

# DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH ZE WZORAMI

redakcja naukowa Mariusz Jagielski

---

Artur Cieřlik, Magdalena Czaplińska, Paweł Fajgielski, Mariusz Jagielski  
Damian Karwala, Paulina Komorowska-Mrozik, Dominik Lubasz, Marta Otto  
Katarzyna Palka-Bartoszek, Wojciech Piszewski, Marlena Sakowska-Baryła  
Paweł Tobiczek, Mariola Więckowska

**EDYTOWALNE WZORY DOSTĘPNE  
NA STRONIE INTERNETOWEJ**

---

**2**

WYDANIE ZAKTUALIZOWANE I UZUPEŁNIONE

---

# DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH ZE WZORAMI

redakcja naukowa Mariusz Jagielski

---

Artur Cieřlik, Magdalena Czaplńska, Paweł Fajgielski, Mariusz Jagielski  
Damian Karwala, Paulina Komorowska-Mrozik, Dominik Lubasz, Marta Otto  
Katarzyna Palka-Bartoszek, Wojciech Piszewski, Marlena Sakowska-Baryła  
Paweł Tobiczcyk, Mariola Więckowska

---

Zamów książkę w księgarni internetowej

**proinfo.pl**  
księgarnia internetowa

**2**

WYDANIE ZAKTUALIZOWANE I UZUPEŁNIONE

---

Materiały uzupełniające na stronie  
[www.dokumentacja-ochrony-danych-osobowych.wolterskluwer.pl](http://www.dokumentacja-ochrony-danych-osobowych.wolterskluwer.pl)  
będą dostępne do 30 czerwca 2024 r.

Jeżeli w książce nie ma zdrapki  
z kodem aktywacyjnym,  
prosimy o kontakt  
tel. 801 04 45 45

# PIKTOGRAMY

wskazują ważne elementy  
książki i ułatwiają  
ich odnalezienie



Ważne



Przykłady



Podstawa prawna  
Kontekst prawny



Pytania  
Zadania



Rozwiązania  
Odpowiedzi



Stanowisko stron  
Pogląd



Orzecznictwo



Literatura



Historia



Nowe przepisy

Stan prawny na 1 maja 2022 r.

Recenzent

Dr hab. Andrzej Krasuski, prof. UJD

Wydawca

Monika Pawłowska

Redaktor prowadzący

Kinga Zając

Opracowanie redakcyjne

Trzy kropki Joanna Maź

Projekt okładek serii

Wojtek Janikowski, Przemek Dębowski

Poszczególne części opracowali:

Artur Cieślik – rozdział 5

Magdalena Czaplińska, Marlena Sakowska-Baryta – rozdział 4

Paweł Fajgielski – rozdział 10

Mariusz Jagielski – przedmowa do drugiego wydania, rozdział 1

Damian Karwala – rozdział 13

Paulina Komorowska-Mrozik – rozdział 6

Dominik Lubasz – rozdział 12

Marta Otto – rozdział 9

Katarzyna Palka-Bartoszek – rozdziały 7, 8

Wojciech Piszewski, Paweł Tobiczuk – rozdział 3

Marlena Sakowska-Baryta, Mariola Więckowska – rozdział 11

Paweł Tobiczuk – rozdział 2

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

ISBN 978-83-8286-382-6

2. wydanie zaktualizowane i uzupełnione

Wolters Kluwer Polska Sp. z o.o.

Dział Praw Autorskich

01-208 Warszawa, ul. Przyokopowa 33

tel. 728 313 462

e-mail: PL-ksiazki@wolterskluwer.com

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

## SPIS TREŚCI

<b>Wykaz skrótów</b> .....	13
<b>Przedmowa do drugiego wydania</b> .....	17
<b>Rozdział 1</b>	
<b>Dokumentacja ochrony danych osobowych zgodna z RODO</b> .....	21
1.1. Wprowadzenie .....	21
1.2. Podstawy prawne i zasady prowadzenia dokumentacji ochrony danych osobowych .....	22
1.3. Podmioty zobowiązane do opracowania dokumentacji ochrony danych osobowych .....	26
1.4. Zakres przedmiotowy dokumentacji ochrony danych osobowych .....	29
Literatura .....	33
<b>Rozdział 2</b>	
<b>Polityka ochrony danych osobowych</b> .....	35
2.1. Wprowadzenie .....	35
2.2. Struktura polityki .....	36
2.3. Zakres przedmiotowy polityki .....	37
2.4. Szczegółowa część polityki – uwagi praktyczne .....	42
2.4.1. Procedura retencji danych osobowych .....	44
2.4.2. Procedura wyboru dostawcy przetwarzającego dane osobowe ...	46
2.4.3. Procedura obsługi żądań podmiotów danych .....	48
2.5. Możliwe rozszerzenie treści polityki .....	49
2.6. Polityka w świetle dotychczasowej dokumentacji .....	50
2.7. Wzory .....	52
2.8. Instrukcja korzystania ze wzorów .....	73
Literatura .....	77
<b>Rozdział 3</b>	
<b>Dokumentacja serwisu internetowego</b> .....	79
3.1. Wprowadzenie .....	79

3.2. Zakres obowiązków informacyjnych w serwisie internetowym .....	81
3.2.1. Obowiązki na gruncie RODO.....	81
3.2.2. Dodatkowe wymogi wynikające z przepisów Prawa telekomunikacyjnego i ustawy o świadczeniu usług drogą elektroniczną.....	83
3.3. Sposób realizacji obowiązków informacyjnych w serwisie internetowym.....	84
3.4. Dokumenty stosowane w serwisie internetowym .....	86
3.4.1. Klauzule zgód i skrócone klauzule informacyjne .....	88
3.4.2. Polityka prywatności.....	89
3.4.3. Polityka cookies.....	91
3.5. Wzory.....	93
3.6. Instrukcja korzystania ze wzorów .....	100
Literatura.....	105

