prywatności	300
4.4. Wskazówki praktyczne	300
4.5. Udostępnianie nieokreślonej liczbie osób	301
4.6. Certyfikacja projektowania prywatności i domyślnej prywatności	302
5. Ocena skutków dla ochrony danych krok po kroku – Katarzyna Kloc	302
5.1. Uwagi wstępne	302
5.2. „Kwalifikowana” analiza ryzyka i rozliczalność	303
5.3. Podobne procesy, jedna DPIA	305
5.4. Analiza ryzyka do kwadratu	305
5.4.1. Analiza ryzyka	306
5.4.2. Jak w praktyce można przeprowadzić analizę ryzyka pierwszego stopnia i mieć wstępny przegląd operacji wymagających DPIA?	307
5.5. DPIA – kiedy trzeba?	307
5.5.1. Duża skala	308

5.5.2. Wytyczne Grupy Roboczej Art. 29	310
5.6. Jak określić, czy w naszej firmie należy przeprowadzić DPIA i w odniesieniu do których procesów?	313
5.6.1. Urzędowy katalog operacji DPIA	314
5.7. Kiedy nie trzeba przeprowadzać DPIA?	315
5.8. DPIA krok po kroku	316
5.8.1. Uwagi ogólne	316
5.8.2. IOD	318
5.8.3. Eksperti	318
5.8.4. Reprezentanci grup docelowych	319
5.8.5. Uprzednie konsultacje z organem nadzorczym	319
5.9. Wytyczne GODO	320

Rozdział IV

Przetwarzający dane

1. Powierzenie danych oraz elementy nowej umowy powierzenia danych – <i>Aleksander P. Czarnowski,</i> <i>Maciej Gawroński, Patrycja Naklicka</i>	321
1.1. Uwagi wstępne	321
1.2. Opis gwarancji zgodności	321
1.3. Pisemna umowa	322
1.4. Zgoda na podpowierzenie danych	322
1.5. Transfer obowiązków na podprzetwarzającego	323
1.6. Zakaz „wydmuszki”	323
1.7. Przedmiot przetwarzania	324
1.8. Pisemność poleceń ADO	324
1.9. Zobowiązania do poufności	324
1.10. Bezpieczeństwo danych	325
1.11. Obsługa praw jednostki	325
1.12. Wsparcie obowiązków bezpieczeństwa administratora	326
1.13. Notyfikacja podejrzenia naruszenia ochrony danych	326
1.14. Usuwanie i zwrot danych	327
1.15. Obowiązek rozliczenia się ze zgodności z umową ...	327

1.16. Podleganie audytom	328
1.17. Odpłatność	328
1.18. Informowanie o legalności poleceń	328
1.19. Procedura rozstrzygania legalności	328
1.20. Zasady odpowiedzialności	329
1.21. Wyznaczanie inspektora ochrony danych	329
2. Powierzenie danych oraz elementy nowej umowy powierzenia danych – <i>Aleksander P. Czarnowski,</i> <i>Maciej Gawroński, Patrycja Naklicka</i>	329
2.1. Umowy powierzenia a umowy SLA	329
2.1.1. Dostępność systemu SLA i czas reakcji	330
2.1.2. SLA w praktyce	330
2.1.3. Standaryzacja umów SLA a zgodność z RODO	331
2.2. Nowe wyzwania dla administratora i procesora	331
2.3. Rekomendacje	332

Rozdział V

Zarządzanie incydentami	333
1. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu (art. 33 RODO) – <i>Maciej Gawroński, Zuzanna Piotrowska</i>	333
1.1. Przepis	333
1.2. Co to jest naruszenie ochrony danych osobowych? ...	334
1.2.1. Naruszenie ochrony danych wg Grupy Roboczej Art. 29	336
1.2.1.1. Naruszenie poufności	336
1.2.1.2. Naruszenie dostępności	337
1.2.1.3. Naruszenie integralności	337
1.3. Czy każde naruszenie trzeba zgłaszać?	337
1.3.1. Procedura zgłaszania	338
1.3.1.1. Termin dla administratora	338
1.3.1.2. Termin dla przetwarzającego	338
1.3.2. Stwierdzenie naruszenia	339
1.3.3. Zgłoszenie – treść i forma	341
1.3.4. Powiadamianie z opóźnieniem	342
1.3.5. Obowiązki podmiotu przetwarzającego	343

1.4. Kiedy mimo wystąpienia incydentu naruszenia ochrony danych nie trzeba powiadamiać organu nadzorczego?	343
1.4.1. Kwestie praktyczne	345
1.4.2. Dokumentowanie naruszeń	346
1.4.3. Sankcja administracyjna	347
1.5. Elementy systemu zgłaszania naruszeń	347
2. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych (art. 34 RODO) – <i>Katarzyna Kloc, Maciej Gawroński</i>	348
2.1. Wstęp	348
2.2. Wysokie ryzyko naruszenia praw lub wolności	348
2.2.1. Prawa i wolności	349
2.3. Wyjątki od obowiązku zawiadomienia	350
2.3.1. Działania prewencyjne	351
2.3.2. Działania następne	351
2.4. Zawiadomienie	351
2.4.1. Treść zawiadomienia	351
2.4.2. Forma zawiadomienia	352
2.4.3. Ogłoszenie w miejscu zawiadomienia	353
2.4.4. Termin zawiadomienia	353
2.5. Uzgodnienia z organem nadzorczym	354

