

OCHRONA DANYCH OSOBOWYCH

Poradnik praktyczny

redakcja Dominik Lubasz, Adam Szkurłat

Witold Chomiczewski, Aneta Frydrych-Romańska
Wojciech Grenda, Dominik Lubasz, Joanna Łuczak-Tarka
Anna Maciaszczyk, Kinga Majczak-Górecka, Karolina Przybysz
Adam Szkurłat, Julia Wawrzyńczak, Paulina Wirska

 **lubasz&wspólnicy**
KANCELARIA RADCÓW PRAWNYCH

 Wolters Kluwer

 **GDPR
RISK TRACKER**
by lubasz&wspólnicy

OCHRONA DANYCH OSOBOWYCH

Poradnik praktyczny

redakcja Dominik Lubasz, Adam Szkurłat

Witold Chomiczewski, Aneta Frydrych-Romańska
Wojciech Grenda, Dominik Lubasz, Joanna Łuczak-Tarka
Anna Maciaszczyk, Kinga Majczak-Górecka, Karolina Przybysz
Adam Szkurłat, Julia Wawrzyńczak, Paulina Wirska

Zamów książkę w księgarni internetowej

profinfo.pl
księgarnia internetowa

Stan prawny na 25 maja 2023 r.

Wydawczyni
Monika Pawłowska

Redaktor prowadząca
Katarzyna Gierłowska

Opracowanie redakcyjne
Agnieszka Witczak

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

prawolubni

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegał przystępujących 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.

Szanujmy prawo i własność
Więcej na www.legalnakultura.pl
Polska Izba Książki

© Copyright by Wolters Kluwer Polska Sp. z o.o., 2023

ISBN 978-83-8328-713-3

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

SPIS TREŚCI

Słowo wstępne	17
Wykaz skrótów	19

CZĘŚĆ OGÓLNA

Rozdział I

Regulacje prawne ochrony danych osobowych

– <i>Dominik Lubasz, Adam Szkurlat</i>	25
1. Wprowadzenie	25
2. Rola rozporządzenia 2016/679	26
3. Cele reformy prawa ochrony danych osobowych	28
4. Zakres zastosowania RODO	29
5. Relacja RODO do polskich regulacji	30

Rozdział II

Podstawowe pojęcia i role w procesie przetwarzania

danych osobowych – <i>Anna Maciaszczyk</i>	34
1. Wprowadzenie	34
2. Dane osobowe	34
3. Dane szczególnych kategorii	40
4. Przetwarzanie	41
5. Profilowanie „zwykłe” i profilowanie kwalifikowane	43
6. Zgoda	47
7. Administrator	48
8. Podmiot przetwarzający	50

Rozdział III**Zasady przetwarzania danych osobowych**

– <i>Anna Maciaszczyk</i>	52
1. Wprowadzenie	52
2. Zasada zgodności z prawem i rzetelności	53
3. Zasada przejrzystości	56
4. Zasada ograniczenia celu	58
5. Zasada minimalizacji danych	61
6. Zasada prawidłowości	63
7. Zasada ograniczenia przechowywania	64
8. Zasada integralności i poufności	66
9. Zasada rozliczalności	70

Rozdział IV**Podstawy prawne przetwarzania – Witold Chomiczewski,**

<i>Dominik Lubasz, Anna Maciaszczyk, Adam Szkurlat</i>	72
1. Wprowadzenie	72
2. Dane osobowe zwykłe	72
3. Dane szczególnych kategorii	74
4. Podstawy prawne przetwarzania danych osobowych zwykłych	77
4.1. Zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a RODO)	77
4.2. Wykonanie umowy lub podjęcie działań przed jej zawarciem (art. 6 ust. 1 lit. b RODO)	81
4.3. Wypełnienie obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO)	82
4.4. Ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d RODO)	84
4.5. Zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 1 lit. e RODO)	85
4.6. Prawnie uzasadniony interes realizowany przez administratora lub stronę trzecią (art. 6 ust. 1 lit. f RODO)	85

Rozdział V**Obowiązki informacyjne i sposób komunikacji**

– <i>Joanna Łuczak-Tarka, Adam Szkurlat</i>	89
1. Wprowadzenie	89
2. Przejrzysta komunikacja	89
3. Typy obowiązków informacyjnych i ich zakresy	91
4. Sposób i termin realizacji obowiązku informacyjnego	94
5. Wyłączenia obowiązku przekazania informacji o przetwarzaniu	99

Rozdział VI**Prawa podmiotów danych i ich realizacja**

– <i>Kinga Majczak-Górecka</i>	101
1. Wprowadzenie	101
2. Prawo dostępu do danych oraz uzyskania informacji o przetwarzaniu (art. 15 RODO)	106
3. Prawo do sprostowania danych (art. 16 RODO)	111
4. Prawo do usunięcia danych (art. 17 RODO)	112
5. Prawo do ograniczenia przetwarzania (art. 18 RODO) ...	119
6. Prawo do przenoszenia danych (art. 20 RODO)	122
7. Prawo do sprzeciwu (art. 21 RODO)	125
8. Prawo do niepodlegania zautomatyzowanym decyzjom (art. 22 RODO)	129
9. Prawo do wniesienia skargi do organu nadzorczego	133
10. Brak realizacji żądania podmiotu danych	135
11. Obowiązek powiadomienia o sprostowaniu, usunięciu lub ograniczeniu przetwarzania	136