## Rozdział 4

### **Prawna i etyczna ocena rozwiązań informatycznych z zastosowaniem sztucznej inteligencji – kwestie dokumentacyjne w kontekście ochrony danych osobowych .....**

<b>Prawna i etyczna ocena rozwiązań informatycznych z zastosowaniem sztucznej inteligencji – kwestie dokumentacyjne w kontekście ochrony danych osobowych .....</b>	<b>107</b>
4.1. Ochrona danych osobowych i sztuczna inteligencja.....	107
4.2. Wykorzystywanie systemów AI, w tym tworzenie nowych danych o osobach fizycznych lub podejmowanie decyzji przez system sztucznej inteligencji wobec takich osób jako wynik działania systemu .....	109
4.3. Uwzględnienie uwarunkowań regulacyjnych oraz dokumentów gremiów europejskich.....	110
4.4. Zakres wstępnych ustaleń i dokumentowania .....	111
4.5. Przejrzystość i wyjaśnialność systemów AI.....	114
4.6. Zagadnienie wykorzystywania w systemach AI danych osobowych ....	117
4.7. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych.....	119
4.8. Prawa osób fizycznych w kontekście przetwarzania danych osobowych w systemach AI .....	121
4.9. Rozliczalność i ryzyko w obszarze zastosowania AI do przetwarzania danych osobowych .....	123
4.10. Analiza modelu biznesowego, w którym będzie wykorzystywany system AI .....	129
Literatura.....	134

## Rozdział 5

<b>Ocena (szacowanie) ryzyka .....</b>	<b>137</b>
5.1. Wprowadzenie .....	137
5.2. Podstawy zarządzania ryzykiem w bezpieczeństwie informacji.....	141

5.3. Wybieranie zabezpieczeń – dobre praktyki.....	176
Literatura.....	179
<b>Rozdział 6</b>	
<b>Ocena skutków dla ochrony danych osobowych.....</b>	<b>181</b>
6.1. Zastosowanie dokumentu .....	181
6.2. Kontekst historyczny.....	182
6.3. Kiedy konieczne jest przeprowadzenie oceny skutków dla ochrony danych .....	182
6.4. Ocena skutków dla ochrony danych – zasady.....	190
6.4.1. Minimalne wymogi DPIA.....	191
6.4.2. Udział osób trzecich w przeprowadzaniu oceny skutków dla ochrony danych.....	193
6.4.2.1. Ekspertci zewnętrzni.....	193
6.4.2.2. Osoby, których dane dotyczą.....	194
6.4.2.3. Podmioty przetwarzające działające w imieniu administratora .....	194
6.5. Ocena skutków dla ochrony danych – wzór.....	194
6.6. Konsekwencje DPIA. Obowiązek konsultacji z organem nadzorczym – Prezesem Urzędu Ochrony Danych Osobowych .....	200
6.6.1. Wniosek o uprzednie konsultacje.....	200
6.6.2. Przebieg i czas trwania konsultacji.....	201
6.6.3. Rezultat konsultacji .....	202
Literatura .....	202
<b>Rozdział 7</b>	
<b>Rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania ....</b>	<b>205</b>
7.1. Wstęp.....	205
7.2. Podstawa prowadzenia rejestrów .....	205
7.2.1. Przepis art. 30 RODO jako formalnoprawne źródło obowiązku prowadzenia rejestrów .....	205
7.2.2. Wpływ ustawodawstwa krajowego na wymóg prowadzenia rejestrów wynikający z art. 30 RODO .....	206
7.2.3. Wyłączenie obowiązku prowadzenia rejestru dla „działalności prasowej”, wypowiedzi w ramach działalności literackiej, wypowiedzi akademickiej .....	208
7.2.4. Wyłączenie obowiązku prowadzenia rejestrów przez przedsiębiorcę lub podmiot zatrudniający mniej niż 250 osób .....	210
7.3. Prawne znaczenie rejestrów w polityce ochrony danych osobowych administratora danych osobowych lub podmiotu przetwarzającego .....	213
7.3.1. Prowadzenie rejestru jako realizacja wymogu przetwarzania danych osobowych zgodnie z RODO .....	214

7.3.2. Prowadzenie rejestru jako narzędzie wykazania przetwarzania danych osobowych zgodnie z RODO wobec organu nadzoru.....	214
7.4. Cel realizacji obowiązku prowadzenia rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania.....	215
7.5. Podmiot zobowiązany do prowadzenia rejestru.....	219
7.6. Dla kogo dostępne są rejestry?.....	222
7.7. Skąd czerpać informacje stanowiące treść rejestru?.....	224
7.8. Obowiązek uaktualniania rejestrów.....	225
7.9. Rejestr i jego forma.....	226
7.10. Czynności przetwarzania danych osobowych.....	227
7.11. Treść rejestru czynności przetwarzania.....	229
7.11.1. Obligatoryjna treść rejestru czynności przetwarzania; art. 30 ust. 1 RODO.....	229
7.11.2. Fakultatywne elementy treści rejestru czynności przetwarzania.....	236
7.12. Kategorie czynności przetwarzania.....	238
7.13. Elementy treści rejestru kategorii czynności przetwarzania.....	239
7.13.1. Obligatoryjne elementy treści rejestru kategorii czynności przetwarzania.....	239
7.13.2. Fakultatywne elementy treści rejestru kategorii czynności przetwarzania.....	240
7.14. Uwagi dotyczące treści zawartych w przykładowych rejestrach: czynności przetwarzania i kategorii czynności przetwarzania.....	240
7.15. Wzory.....	241
Literatura.....	261