Rozdział VI

Inspektor ochrony danych (IOD)	355
1. Inspektor ochrony danych – wyznaczenie i status – <i>Michał Kibil, Maciej Gawroński</i>	355
1.1. IOD – ewolucja czy rewolucja	355
1.2. Kto ma obowiązek wyznaczenia inspektora ochrony danych?	356
1.2.1. Organ lub podmiot publiczny	357
1.2.2. Działalność wymagająca systematycznego i regularnego monitorowania oraz przetwarzanie na dużą skalę	358
1.2.2.1. Główna działalność	358
1.2.2.2. Monitorowanie osób	358
1.3. Działanie w ramach zrzeczeń i grup przedsiębiorców ...	362

1.4. Kwalifikacje IOD	363
1.5. Zatrudnienie IOD	364
1.6. Status inspektora danych	365
1.6.1. Obowiązki administratora względem IOD ...	365
1.6.2. Niezależność IOD	367
2. Zadania inspektora ochrony danych osobowych	
– <i>Michał Kibil, Maciej Gawroński</i>	368
2.1. Wstęp	368
2.2. Informacje poufne oraz unikanie konfliktu	
interesów	368
2.3. Zadania inspektora ochrony danych	370

Rozdział VII

Regulator	372
1. Organ nadzorczy – status, rola i obowiązki	
– <i>Katarzyna Kunda, Patrycja Naklicka,</i>	
<i>Zuzanna Piotrowska</i>	372
1.1. Niezależność	372
1.2. Cechy i gwarancje niezależności	373
1.3. Członkowie organu nadzorczego	374
1.3.1. Wybór	374
1.3.2. Okres kadencji – konflikt interesów	375
1.4. Rola organu nadzorczego	375
1.4.1. Kompetencje z art. 57 RODO	375
1.5. Bezpłatność	376
2. Uprawnienia organu nadzorczego z zakresu ochrony danych	
osobowych – <i>Katarzyna Kunda, Patrycja Naklicka,</i>	
<i>Zuzanna Piotrowska</i>	377
2.1. Wstęp	377
2.2. Uprawnienia kontrolne	377
2.2.1. Rodzaje i techniki kontroli	378
2.2.2. Przebieg kontroli	378
2.2.3. Zakres kontroli	379
2.2.4. Uprawnienia pokontrolne	380
2.2.5. Obowiązek zachowania tajemnicy	380
2.3. Kary przewidziane przez RODO	380

2.4. Udzielanie zezwoleń i kompetencje doradcze	381
2.5. Obowiązek rozpatrywania skarg przez PUODO	381

Rozdział VIII

Środki ochrony prawnej, odpowiedzialność i sankcje

1. Środki ochrony prawnej – odpowiedzialność cywilnoprawna i administracyjna – <i>Maciej Gawroński</i> ...	382
1.1. Wstęp	382
1.2. Skarga do organu nadzorczego	383
1.3. Skarga do sądu (administracyjnego) na organ nadzorczy	384
1.4. Odpowiedzialność cywilnoprawna – żądanie zaniechania lub zachowania	385
1.4.1. Prawo do sądu	385
1.4.2. Właściwość miejscowa sądu	386
1.4.3. Tryb procesowy	386
1.5. Odpowiedzialność odszkodowawcza	387
1.5.1. Szkada majątkowa i niemajątkowa	387
1.5.2. Administrator i przetwarzający	387
1.5.3. Uwolnienie się od odpowiedzialności	388
1.5.4. Domniemanie winy	389
1.5.5. Współodpowiedzialność	389
1.5.6. Właściwość sądu	390
1.5.7. Proces cywilny	390
1.6. Reprezentacja podmiotów danych przez wyspecjalizowane podmioty	390
2. Sankcje administracyjne za naruszenie przepisów RODO – <i>Maciej Gawroński</i>	391
2.1. Wstęp	391
2.2. Komu grożą kary?	391
2.3. Jakie powinny być kary?	391
2.4. Kara większa i kara mniejsza	391
2.5. Księgowość karania	392
2.6. Konfiskata korzyści z „rodoprzestępstwa”	394
3. Odpowiedzialność podmiotu przetwarzającego – <i>Maciej Gawroński</i>	394