Rozdział VII**Analiza ryzyka jako podstawa do realizacji obowiązków**

administratora – <i>Dominik Lubasz</i>	138
1. Wprowadzenie	138
2. Analiza ryzyka	140
3. Mapowanie czynności przetwarzania danych osobowych ...	146
4. Przykłady rejestrów	146
5. Obowiązek zapewnienia zgodności	150
6. Bezpieczeństwo przetwarzania danych osobowych	153

Rozdział VIII

Praktyczne i narzędziowe aspekty analizy ryzyka

– Wojciech Grenda	158
1. Wprowadzenie	158
2. Etapy analizy	159
3. Mapowanie zagrożeń	161
4. Zabezpieczenia	162
5. Waga danych	163
6. Skutek	163
7. Podsumowanie	164

Rozdział IX

Data protection by design i data protection by default

– Adam Szkurlat	167
1. Wprowadzenie	167
2. Istota data protection by design	167
3. Idea data protection by default	170
4. Czynniki determinujące skuteczne wdrożenie data protection by default i data protection by design	171
5. Certyfikacja na gruncie art. 25 ust. 3 RODO	176

Rozdział X

Naruszenie ochrony danych osobowych

– Witold Chomiczewski, Kinga Majczak-Górecka, Adam Szkurlat	177
1. Wprowadzenie	177
2. Ocena naruszenia	181
3. Mechanizm Grupy Roboczej Art. 29	183
4. Wzór Bernoulliego	184
5. Algorytm ENISA	185
6. Zgłoszenie naruszenia organowi nadzorcemu	188
7. Elementy zgłoszenia	190
8. Zawiadamianie o naruszeniu osoby, której dane dotyczą	191
9. Dokumentowanie naruszeń	199

Rozdział XI**Powierzenie przetwarzania danych osobowych**

– <i>Anna Maciaszyk</i>	203
1. Wprowadzenie	203
2. Prawa i obowiązki administratora i podmiotu przetwarzającego w ramach powierzenia przetwarzania danych osobowych	206
3. Wybór podmiotu przetwarzającego	208
4. Umowa powierzenia przetwarzania danych osobowych ...	211
4.1. Forma umowy	211
4.2. Treść umowy	212
4.3. Standardowe klauzule umowne	215
5. Podwykonawcy przetwarzania	216
6. Decyzje Prezesa UODO dotyczące procesu powierzenia przetwarzania danych osobowych	218

Rozdział XII**Współadministrowanie – *Adam Szkurlat*** 220

1. Wprowadzenie	220
2. Istota współadministrowania	220
3. Zakres uzgodnień	223

Rozdział XIII**Obowiązki dokumentacyjne – *Adam Szkurlat*** 225

1. Wprowadzenie	225
2. Polityki ochrony danych	227
3. Rejestry dotyczące przetwarzania	230
4. Rejestr czynności przetwarzania	230
5. Rejestr kategorii czynności przetwarzania	232

Rozdział XIV**Rejestr czynności przetwarzania – *Joanna Łuczak-Tarka*** 234

1. Wprowadzenie	234
2. Zakres podmiotowy obowiązku prowadzenia rejestru ...	235
3. Zakres przedmiotowy rejestru i jego forma	239
4. Dostęp do rejestru	243

Rozdział XV**Dopuszczenie do przetwarzania danych osobowych**

– <i>Dominik Lubasz, Adam Szkurłat</i>	247
1. Wprowadzenie	247
2. Polecenie administratora	248
3. Indywidualne upoważnienie	251
4. Zakres uprawnień i okres ważności	253
5. Szkolenia personelu	254

Rozdział XVI**Ocena skutków dla ochrony danych – *Dominik Lubasz,***

<i>Julia Wawrzyńczak</i>	255
1. Wprowadzenie	255
2. Konsultacje z inspektorem ochrony danych	257
3. Przesłanki obligatoryjnej oceny skutków dla ochrony danych	257
4. Wykaz rodzajów operacji podlegających i niepodlegających DPIA	261
5. Zakres i etapy DPIA	262
6. Kodeksy postępowania	267
7. Konsultacje – opinia podmiotów danych	267
8. Przegląd operacji przetwarzania oraz dokonanej oceny skutków dla ochrony danych	268

Rozdział XVII**Inspektor ochrony danych – *Adam Szkurłat***

1. Wprowadzenie	269
2. Obligatoryjne powołanie inspektora ochrony danych	270
3. Zawiadomienie organu nadzorczego o powołaniu inspektora ochrony danych	273
4. Status inspektora ochrony danych w organizacji	274
5. Kwalifikacje i zasoby inspektora ochrony danych	278
6. Zadania inspektora ochrony danych	280
7. Konflikt interesów	280