## Rozdział 8

<b>Współadministrowanie danymi osobowymi.....</b>	<b>263</b>
8.1. Wstęp.....	263
8.2. Podstawa prawna współadministrowania.....	264
8.3. Elementy istotne dla rozpoznania, czy występuje współadministrowanie.....	265
8.4. Kryteria ustalenia współadministrowania.....	267
8.4.1. Wspólne lub zbieżne decyzje współadministratorów.....	268
8.4.2. Wspólne cele współadministratorów.....	269
8.4.3. Wspólne sposoby przetwarzania danych przez współadministratorów.....	270
8.5. Obowiązki formalne współadministratorów.....	275
8.5.1. Forma porozumienia współadministratorów.....	275
8.5.2. Treść umowy.....	276
8.5.2.1. Elementy obligatoryjne.....	276
8.5.2.2. Elementy fakultatywne.....	276



8.5.3. Znaczenie umowy w stosunkach wewnętrznych między współadministratorami .....	277
8.5.4. Znaczenie umowy wobec osób, których dane dotyczą.....	277
8.5.5. Udostępnienie zasadniczej treści uzgodnień osobom, których dane dotyczą .....	278
8.5.6. Wyznaczenie punktu kontaktowego.....	279
8.5.7. Obowiązki współadministratorów wobec PUODO .....	279
8.6. Współadministrowanie podmiotów publicznych – przykłady.....	280
8.6.1. Współadministrowanie w Systemie Wspomagania Decyzji Państwowej Straży Pożarnej.....	280
8.6.2. Współadministrowanie na potrzeby obsługi bonu turystycznego.....	280
8.6.3. Współadministrowanie Komisji, organów celnych i organów nadzoru.....	281
Literatura.....	292

## **Rozdział 9**

<b>Przetwarzanie danych osobowych w kontekście zatrudnienia.....</b>	<b>293</b>
9.1. Upoważnienie do przetwarzania danych osobowych.....	293
9.1.1. Wprowadzenie.....	293
9.1.2. Wzory upoważnienia do przetwarzania danych osobowych oraz oświadczenia osoby upoważnionej do przetwarzania danych osobowych.....	297
9.1.3. Praktyczne wskazówki .....	300
9.2. Ewidencja osób upoważnionych do przetwarzania danych.....	302
9.2.1. Wprowadzenie.....	302
9.2.2. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych.....	303
9.2.3. Praktyczne wskazówki .....	304
9.3. Umowa powierzenia przetwarzania danych osobowych.....	305
9.3.1. Wprowadzenie.....	305
9.3.2. Wzór ankiety oceny spełnienia wymagań dotyczących ochrony danych osobowych wynikających z RODO oraz wzór umowy powierzenia przetwarzania danych osobowych.....	311
9.3.3. Wskazówki praktyczne .....	325
9.4. Klauzula informacyjna dotycząca przetwarzania danych osobowych pracowników .....	327
9.4.1. Wprowadzenie.....	327
9.4.2. Wzór klauzuli informacyjnej dotyczącej przetwarzania danych osobowych.....	328
9.4.3. Wskazówki praktyczne .....	332
9.5. Monitoring wizyjny.....	332

9.5.1. Wprowadzenie.....	332
9.5.2. Wzory informacji o monitoringu wizyjnym oraz klauzuli informacyjnej o przetwarzaniu danych osobowych w ramach monitoringu wizyjnego.....	337
9.5.3. Praktyczne wskazówki.....	341
9.6. Monitoring poczty elektronicznej i inne formy monitoringu .....	344
9.6.1. Wprowadzenie.....	344
9.6.2. Wzory informacji o funkcjonowaniu monitoringu poczty elektronicznej oraz monitoringu GPS .....	346
9.6.3. Praktyczne wskazówki.....	351
Literatura.....	352

## Rozdział 10

<b>Dokumentacja naruszeń ochrony danych osobowych.....</b>	<b>355</b>
10.1. Wprowadzenie .....	355
10.2. Naruszenie ochrony danych – pojęcie, zakres .....	356
10.3. Obowiązek dokumentowania naruszeń.....	356
10.4. Rejestr naruszeń – zawartość.....	359
10.5. Instrukcja wypełnienia rejestru naruszeń ochrony danych osobowych .....	362
Literatura.....	364

## Rozdział 11

<b>Dokumentacja monitorowania zgodności z RODO – audyty wewnętrzne i weryfikacja powierzenia przetwarzania.....</b>	<b>365</b>
11.1. Wprowadzenie – po co audytować?.....	365
11.2. Audyt wewnętrzny, sprawdzenie, kontrola.....	366
11.3. Wobec kogo wykazywać zgodność z RODO.....	369
11.4. Dokumentacja audytu wewnętrznego.....	371
11.5. Plan audytów wewnętrznych (sprawdzeń, kontroli) .....	373
11.6. Audyty pozaplanowe.....	375
11.7. Sposób i zakres dokumentowania audytu .....	378
11.8. Audyt stanu stosowania RODO .....	380
11.9. Audyt podmiotu przetwarzającego .....	390
11.10. Audyt umów powierzenia przetwarzania danych .....	393
11.11. Zagadnienia audytowe.....	397
11.12. Raport (sprawozdanie) z audytu wewnętrznego .....	406
Literatura.....	408