Część B

Wzory dokumentów

Wzór nr 1a. Klauzula zgody na przetwarzanie danych osobowych zwykłych	399
Wzór nr 1b. Klauzula zgody na przetwarzanie danych osobowych „szczególnych kategorii”	400
Wzór nr 2. Klauzula informacyjna o prawie do cofnięcia zgody	402
Wzór nr 3. Klauzula informacyjna o przetwarzaniu danych	403
Wzór nr 4. Klauzula informacyjna w przypadku współadministrowania danymi	411
Wzór nr 5. Klauzula o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu – element klauzuli informacyjnej	413
Wzór nr 6. Umowa powierzenia przetwarzania danych osobowych	415
Wzór nr 7. Szczegółowa klauzula zgody na podpowierzenie ...	426
Wzór nr 8. Sprzeciw administratora danych osobowych wobec podpowierzenia	427
Wzór nr 9. Upoważnienie do przetwarzania danych osobowych	428
Wzór nr 10. Klauzula informacyjna dla osoby, której dane dotyczą, o przekazaniu jej danych do państwa trzeciego	430
Wzór nr 11. Polityka ochrony danych osobowych	433

Wzory rejestrów

Wzór Rejestru Czynności Przetwarzania Danych	455
Tożsamość administratora	455
Rejestr przetwarzającego	456
RCPD ADO	wklejka
Wzór Rejestru Naruszeń Ochrony Danych Osobowych ...	wklejka

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)
- 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. (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 2017 r. poz. 459 ze zm.)
- 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. 108 ze zm.)
- 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.)

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 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.)
u.r.	– ustawa z 29.09.1994 r. o rachunkowości (Dz.U. z 2018 r. poz. 395 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.)
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

Część A

KOMPENDIUM RODO

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 zdecydo-

wanego 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 ryzyk związanych z przetwarzaniem danych osobowych i dostosowania sposobów ochrony danych do tych ryzyk, a także ze względu na wprowadzenie zasady rozliczalności – obowiązku wykazania zgodności przez obowiązanego.



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

Ogólne rozporządzenie o ochronie danych 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).

1.2.3. Bezpośredniość

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

Bezpośredniość stosowania i w konsekwencji rola „ustawy” o ochronie danych osobowych to cechy odróżniające RODO od tracącej wkrótce moc 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), która 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.

RODO jako wspólna nowa „ustawa” o ochronie danych ma zapewnić wysoki, ujednolicony poziom ochrony danych w całej Unii Europejskiej. Dzięki swojej ogólności i wysokopoziomowości RODO pozostawia jednocześnie duży zakres swobody w podejściu, luz interpretacyjny i praktykę do wypracowania w poszczególnych państwach członkowskich.

1.2.4. Konsekwencje dla polskich przedsiębiorców

Od 25.05.2018 r. przedsiębiorcy szukający przepisów dotyczących ochrony danych osobowych przetwarzanych w organizacji muszą sięgnąć w pierwszej kolejności i bezpośrednio do przepisów unijnych, tj. do RODO, a nie jak dotychczas do ustawy z 29.08.1997 r. o ochronie danych osobowych i aktów wykonawczych do niej czy też do nowej ustawy o ochronie danych osobowych, która ma zostać przyjęta, według zapowiedzi Ministerstwa Cyfryzacji z grudnia 2017 r., najpóźniej w kwietniu 2018 r.

RODO formalnie weszło w życie już 25.05.2016 r., ale jego bezpośrednie stosowanie (i tym samym egzekwowalność) rozpocznie się dopiero 25.05.2018 r. Nie bez powodu organizacje dostały 2 lata na dostosowanie do wymogów RODO swoich procesów przetwarzania danych osobowych na poziomie organizacyjnym, dokumentowym, proceduralnym, technicznym i świadomościowym.

1.3. Prywatność, prawa, bezpieczeństwo – filary RODO

RODO ma na celu budowę nowego, jednolitego na poziomie UE systemu ochrony danych osobowych, który opiera się na trzech filarach: I. **Legalność** – zasady, które organizacje muszą wdrożyć i stale przestrzegać.

II. **Prawa jednostki** – wiele praw osób, których dane dotyczą, związanych z przetwarzaniem ich danych osobowych, z punktu widzenia organizacji – konkretne procesy do obsłużenia.

III. **Bezpieczeństwo danych** – proces ciągłego zapewniania bezpieczeństwa rozumiany jako zespół działań podejmowanych przez organizacje w celu zapewnienia poufności, integralności, dostępności przetwarzanych danych osobowych i obrony przed zagrożeniami.

Każdy z filarów RODO to zasady do zrozumienia i wdrożenia, obowiązki do spełnienia, procesy do obsłużenia, dokumentacja

do opracowania i przyjęcia w ramach organizacji, funkcjonalności IT do wdrożenia i wszelkie inne działania, dzięki którym organizacja będzie mogła stwierdzić i wykazać, że przetwarza dane osobowe w duchu i zgodnie z RODO. Każdy filar to w praktyce nowe wyzwania.