**Rozdział 12**

<b>Klauzule wyrażenia zgód i klauzule informacyjne .....</b>	<b>411</b>
12.1. Zgoda na przetwarzanie danych osobowych .....	411
12.1.1. Wprowadzenie .....	411
12.1.2. Zgoda jako przesłanka legalizacyjna – zagadnienia ogólne ....	413
12.1.3. Wzory oświadczeń o wyrażeniu zgody .....	415
12.1.3.1. Wyrażenie zgody w procesie rekrutacyjnym.....	415
12.1.3.2. Zgoda na działania marketingowe inne niż przesyłanie informacji handlowej drogą elektroniczną oraz inne niż marketing bezpośredni na podstawie Prawa telekomunikacyjnego.....	416
12.1.3.3. Zgoda na otrzymywanie informacji handlowej drogą elektroniczną .....	417
12.1.4. Szczegółowe wymogi dotyczące zgody .....	418
12.1.4.1. Dobrowolność zgody.....	418
12.1.4.2. Konkretność zgody.....	420
12.1.4.3. Świadomość zgody.....	421
12.1.4.4. Jednoznaczność zgody .....	422
12.1.4.5. Wyraźność zgody.....	424
12.1.4.6. Forma zgody.....	425
12.1.4.7. Dodatkowe wymogi dotyczące pisemnej zgody .....	426
12.1.4.8. Wycofanie zgody.....	426
12.1.4.9. Ciężar dowodu – rozliczalność.....	427
12.2. Klauzule informacyjne.....	429
12.2.1. Wprowadzenie .....	429
12.2.2. Obowiązki informacyjne – zagadnienia ogólne .....	430
12.2.3. Wzory klauzul informacyjnych.....	431
12.2.3.1. Klauzula rekrutacyjna.....	431
12.2.3.2. Klauzula kontrahencka.....	435
12.2.3.3. Klauzula kliencka .....	438
12.2.3.4. Klauzula newsletterowa .....	441
12.2.4. Szczegółowe wymogi dotyczące realizacji obowiązków informacyjnych .....	443
12.2.4.1. Typy obowiązków informacyjnych .....	443
12.2.4.2. Zakres obowiązków informacyjnych.....	445
12.2.4.3. Sposób realizacji obowiązków informacyjnych .....	449
12.2.4.4. Termin realizacji obowiązków informacyjnych.....	452
12.2.4.5. Aktualizacja informacji .....	453
12.2.4.6. Wyłączenia spod obowiązku realizacji.....	454
Literatura.....	458

---

<b>Rozdział 13</b>	
<b>Transfer danych osobowych do państw trzecich.....</b>	<b>459</b>
13.1. Wprowadzenie .....	459
13.2. Podstawy dopuszczalnego transferu danych osobowych oraz kolejność ich stosowania.....	460
13.3. Kontekst historyczny, najważniejsze zmiany .....	464
13.4. Umowy transferowe oparte na klauzulach modelowych .....	466
13.5. Zgoda na transfer danych oraz obowiązek informacyjny .....	468
13.6. Wzory .....	470
13.7. Instrukcja korzystania ze wzorów .....	470
Literatura.....	539
<b>O Autorach .....</b>	<b>541</b>

## PRZEDMOWA DO DRUGIEGO WYDANIA

Przedstawiając w 2019 r. Czytelnikom pierwsze wydanie książki, napisałem, że ochrona danych osobowych to jedna z najbardziej dynamicznie zmieniających się dziedzin prawa. Trzy lata, które upłynęły od tego czasu, w pełni potwierdziły powyższą konstatację. Mimo że podstawowy akt prawny w tej dziedzinie – RODO, nie uległ zmianie, pojawiły się liczne nowe regulacje, dokumenty i rozstrzygnięcia precyzujące, rozszerzające, a w pewnym stopniu także modyfikujące wymagania nałożone na podmioty zobowiązane realizować obowiązki z dziedziny ochrony danych osobowych. Przybrały one postać nowych przepisów szczególnych oraz poprawek do dotychczas obowiązujących aktów prawnych, wytycznych interpretacyjnych, wydanych w szczególności przez Europejską Radę Ochrony Danych (EROD) oraz Prezesa Urzędu Ochrony Danych Osobowych (PUODO), orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE) i sądów polskich oraz decyzji PUODO. Konieczność ich uwzględnienia wymaga m.in. przeprowadzenia analizy dotychczas posiadanej dokumentacji ochrony danych osobowych i jej dostosowania do nowych przepisów, wytycznych i rekomendacji.

Oddawane do rąk Czytelników drugie wydanie *Dokumentacji ochrony danych osobowych ze wzorami* stanowi odpowiedź na powyższe wyzwanie. Zawiera ono nie tylko aktualizację treści zawartych w wydaniu pierwszym, lecz także zostało poszerzone o liczne nowe zagadnienia i wzory. Dość powiedzieć, że w aktualnej wersji książki Czytelnik znajdzie trzy całkowicie nowe rozdziały, a niemal każdy dotychczasowy rozdział jest uzupełniony o nowe formatki, tabele i szablony. Nowe wydanie liczy o 218 stron tekstu więcej niż wydanie pierwsze. Śmiało można powiedzieć, że przedstawiana Czytelnikom publikacja stanowi nowe opracowanie problematyki dokumentacji ochrony danych osobowych.

Przygotowane na potrzeby Czytelników pierwszego wydania zestawienie najważniejszych aktualizacji, zmian i uzupełnień, jakie znajdują się w niniejszym opracowaniu, prezentuje się następująco.

Dodano nowy rozdział odnoszący się do dokumentacji serwisu internetowego. Rozdział zawiera wytyczne dotyczące zakresu i funkcji poszczególnych dokumentów stosowanych powszechnie przez administratorów serwisów WWW, w tym tzw. skróconych klauzul informacyjnych i klauzul zgód, polityki prywatności oraz polityki cookie. W rozdziale

zamieszczone zostały wzory poszczególnych dokumentów wraz z ich omówieniem i instrukcją stosowania przez administratorów serwisów internetowych.

Dodano nowy rozdział omawiający prawne i etyczne zagadnienia, które powinny być uwzględnione w przypadku zastosowania rozwiązań informatycznych z zastosowaniem sztucznej inteligencji. Zgodnie z profilem książki zastosowano w tym względzie podejście praktyczne: prezentowane zagadnienia zostały opracowane w postaci wzorów, tabel i zestawów ułatwiających sprawdzenie stopnia realizacji wymogów. Rozdział zawiera też użyteczne rekomendacje.

Dodano nowy rozdział dotyczący współadministrowania danymi osobowymi oraz statusu współadministratorów. Rozdział uwzględnia treść najnowszych wyroków TSUE dotyczących współadministrowania w przypadku wykorzystywania narzędzi informatycznych, jak również Wytyczne w sprawie koncepcji administratora i procesora nr 7/2020 przyjęte przez EROD w lipcu 2021 r. Kluczowym elementem tej części opracowania jest wzór umowy o współadministrowanie danymi osobowymi.

Rozdział poświęcony audytom wewnętrznym został zmodyfikowany tak poważnie, że wymagał zmiany tytułu na „Dokumentacja monitorowania zgodności z RODO – audyty wewnętrzne i weryfikacja powierzenia przetwarzania”. Zawiera on liczne nowe tabele audytów wraz z ich omówieniem, w tym obejmujące takie obszary, jak: działania zarządcze w organizacji, inwentaryzacja danych osobowych, prowadzenie rejestru czynności przetwarzania oraz mapa przepływu danych w organizacji, wdrożenie zasad ochrony danych osobowych wewnątrz organizacji, oddziaływanie systemu ochrony danych na działania organizacji, zarządzanie procesem szkoleń oraz działaniami zwiększającymi świadomość, zarządzanie ryzykiem związanym z bezpieczeństwem przetwarzania danych osobowych, zarządzanie ryzykiem związanym z przekazywaniem danych osobowych podmiotom zewnętrznym, w tym umowy powierzenia przetwarzania danych i standardowe klauzule umowne, zarządzanie komunikacją z podmiotami danych, realizacja praw podmiotów danych, w tym odpowiadanie na ich żądania oraz obsługa ich skarg, ocena skutków dla ochrony danych oraz stosowanie podejścia opartego na ryzyku, w tym ochrona danych w fazie projektowania i domyślna ochrona danych, proces zarządzania incydentami bezpieczeństwa i naruszeniami ochrony danych wraz z ich zgłoszeniem do organu nadzorczego, monitorowanie sposobu postępowania z danymi, monitorowanie przez IOD lub inne wyznaczone do tego osoby przestrzegania RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych, audyt podmiotu przetwarzającego, audyt umów powierzenia przetwarzania, audyt cyberbezpieczeństwa w IT według ENISA i audyt obszaru przetwarzania danych osobowych.

Rozdział na temat polityki ochrony danych osobowych został uzupełniony o praktyczne wytyczne dotyczące przygotowania szczegółowych procedur w ramach polityki. Nowe

zagadnienia obejmują m.in. procedurę retencji danych osobowych, procedurę wyboru dostawcy oraz procedurę obsługi żądań podmiotów danych.

Rozdział dotyczący oceny (szacowania) ryzyka uzupełniono o nowe szablony, w szczególności wykaz aktywów wspomagających, klasyfikację informacji – czynności przetwarzania danych osobowych, opis rodzaju źródeł ryzyka na potrzeby analizy ryzyka, rejestr ryzyka, raport z szacowania ryzyka. Przedstawiono liczne nowe przykłady, w tym wykaz zawierający 73 przykłady zagrożeń dla bezpieczeństwa danych. W ramach prezentacji sposobów postępowania uwzględniono organizacje o mniejszej skali działalności.

W rozdziale omawiającym problematykę oceny skutków dla ochrony danych osobowych uwzględniono nowy, zmieniony wykaz rodzajów operacji wymagających przeprowadzenia oceny skutków dla ochrony danych (PUODO 8 lipca 2019). Zaktualizowano też wzór oceny skutków dla ochrony danych oraz uzupełniono rozdział o nowe przykłady praktyczne, kiedy ocena skutków dla ochrony danych jest wymagana.

W rozdziale poświęconym rejestrom czynności przetwarzania i kategorii czynności przetwarzania poszerzono liczbę przykładów uzupełnienia rejestrów. W ten sposób wzory rejestrów zostały dostosowane do potrzeb większej liczby adresatów.

Rozdział odnoszący się do dokumentacji pracowniczej został uzupełniony o wzory dotyczące innego niż wizyjny monitoring pracowniczego oraz ankiety kontrolnej. Zawarto w nim też liczne nowe wskazówki praktyczne, przygotowane na podstawie stosownych wytycznych i interpretacji EROD i PUODO oraz tzw. dobrych praktyk.

W rozdziale prezentującym wzory zgód i klauzul informacyjnych uwzględniono najnowsze decyzje PUODO i orzecznictwo sądów administracyjnych, a także przepisy implementujące RODO z 2019 r., w tym przepisy Kodeksu pracy w zakresie dotyczącym zgody pracowników.


W rozdziale poświęconym międzynarodowym transferom danych uwzględniono nowe standardowe klauzule umowne opublikowane przez Komisję Europejską w czerwcu 2021 r., które zastąpiły dotychczasowe klauzule modelowe, uznane za niezapewniające zgodności z RODO. Rozdział prezentuje cztery odrębne wzory umów, bazując na modułach (wariantach) uwzględnionych w nowych klauzulach Komisji. Dodatkowo omówiono kluczowe zmiany w podejściu do stosowania klauzul modelowych i innych instrumentów transferowych będących skutkiem orzeczenia TSUE w sprawie Schrems II.