Fundamentem RODO jest zasada **rozliczalności**. W praktyce oznacza to, że przedsiębiorca i inna organizacja muszą być w stanie rozliczyć się z tego, jak przestrzegają oraz jak realizują poszczególne przepisy RODO. Jest to nie lada wyzwanie, ponieważ przepisy te są bardzo ogólne i nie zawierają konkretnych i praktycznych wskazówek, jak rozumieć i stosować daną normę.

Takie podejście można uznać za domniemanie winy.

Np.**Przykład 1****Rozliczenie wdrożenia RODO**

Administrator wdraża i dokumentuje każdy element i krok tego procesu, poczynawszy od uchwały zarządu inicjującej projekt wdrożenia RODO po dokumentowanie szkoleń, spotkań, rozłożenie RODO na konkretne obowiązki i opracowanie odpowiedniej dokumentacji. Wdrożenie i utrzymanie takiej dokumentacji wdrożenia RODO oraz dokumentacji zgodności pozwala administratorowi rozliczyć się z RODO.

Np.**Przykład 2****Nierozliczenie zgody marketingowej**

Klient zwraca się o dostęp do danych i kopię danych, w tym o kopię zgody marketingowej udzielonej administratorowi. Administrator nie jest w stanie odszukać zgody, w związku z tym przedstawia tylko informację, że zgoda została udzielona, i podaje jej domniemany zakres. Klient skarży się do Urzędu Ochrony Danych, że takiej zgody nie udzielał, i Urząd wszczyna postępowanie kontrolne, w trakcie którego okazuje się, że administrator danych nie zadbał o uporządkowaną archiwizację zgód marketingowych. Administrator otrzymuje karę, a równocześnie musi zaprzestać marketingu bezpośredniego do czasu uzyskania nowych zgód lub skatalogowania posiadanych.

1.4. Wymagania RODO

Dotychczas ani w prawie polskim, ani w prawie Unii Europejskiej nie było aktu, który nakładałby tak wysokie kary za nieprzestrzeganie tak niejasnych przepisów praktycznie na wszystkie organizacje. Można się pokusić o stwierdzenie, że RODO jest trudne, inteligentne, surowe, niezrozumiałe, jednak po głębszej analizie, opartej na filarach prywatności, praw jednostki, bezpieczeństwie oraz fundamencie w postaci rozliczalności, ogólne i wysokopoziomowe RODO jawi się po prostu jako **wymagające**.

RODO to:

- a) ogólnikowość,
- b) mierzalność,
- c) bezpośredniość,
- d) surowość,
- e) domniemanie winy.

1.4.1. Ogólnikowość

Zgodnie z art. 5 RODO do danych osobowych powinniśmy podchodzić zgodnie z następującymi zasadami:

- 1) zgodnie z prawem (legalność, oparcie w podstawie prawnej, spełnienie pozostałych obowiązków),
- 2) rzetelnie (bez wprowadzania w błąd, lojalnie, uczciwie, w dobrej wierze),
- 3) przejrzystość (czytelnie, w zrozumiały sposób),
- 4) w konkretnym celu (ograniczenie celu),
- 5) w miarę potrzeb (minimalizacja danych),
- 6) z dbałością o prawidłowość i aktualność danych (prawidłowość),
- 7) nie dłużej niż potrzeba (minimalizacja czasu, czasowość, ograniczenie przechowywania),
- 8) bezpiecznie (integralność i poufność).

W powyższy sposób RODO formułuje podstawowe zasady ochrony danych osobowych. W kolejnych przepisach daje tylko ogólne

wskazówki, w jaki sposób powinny być realizowane. Nie mówi, co to jest „duża skala” przetwarzania, mimo że uzależnia od tego niektóre obowiązki. Nawet w kwestii bezpieczeństwa, poza przykładowym szyfrowaniem i pseudonimizacją, RODO nie daje żadnych konkretnych odpowiedzi, jak spełnić wymóg bezpiecznego przetwarzania danych. Dlatego **wymaga** od administratorów i przetwarzających sporego wysiłku intelektualnego oraz organizacyjnego, aby tak ogólne normy przeanalizować i przełożyć na konkretne oraz dostosowane do danej organizacji dokumenty, technologie, procesy i działania.

1.4.2. Mierzalność

Z jednej strony brak konkretów, z drugiej strony sztywne terminy na obsługę pewnych procesów – to kolejne wyzwanie, jakie RODO stawia przed organizacjami. W przypadku obsługi żądań osób (obsługa praw jednostki) przedsiębiorca ma miesiąc, aby udzielić odpowiedzi na żądanie osoby, której dane dotyczą (np. żądanie usunięcia danych czy przekazania raportu, jakie dane i w jakim celu przedsiębiorca przetwarza). Maksymalnie termin ten może zostać wydłużony o 2 miesiące, ale o przedłużeniu i jego przyczynach należy poinformować w ciągu miesiąca.

W przypadku obowiązkowego zgłaszania naruszenia ochrony danych do organu nadzorczego (nowość w stosunku do starych przepisów) organizacje muszą to zrobić w ciągu 72 godzin od momentu powzięcia wiadomości o naruszeniu.

Konkretne, mierzalne terminy na wykonanie obowiązków ciążyących na administratorze wymagają, aby procesy, w których terminy są nałożone przez prawo, były z góry dobrze i starannie zaplanowane. Mierzalność **wymaga** zapewnienia odpowiednich zasobów, przeszkolenia personelu, zapewnienia odpowiednich środków i procedur, w tym współpracy z podwykonawcami.

1.4.3. Bezpośredniość

RODO obowiązuje w całej Unii Europejskiej i – jak wspomniano – stanowi nową „ustawę” o ochronie danych osobowych. Tylko w Polsce będzie miało bezpośrednie zastosowanie w odniesieniu do ponad 2 mln przedsiębiorców oraz wielu innych organów, organizacji czy instytucji. Bezpośredniość stosowania oznacza, że w praktyce od 25.05.2018 r. na wszystkich administratorach czy przetwarzających ciąży ryzyko ukarania. W związku z tym RODO **wymaga** dogłębnej analizy jego postanowień i przeprowadzenia rzetelnego procesu wdrożenia przez każdego przedsiębiorcę.

1.4.4. Surowość

Mimo ogólności większości przepisów RODO w zakresie kar jest bardzo konkretne. Wprowadza astronomiczny pułap administracyjnych kar pieniężnych za naruszenie jego postanowień. Wysokość kary ma być określana indywidualnie w stosunku do każdego przedsiębiorcy na podstawie co najmniej 18 kryteriów. Kary powinny być „skuteczne, proporcjonalne i odstrasające” (art. 83 ust. 1 RODO).

RODO wyróżnia dwa przedziały kar pieniężnych:

- 1) do 10 mln euro, ewentualnie do 2% całkowitego rocznego światowego obrotu przedsiębiorcy z poprzedniego roku obrotowego, jeśli te 2% to więcej niż 10 mln euro (czyli gdy obrót przedsiębiorcy lub grupy przedsiębiorstw przekracza 500 mln euro),
- 2) do 20 mln euro, ewentualnie do 4% całkowitego rocznego światowego obrotu przedsiębiorcy z poprzedniego roku obrotowego, jeśli te 4% to więcej niż 20 mln euro (czyli gdy obrót przedsiębiorcy lub grupy przedsiębiorstw przekracza 500 mln euro).

RODO **wymaga** więc poważnego podejścia w organizacji do kwestii ochrony danych osobowych, która dotychczas ze względu na brak egzekwowalności bywała traktowana po macoszemu. Surowość i prawdopodobnie nieuchronność kar, o czym będziemy mieli okazję przekonać się już od 25.05.2018 r., nie pozwala na zbagatelizowanie tego

obszaru działalności przedsiębiorców i rzuca zupełnie nowe światło na kwestię ochrony prywatności i danych osobowych.

1.4.5. Domniemanie winy

Jak już wspomniano, fundamentem RODO jest rozliczalność. Domniemanie winy przewidziane w RODO **wymaga**, aby organizacja była w stanie wykazać, rozliczyć się, udowodnić, że przestrzega przepisów o ochronie danych osobowych, nie mając przy tym prostej checklisty zadań czy środków organizacyjnych i technicznych do podjęcia lub wdrożenia. Domniemanie winy wynika z następujących przepisów RODO:

§ art. 5 ust. 2 RODO:
Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i **musi być w stanie wykazać ich przestrzeganie** (rozliczalność);

§ art. 82 ust. 3 RODO:
Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, **jeżeli udowodnią, że w żaden sposób nie ponoszą winy** za zdarzenie, które doprowadziło do powstania szkody.

Podsumowując, wszystkie powyższe elementy powodują, że nowy system ochrony danych osobowych wymaga i wręcz wymusza na organizacjach podjęcie dużego wysiłku związanego z dostosowaniem swoich procesów przetwarzania danych osobowych do RODO. Wysiłek ten musi zostać podjęty wielopoziomowo i kompleksowo w odniesieniu do całej organizacji, nie tylko w aspekcie prawno-dokumentowym, lecz także organizacyjnym, procesowym, świadomościowym i technologicznym.

W zasadzie aby prawidłowo wdrożyć RODO, należy być specjalistą z dziedziny prawa ochrony danych osobowych, informatyki, cyberbezpieczeństwa, organizacji i prowadzenia projektów. Mamy jednak

nadzieję, że w najbliższych latach wykształcą się dobre gotowe wzorce, z których będzie można skorzystać w celu zapewnienia zgodności z RODO, bez konieczności specjalizowania się w tych wszystkich dziedzinach.

1.5. Podział funkcjonalny RODO

RODO ma typową dla unijnych aktów prawnych systematykę i składa się z preambuły (140 motywów zajmuje około 31 z 88 stron RODO) oraz następujących rozdziałów:

- I. Przepisy ogólne
- II. Zasady
- III. Prawa osoby, której dane dotyczą
- IV. Administrator i podmiot przetwarzający
- V. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych
- VI. Niezależne organy nadzorcze
- VII. Współpraca i spójność
- VIII. Środki ochrony prawnej, odpowiedzialność i sankcje
- IX. Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem
- X. Akty delegowane i akty wykonawcze
- XI. Przepisy końcowe.