*Mariusz Jagielski*

## Rozdział 1

# DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH ZGODNA Z RODO

## 1.1. Wprowadzenie

 Dzień 25.05.2018 r., czyli dzień, w którym zaczęło być stosowane 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), zwane RODO, nie stanowi daty początkowej prawnej ochrony danych osobowych. W Europie Zachodniej pierwsze przepisy chroniące dane osobowe pojawiły się już w latach 70. XX w. Ochrona danych na poziomie europejskim funkcjonuje od lat 90. XX w. – kluczową rolę w tym względzie odegrało przyjęcie poprzedniczki RODO – 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<sup>1</sup>. Natomiast w Polsce odpowiednia ustawa o ochronie danych osobowych została uchwalona 29.08.1997 r. (weszła w życie 30.04.1998 r.).

Przez cały ten czas twórcom regulacji prawnych przyświecała idea wypracowania rozwiązań jak najskuteczniej chroniących osoby, których dane są przetwarzane. Zadanie to było o tyle trudne, że w interesie tych ostatnich wcale nie leży wyłącznie ograniczanie wykorzystywania dotyczących ich informacji. Wręcz odwrotnie, zazwyczaj przynosi im to korzyści. Chodzi zarówno o korzyści indywidualne – dostarczenie im potrzebnych usług i świadczeń, jak i o te o charakterze zbiorowym – rozwój ekonomiczny i społeczny dobrobyt, jak również właściwe funkcjonowanie instytucji publicznych. W konsekwencji ochronę danych osobowych należy widzieć w kategoriach próby poszukiwania kompromisu pomiędzy gospodarczymi i administracyjnymi potrzebami przetwarzania informacji o człowieku a koniecznością zagwarantowania mu ochrony jego praw. Ochrona danych osobowych stanowi zatem próbę znalezienia złotego środka

---

<sup>1</sup> Por. M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 10–12.




i wyważenia interesów na rynku (w ramach relacji przedsiębiorcy – klienci) i w państwie (w ramach relacji organy państwowe – obywatele). Przy tym przyjmowane w zajmującej nas dziedzinie regulacje podlegały i podlegają nieustannej ewolucji. Dzieje się tak dlatego, że metody ochrony trzeba na bieżąco dostosowywać do nowych wyzwań, zwłaszcza przemian technologicznych<sup>2</sup>. Te zaś następowały w ostatnich dziesięcioleciach z niezwykłą intensywnością. W konsekwencji prawna ochrona danych osobowych to jedna z najbardziej dynamicznie zmieniających się dziedzin prawa.

Częsta zmiana przepisów nie jest korzystna – ani dla tych, którzy mają je stosować, ani dla tych, którzy mają być przez nie chronieni. Stąd zamysł, by spróbować odnaleźć takie rozwiązania, które będą w stanie przetrwać próbę czasu. Takie właśnie było założenie reformy ochrony danych osobowych, której ostatecznym efektem stało się RODO. Skoro przemiany technologiczne są tak szybkie, że unormowania prawne nie potrafią za nimi nadążyć – jak założyli twórcy reformy – trzeba wypracować na tyle elastyczne metody podejścia, by umożliwiły one reagowanie na bieżąco na pojawiające się zagrożenia, bez konieczności zmiany przepisów. To zaś jest możliwe jedynie w przypadku, gdy ciężar reakcji przeniesiemy z poziomu legislacyjnego na poziom zarządzania bezpieczeństwem. Oznacza to, że trzeba pozostawić swobodę podmiotom odpowiedzialnym za realizację ochrony – administratorom, podmiotom przetwarzającym. Tylko one mogą na bieżąco analizować zagrożenia i dostosowywać metody ochrony do najnowszych wyzwań. Podejście takie nazwano podejściem opartym na ocenie ryzyka (*risk-based approach*) i wokół niego zorganizowano system ochrony danych osobowych w RODO<sup>3</sup>.

Przewidziane reformą nowe rozwiązania ochronne są więc znacznie bardziej elastyczne niż te, które obowiązywały pod rządami wcześniejszych przepisów. Powyższą konstatację można odnieść do większości obszarów ochrony danych osobowych. Jednym z nich – gdzie powyższa zmiana rysuje się najbardziej spektakularnie – jest problematyka dokumentacji ochrony danych osobowych.

## 1.2. Podstawy prawne i zasady prowadzenia dokumentacji ochrony danych osobowych

 Przed 25.05.2018 r. przepisy w miarę precyzyjnie wskazywały dokumenty, które powinni posiadać wszyscy administratorzy oraz podmioty przetwarzające, nierzadko determinując w sposób szczegółowy ich treść. Zasadnicze elementy tej dokumentacji stanowiły:

<sup>2</sup> A. Grzelak, *Główne cele ogólnego rozporządzenia o ochronie danych* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017, s. 21–22; A. Krasuski, *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018, s. 17.

<sup>3</sup> RODO. *Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2017, s. 341. O ryzyku w kontekście RODO por. też A. Krasuski, *Ochrona...*, s. 295 i n.

- 1) polityka bezpieczeństwa informacji (§ 4 r.d.p.d.o.),
- 2) instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (§ 5 r.d.p.d.o.),
- 3) indywidualne upoważnienia do przetwarzania danych osobowych nadane każdej osobie, która bierze udział w procesie przetwarzania danych osobowych (art. 37 u.o.d.o. z 1997 r.),
- 4) indywidualne zobowiązanie do zachowania danych oraz sposobu ich zabezpieczenia w tajemnicy (art. 39 ust. 2 u.o.d.o. z 1997 r.),
- 5) ewidencja osób upoważnionych do przetwarzania danych osobowych (art. 39 u.o.d.o. z 1997 r.),
- 6) dokumentacja sprawdzeń (art. 36b u.o.d.o. z 1997 r. oraz § 3 ust. 3 i § 5 ust. 2 r.t.s.r.z.).