Z punktu widzenia organizacji, które muszą zrozumieć RODO i przełożyć na konkretne i stosowalne w ich przedsiębiorstwie działania, RODO można podzielić funkcjonalnie, grupując poszczególne zagadnienia w logiczne i powiązane ze sobą merytorycznie **strumienie**. Idąc takim tokiem myślenia, RODO dzieli się na następujące strumienie, w których można wyróżnić pewne zagadnienia:

Zgodność podstawowa:

- podstawowe zasady przetwarzania danych (zgodność z prawem, rzetelność, przejrzystość, konkretność, aktualność, czasowość, retencja, okres przechowywania danych) (art. 5 RODO),

- zgody i informowanie, inne podstawy przetwarzania danych (art. 6 RODO),
- minimalizacja danych i dostępu do nich (*privacy by default*),
- projektowanie prywatności (*privacy by design*), czyli uwzględnianie prywatności przy projektowaniu zmian w swojej działalności, w szczególności technologicznych i organizacyjnych,
- przetwarzanie danych szczególnych kategorii (art. 9 RODO) i danych karnych (art. 10 RODO),
- przetwarzanie niewymagające identyfikacji (art. 11 RODO),
- rejestr czynności przetwarzania danych (art. 30 RODO),
- profilowanie.

Prawa jednostki:

- prawo do informacji o zbieraniu danych (art. 12–14 RODO),
- prawo dostępu do danych i do kopii danych (art. 15 RODO),
- prawo sprostowania i uzupełnienia (art. 16 RODO),
- prawo do usunięcia danych (bycia zapomnianym) (art. 17 RODO),
- prawo do ograniczenia przetwarzania (art. 18 RODO),
- prawo do przenoszenia danych (art. 20 RODO),
- prawo do sprzeciwu względem przetwarzania (art. 21 RODO),
- prawo do ludzkiej interwencji przy przetwarzaniu zautomatyzowanym (art. 22 RODO),

a także inne wymogi tworzące obowiązki po stronie przedsiębiorców i innych organizacji, takie jak:

- prawo do bycia obsługowanym (zakaz ignorowania),
- prawo do „czytelności”,
- prawo do ułatwiania (do przewodnika),
- prawo do terminowości,
- prawo do informacji o prawach,
- prawo do cofnięcia zgody,
- prawo do „równolaćności” niezgody,
- prawo do informacji o odbiorcach danych sprostowywanych,
- prawo do informacji o naruszeniu,
- prawo do skargi i do odwołania,
- prawo do odszkodowania,
- prawo do wsparcia organizacji społecznej.

Bezpieczeństwo:

- integralność i poufność danych jako jedna z podstawowych zasad przetwarzania danych osobowych (art. 5 ust. 1 lit. f, motyw 39 RODO),
- podejście oparte na analizie ryzyka i konieczności ustalenia i zastosowania środków bezpieczeństwa odpowiednich do ryzyka (art. 24, 32 RODO),
- uwzględnienie ochrony danych w fazie projektowania (*privacy by design*) i domyślna ochrona danych (*privacy by default*) (art. 25 RODO),
- ocena skutków dla ochrony danych (*data protection impact assessment*) (art. 35 RODO),
- uprzednie konsultacje z organem nadzorczym po przeprowadzeniu oceny skutków dla ochrony danych (art. 36 RODO).

Przetwarzający:

- umowne uregulowanie relacji między administratorem danych a podmiotem przetwarzającym – nowe wymogi umowy powierzenia przetwarzania danych (art. 28 ust. 3 RODO),
- odpowiedzialność podmiotów przetwarzających (procesorów),
- zasady i standardy wyboru podmiotu przetwarzającego (art. 28 ust. 1 RODO),
- podpowierzenie przetwarzania danych (art. 28 ust. 2 i 4 RODO).

Zgłaszanie incydentów:

- rozumienie i określenie w swojej organizacji, czym jest naruszenie ochrony danych osobowych – klasyfikacja incydentów (art. 4 pkt 12 RODO),
- zgłaszanie naruszeń ochrony danych organowi nadzorczemu w ciągu 72 godzin od stwierdzenia naruszenia (art. 33 ust. 1 RODO),
- procedura i organizacja stwierdzenia naruszenia,
- zgłaszanie naruszeń ochrony danych administratorowi przez podmiot przetwarzający (art. 33 ust. 2 RODO),
- zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 RODO).

Inspektor ochrony danych:

- analiza, czy w organizacji istnieje obowiązek powołania inspektora ochrony danych (obecnie: ABI) (art. 37 RODO),
- status inspektora ochrony danych (art. 38 RODO),
- zadania inspektora ochrony danych (art. 39 RODO),
- zakres odpowiedzialności inspektora ochrony danych.

Regulator:

- status, niezależność, ogólne warunki, właściwość, zadania, uprawnienia organu nadzorczego (art. 51–59 RODO),
- szczegółowe regulacje – nowa krajowa ustawa o ochronie danych osobowych, która jest na etapie prac legislacyjnych.

Eksport danych (poza UE):

- zasady przekazywania danych osobowych do państw trzecich,
- wyjątkowe sytuacje eksportu danych (art. 44–49 RODO).

Przetwarzanie transgraniczne:

- identyfikacja przetwarzania transgranicznego (czyli w kilku krajach UE) w ramach organizacji,
- ustalenie wiodącego organu nadzorczego,
- ustalenie głównej jednostki organizacyjnej.

Kodeksy i certyfikacja:

- kodeksy branżowe i sektorowe związane z postępowaniem z danymi osobowymi (art. 40 RODO),
- monitorowanie zatwierdzonych kodeksów (art. 41 RODO),
- certyfikacja (art. 42 RODO),
- podmioty certyfikujące (art. 43 RODO).

Kary i odpowiedzialność:

- prawo do wniesienia skargi do organu nadzorczego (art. 77 RODO),
- prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu (art. 78 RODO),
- prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu (art. 79 RODO),

- prawo do odszkodowania (art. 82 RODO),
- administracyjne kary pieniężne (art. 83 RODO),
- przepisy karne.

2. Przedmiotowy i terytorialny zakres stosowania RODO

2.1. Zakres stosowania RODO

Materialny i terytorialny zakres stosowania RODO został wyznaczony w art. 2 i 3.

2.1.1. Zakres przedmiotowy

Zgodnie z brzmieniem art. 2 ust. 1 RODO ma zastosowanie do **(a)** przetwarzania **(b)** danych osobowych w **(c)** sposób całkowicie lub częściowo zautomatyzowany oraz do **(d)** przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

Dla zrozumienia przepisu dotyczącego przedmiotowego zakresu stosowania RODO należy się odnieść do regulacji z art. 1, mówiącej o przedmiocie i celu RODO, i z art. 3, dotyczącej terytorialnego zakresu, oraz do definicji. Aby określić, czy RODO ma zastosowanie do danego przedsiębiorcy (jakiegokolwiek organizacji) lub danego procesu, należy zrozumieć, co oznaczają poszczególne elementy przepisu wyznaczającego przedmiotowy zakres stosowania RODO, tj.:

- a) przetwarzanie danych – wszelkie operacje (czynności) wykonywane na danych osobowych, np. samo ich przechowywanie;
- b) dane osobowe – informacje o zidentyfikowanych (konkretnych) lub możliwych do zidentyfikowania osobach fizycznych, np. imię, nazwisko, PESEL, numer telefonu;
- c) całkowite lub częściowo zautomatyzowane przetwarzanie danych – przetwarzanie danych za pomocą systemów informatycznych,

np. w Outlooku, baza danych w zaawansowanym systemie klasy CRM, ale również rejestrowanie danych za pomocą kamer wideo (telewizja przemysłowa, ochrona obiektów). Pojęcie zautomatyzowanego przetwarzania danych celowo nie zostało w RODO zdefiniowane, aby zachować technologiczną neutralność regulacji. Ponieważ przetwarzanie zautomatyzowane nie musi odnosić się do danych stanowiących część zbioru danych (uporządkowanych), RODO stosuje się również do danych nieustrukturyzowanych, np. danych osobowych zawartych w treści e-maili między pracownikami;

- d) przetwarzanie w inny sposób danych osobowych stanowiących część zbioru lub mających stanowić część zbioru danych – przetwarzanie manualne (ręczne) danych osobowych, które w tym wypadku muszą stanowić część zbioru danych, uporządkowanego zestawu tych danych (np. alfabetycznie).



Przykład

Nieduży przedsiębiorca posiadający dane swoich klientów czy pracowników i wykonujący na tych danych jakiekolwiek operacje, choćby prowadzący z nimi korespondencję i przechowujący ją na komputerze, niezależnie od liczby tych danych (np. pięciu klientów w postaci spółek z o.o., dwóch pracowników), ma obowiązek przetwarzać te dane zgodnie z RODO. Nawet jeśli klientami są spółki kapitałowe, należy stosować RODO, ponieważ w spółkach tych pracują ludzie i przedsiębiorca komunikuje się z konkretnymi osobami i na ogół przetwarza różne informacje o nich, jak choćby adres e-mail i telefon komórkowy.