**N!** Reforma ochrony danych osobowych z 2018 r. doprowadziła do tego, że wszystkie akty normatywne, które wymagały opracowania i wdrożenia powyższych dokumentów, przestały obowiązywać<sup>4</sup>. Zaowocowało to istotnymi zmianami w interesującej nas dziedzinie<sup>5</sup>. Zgodnie z nowym podejściem RODO nie zawiera generalnych wytycznych ani co do struktury dokumentacji, ani co do sposobu jej prowadzenia, ani – w końcu – co do jej merytorycznej treści. Swoboda, jaką pozostawiono administratorom i podmiotom przetwarzającym w zakresie zapewnienia ochrony danych osobowych, przejawia się między innymi w tym, że mogą one nie tylko samodzielnie kształtować, ale także opisywać stosowane metody przetwarzania danych osobowych, związane z nimi procedury, jak również zastosowane zabezpieczenia techniczne i organizacyjne. Chodzi o to, by opracowywane dokumenty mogły być jak najbardziej praktyczne, dostosowane do potrzeb konkretnego podmiotu, a także by ograniczyć przypadki tworzenia dokumentów zbędnych, takich, które w kontekście skali i sposobu przetwarzania danych przez dany podmiot nie są użyteczne.

---

<sup>4</sup> Nastąpiło to na podstawie art. 175 u.o.d.o. zasadniczo z dniem 25.05.2018 r. Wyjątkiem jest sektor zapobiegania i zwalczania przestępczości, w którym to przedłużono obowiązywanie niektórych regulacji u.o.d.o. z 1997 r., w tym tych będących podstawą opracowania dokumentacji ochrony danych osobowych, do dnia wejścia w życie przepisów wdrażających dyrektywę 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 uchyłającą decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89, ze sprost.). Przepisy te przybrały ostatecznie postać ustawy z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), która weszła w życie 6.02.2019 r. W tym dniu przepisy u.o.d.o. z 1997 r. oraz przepisy wykonawcze nakazujące opracowanie i wdrożenie wskazanych dokumentów przestały ostatecznie obowiązywać.

<sup>5</sup> Praktyczne porównanie rozwiązań z ustawy o ochronie danych osobowych funkcjonujących przed 25.05.2018 r. oraz z RODO obowiązujących po 25.05.2018 r. zob. D. Lubasz, *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi*, Warszawa 2018, s. 16 i n.

Za ilustrację powyższego problemu mogą posłużyć dotychczasowe dokumenty: polityka bezpieczeństwa informacji oraz instrukcja zarządzania systemem informatycznym. Były to dokumenty, które w poprzednim stanie prawnym obowiązkowo musieli przygotować i wdrożyć niemal wszyscy administratorzy<sup>6</sup>, bez względu na skalę, zakres i sposób działania. Treść obydwu dokumentów wynikała z r.d.p.d.o. i była zasadniczo taka sama dla wszystkich adresatów tego aktu prawnego. Jej opracowanie było uciążliwe, a w niektórych przypadkach, zwłaszcza tzw. mikroprzedsiębiorców, praktyczna przydatność wątpliwa.

 Powyższe nie oznacza, że po 25.05.2018 r. administratorzy i przetwarzający dane osobowe mogą zrezygnować z dokumentacji w ogóle<sup>7</sup>. Wymagania nakładane na nich przez RODO są tak ukształtowane, że w pewnych przypadkach prowadzenie odpowiedniej dokumentacji stanie się celowe. Z tego punktu widzenia zawarte w RODO regulacje można podzielić na dwa rodzaje. Pierwsze to takie, w których wskazano obowiązki, z których wprost wynika konieczność opracowania pewnych konkretnych dokumentów. Prezes Urzędu Ochrony Danych Osobowych wskazuje następujące takie przypadki:

- 1) prowadzenie rejestru czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;
- 2) zgłaszanie naruszenia ochrony danych do organu nadzorczego (UODO) – art. 33 ust. 3 RODO;
- 3) prowadzenie wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO;
- 4) zawartość raportu dokumentującego wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7 RODO<sup>8</sup>.

Cechą charakterystyczną powyższych rozwiązań jest to, że RODO wskazuje przy ich pomocy wprost konkretne treści, które adresat jest zobowiązany opracować. W tym zakresie sporządzenie dokumentu staje się więc koniecznością, gdyż w przeciwnym wypadku administrator lub podmiot przetwarzający nie zrealizowałby nałożonego nań konkretnego obowiązku.

Przypadek drugi to sytuacja, gdy RODO, określając w sposób ogólny zasady i wymogi, którym musi odpowiadać przetwarzanie danych osobowych, tak je formułuje, że ich wykonanie nie będzie możliwe albo bardzo utrudnione, jeśli nie obejmie opracowania stosownych dokumentów. Kluczową rolę w tym względzie odgrywa wyrażona w art. 5 ust. 2 RODO zasada rozliczalności. Wymaga ona, by administratorzy nie tylko prze-

<sup>6</sup> W drugim przypadku pod warunkiem, że przetwarzali dane osobowe w systemie informatycznym.

<sup>7</sup> M. Cwener, *Nowe obowiązki dokumentacyjne związane z przetwarzaniem danych osobowych* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017, s. 100.

<sup>8</sup> UODO, *Dokumentacja przetwarzania danych osobowych zgodnie z RODO*, <https://uodo.gov.pl/pl/138/273> (dostęp: 15.04.2022 r.).

strzegali zasad przetwarzania określonych w RODO, ale by byli w stanie to wykazać<sup>9</sup>. Jak widać, konieczność udokumentowania konkretnych treści nie jest w tym przepisie wyrażona wprost, jednak wymóg umiejętności wykazania, że przestrzega się postanowień rozporządzenia, najprościej zrealizować, dokumentując podejmowane działania i stosowane procedury.