2.1.2. Wyłączenia stosowania RODO

W niektórych sytuacjach, mimo że organizacja przeprowadza operacje na danych osobowych, które wchodzą w zakres przedmiotowy określony w art. 2 ust. 1, RODO nie ma zastosowania:

- 1) działalność nieobjęta zakresem prawa Unii Europejskiej – aktywność wyłączona z kompetencji organów unijnych w zakresie tworzenia prawa, np. bezpieczeństwo narodowe, obronność, zagadnienia stanu cywilnego;

- 2) działania państw członkowskich wchodzące w zakres tytułu V rozdział 2 Traktatu o Unii Europejskiej – wspólna polityka zagraniczna i bezpieczeństwo;
- 3) działania osób fizycznych o czysto osobistym lub domowym charakterze – działalność pozostająca bez związku z działalnością zawodową lub handlową, np. lista gości weselnych, lista adresów przyjaciół;
- 4) działania właściwych organów do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom – działania takie podlegają szczególnemu aktowi prawnemu – tzw. dyrektywie policyjnej, czyli dyrektywie 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 uchyłającej decyzję ramową Rady 2008/977/WSiSW. RODO znajduje jednak zastosowanie do sądów i innych organów wymiaru sprawiedliwości w ich sprawach wewnętrznych (np. pracowniczych);
- 5) wypowiedź dziennikarska, akademicka lub literacka – RODO stosuje się w ograniczonym zakresie do tego typu wypowiedzi, aby pogodzić prawo do ochrony danych osobowych na mocy niniejszego rozporządzenia z wolnością wypowiedzi i informacji. Stosownych wyjątków należy szukać przede wszystkim w nowej ustawie o ochronie danych osobowych i przepisach wprowadzających.

2.1.3. Zakres terytorialny

§ Artykuł 3 ust. 1 RODO wyznacza terytorialny zakres jego stosowania:

Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych **w związku z działalnością prowadzoną przez**

jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, **niezależnie od tego, czy przetwarzanie odbywa się w Unii.**

Takie ujęcie zakresu terytorialnego jest szerokie i ma zapewnić jak najpełniejszą ochronę danych osobowych, niezależnie od tego, gdzie faktycznie znajdują się środki techniczne wykorzystywane do przetwarzania danych. Ponadto aby RODO miało zastosowanie, wystarczy jedynie związek przetwarzania z działalnością jednostki organizacyjnej znajdującej się na terenie Unii Europejskiej. Samo przetwarzanie może odbywać się poza Unią, co stanowi istotną różnicę w odniesieniu do dotychczas obowiązujących przepisów. Nowością jest również rozszerzenie stosowania RODO pod względem terytorialnym do procesorów.



Zgodnie z art. 3 ust. 2 RODO zakres terytorialny stosowania RODO rozciąga się również na następujące sytuacje:

Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych **osób**, których dane dotyczą, **przebywających w Unii**, przez administratora lub podmiot przetwarzający, niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

- a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
- b) monitorowaniem ich zachowania, o ile do zachowania zachodzi w Unii.

Oznacza to, że nawet podmioty zlokalizowane poza Unią Europejską w przypadku przetwarzania danych osób z UE będą musiały stosować europejskie przepisy o ochronie danych osobowych. Jest to bardzo istotna zmiana w stosunku do dotychczas obowiązujących przepisów, zgodnie z którymi podmioty mające siedzibę w państwie trzecim i przetwarzające dane osobowe spoza Europejskiego Obszaru Gospodarczego lub wykorzystujące środki techniczne znajdujące się na terenie Polski wyłącznie do przekazywania danych do państwa trzeciego nie podlegały polskiej ustawie o ochronie danych osobowych.

Dotychczasowe uwarunkowania prawne stwarzały możliwość ucieczki spod reżimu surowych, sformalizowanych standardów ochrony danych osobowych wyznaczonych przez polskie przepisy o ochronie danych osobowych. Międzynarodowe grupy kapitałowe mogły tak zorganizować procesy przetwarzania danych, aby podmiotem decydującym o celach i środkach przetwarzania danych była faktycznie np. spółka matka z siedzibą w Stanach Zjednoczonych, a działalność polskiej spółki lokalnej ograniczała się do przekazywania danych do spółki matki. W ten sposób można było próbować „ucieć” od polskiego rygoru ochrony danych.

RODO takiej możliwości nie daje. Jakikolwiek oferowanie towarów lub usług osobom z UE, nawet nieodpłatnie, bez względu na siedzibę administratora i miejsce przetwarzania danych, będzie musiało się odbywać zgodnie z RODO.

Również w przypadku monitorowania zachowania osób przebywających na terenie Unii Europejskiej przez organizacje z państw trzecich organizacje te będą musiały proces ten przeprowadzać zgodnie z RODO.



Przykład

Spółka znajdująca się w USA i prowadząca globalny sklep internetowy działający również w Polsce będzie musiała prowadzić działalność w zakresie polskiego sklepu internetowego zgodnie z RODO, nawet jeżeli przetwarza dane za pomocą środków technicznych znajdujących się na terenie USA.

Ustęp 3 art. 3 RODO mówi z kolei o tym, że RODO ma zastosowanie również do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale w miejscu, gdzie na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego, czyli np. w ambasadach, konsulatach, na statkach morskich czy w samolotach.