Idea powyższa została rozwinięta i doprecyzowana w art. 24 ust. 1 RODO<sup>10</sup>. Przepis ten nakłada na administratorów obowiązek wdrożenia takich środków technicznych i organizacyjnych, które zapewnią, że przetwarzanie będzie odbywało się zgodnie z rozporządzeniem i administratorzy będą w stanie to wykazać. Realizując wskazany obowiązek, administratorzy powinni uwzględnić charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, a także mają obowiązek poddawania przeglądowi i uaktualniania zastosowanych środków, jeśli tylko zajdzie taka potrzeba.

Powyższy przepis, analogicznie do art. 5 ust. 2 RODO, nie nakłada wprost obowiązku przygotowania konkretnych dokumentacji, jednak nie ulega wątpliwości, że nie można zrealizować wskazanych w nim zaleceń, unikając tworzenia dokumentów. Wręcz przeciwnie, opracowanie i wdrożenie właściwych dokumentów można potraktować jako wspomniany w tym przepisie „środek organizacyjny”, którego zastosowanie umożliwi realizację zawartych w nim wymogów. W świetle zasady rozliczalności przygotowanie dokumentacji ochrony danych osobowych nie jest zatem celem samym w sobie. Stanowi metodę realizacji wskazanych we wspomnianym przepisie obowiązków – zapewnienia, by przetwarzanie odbywało się zgodnie z przepisami, i wymogu, by być w stanie to wykazać.

Z powyższego wynika, że do dokumentacji ochrony danych osobowych należy podchodzić funkcjonalnie. Nie ma znaczenia forma i struktura prowadzonej dokumentacji, czyli nazwy poszczególnych dokumentów oraz podział materii między nimi. W tym zakresie administratorzy i podmioty przetwarzające dysponują daleko idącą swobodą. Ważne, by zrealizować cele wskazane w RODO – zagwarantować, że przetwarzanie będzie odbywało się zgodnie z rozporządzeniem, oraz zapewnić, że będzie się umiało to wykazać.

Cel powyższy rozpada się na liczne bardziej konkretne wymagania zawarte w znacznie szczegółowszych przepisach RODO. Przepisy te stają się w ten sposób bardziej precyzyjnymi podstawami opracowania dokumentacji niż zasada rozliczalności. Prezes Urzędu

<sup>9</sup> Szerzej: P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022, s. 167–168; RODO. *Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D. Lubasz, s. 342–343.

<sup>10</sup> Por. też P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych*, Warszawa 2018, s. 268.

Prezentowana książka zawiera liczne przykłady, które pomogą czytelnikowi w zrozumieniu wymagań w zakresie dokumentacji ochrony danych osobowych, oraz praktyczne wskazówki ułatwiające ich realizację. W publikacji zamieszczono także wzory oraz instrukcje krok po kroku wyjaśniające, w jaki sposób wypełnić dany wzór i dostosować go do własnych potrzeb.

Nowe wydanie poszerzono o szczegółowe omówienie m.in. następujących zagadnień:

- dokumentacja serwisu internetowego,
- prawne i etyczne kwestie, które powinny być uwzględnione w przypadku zastosowania rozwiązań informatycznych z zastosowaniem sztucznej inteligencji,
- współadministrowanie danymi osobowymi oraz status współadministratorów,
- nowe tabele audytów,
- nowe szablony w zakresie oceny ryzyka, w szczególności wykaz aktywów wspomagających czy klasyfikację informacji,
- nowy wykaz rodzajów operacji wymagających przeprowadzenia oceny skutków dla ochrony danych,
- nowe wskazówki praktyczne w zakresie dokumentacji pracowniczej (w tym wzory dotyczące innego niż wizyjny monitoringu pracowniczego oraz ankiety kontrolnej).

„Nowe wydanie liczy o 218 stron tekstu więcej niż wydanie pierwsze. Śmiało można powiedzieć, że przedstawiana Czytelnikom publikacja stanowi nowe opracowanie problematyki dokumentacji ochrony danych osobowych”.

*Z przedmowy do drugiego wydania*

Książka jest przeznaczona dla adwokatów, radców prawnych, pracowników administracji rządowej i samorządowej, działów kadr, zasobów ludzkich, IT, sprzedaży, marketingu i PR, menedżerów, przedsiębiorców, inspektorów ochrony danych osobowych i innych osób, które realizują obowiązki z tej dziedziny. Będzie cennym źródłem wiedzy dla przedstawicieli nauki oraz studentów prawa, administracji, zarządzania i przedsiębiorczości.

Wzory dostępne w wersji elektronicznej do pobrania ze strony [www.dokumentacja-ochrony-danych-osobowych.wolterskluwer.pl](http://www.dokumentacja-ochrony-danych-osobowych.wolterskluwer.pl) po wpisaniu zamieszczonego w książce kodu aktywacyjnego. Wzory można modyfikować i dostosowywać do indywidualnych potrzeb.

**Mariusz Jagielski** – doktor habilitowany nauk prawnych, profesor Uniwersytetu Śląskiego w Katowicach; od 1994 r. pracownik naukowo-dydaktyczny, a w latach 2011–2016 prodziekan Wydziału Prawa i Administracji UŚ; od 2018 r. pełnomocnik rektora UŚ ds. ochrony danych osobowych; prowadzi uniwersyteckie zajęcia z przedmiotów: ochrona danych osobowych, GDPR in business i dokumentacja ochrony danych osobowych oraz szkolenia z tego zakresu dla kadry zarządzającej i pracowników przedsiębiorstw, a także organów administracji rządowej i samorządowej; autor wielu opracowań naukowych we wskazanych dziedzinach.



9788382863826 w02P01

ISBN 978-83-8286-382-6



9 788382 863826

**ZAMÓWIENIA:**

INFOLINIA 801 04 45 45

ZAMOWIENIA@WOLTERSKLUWER.PL

WWW.PROFINFO.PL

Kup e-book i czytaj  
w aplikacji Smarteca



CENA 99 ZŁ (W TYM 5% VAT)