Rozdział XVIII**Transfery danych osobowych – Adam Szkuřat,**

<i>Paulina Wirska</i>	283
1. Definicja transferu danych osobowych	283
2. Regulacje prawne dotyczące zagadnień transferowych ...	284
3. Przekazywanie danych na podstawie decyzji Komisji Europejskiej w sprawie odpowiedniego poziomu ochrony danych osobowych	285
4. Przekazywanie danych z zastrzeżeniem odpowiednich zabezpieczeń	286
5. Wyjątki w szczególnych sytuacjach	288
6. Transfer zwrotny	289
7. Dalszy transfer	290
8. Transfer danych osobowych do Wielkiej Brytanii	291
9. Transfer danych osobowych do Stanów Zjednoczonych ...	293
10. Dostęp do danych spoza Europejskiego Obszaru Gospodarczego	296
11. Stanowiska organów odnoszące się do zagadnień transferowych	297

Rozdział XIX

Organ nadzorczy – Adam Szkuřat	300
1. Wprowadzenie	300
2. Procedura powołania organu nadzorczego	302
3. Kompetencje i uprawnienia organu nadzorczego	304

ZAGADNIENIA SZCZEGÓŁOWE**Rozdział XX****Przetwarzanie danych osobowych przez pracodawców**

– <i>Adam Szkuřat</i>	311
1. Wprowadzenie	311
2. Przetwarzanie danych osobowych w procesie rekrutacji ...	312
3. Przetwarzanie danych osobowych w związku z zatrudnieniem	314
4. Monitoring	318

Rozdział XXI**Kontrola trzeźwości pracownika a ochrona danych**

osobowych – <i>Joanna Łuczak-Tarka</i>	324
1. Wprowadzenie	324
2. Cel, podstawa prawna i zakres przetwarzanych danych ...	326
3. Retencja danych gromadzonych w wyniku kontroli	329
4. Prowadzenie działań kontrolnych wobec osób innych niż pracownicy i przetwarzanie danych tych osób	330

Rozdział XXII**Praca zdalna z perspektywy ochrony danych osobowych –**

<i>Joanna Łuczak-Tarka</i>	332
1. Wprowadzenie	332
2. Wprowadzenie pracy zdalnej	334
3. Procedury ochrony danych osobowych a praca zdalna	337
4. Kontrola przestrzegania wymogów w zakresie procedur ochrony danych osobowych	343

Rozdział XXIII**Przetwarzanie danych osobowych na potrzeby marketingu**

bezpośredniego – <i>Adam Szkurłat</i>	347
1. Wprowadzenie	347
2. Szczególne regulacje prawa polskiego	349
3. Regulacja ustawy o świadczeniu usług drogą elektroniczną	350
4. Regulacja Prawa telekomunikacyjnego	351

Rozdział XXIV**Profilowanie i automatyczne podejmowanie decyzji**

– <i>Witold Chomiczewski</i>	355
1. Wprowadzenie	355
2. Istota przepisu art. 22 RODO	356
3. Ograniczenia w zakresie zastosowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu	357
4. Dodatkowe środki ochrony	359
5. Zautomatyzowane przetwarzanie	359
6. Charakter decyzji	360

7. Wyjątki od zakazu podejmowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu 362

Rozdział XXV

RODO a ustawa o świadczeniu usług drogą elektroniczną

i Prawo telekomunikacyjne – Anna Maciaszczyk 364

1. Wprowadzenie 364
2. Relacje pomiędzy dyrektywą o prywatności i łączności elektronicznej a RODO 365
3. Ustawa o świadczeniu usług drogą elektroniczną 368
4. Prawo telekomunikacyjne 370
 - 4.1. Przetwarzanie danych osobowych użytkowników wchodzących w zakres tajemnicy komunikacyjnej oraz innych danych osobowych 370
 - 4.2. Marketing bezpośredni i przesyłanie niezamówionej informacji handlowej 371
 - 4.3. Pliki *cookies* 374
5. Aktualne problemy związane z ochroną prywatności w łączności elektronicznej 377
6. Rozporządzenie *ePrivacy* 378

Rozdział XXVI

Administracyjne kary pieniężne – Adam Szkurlat 380

1. Wprowadzenie 380
2. Administracyjna kara pieniężna 381
3. Podstawy decyzji 384
4. Wysokość sankcji 387
5. Zasady dla sektora publicznego 391

Rozdział XXVII

Odpowiedzialność cywilna za naruszenie przepisów

o ochronie danych osobowych – Aneta Frydrych-Romańska 393

1. Wprowadzenie 393
2. Roszczenia wynikające z art. 82 RODO 394
3. Przesłanki odpowiedzialności 394
4. Podmioty odpowiedzialne 396
5. Roszczenia z tytułu ochrony dóbr osobistych 397

6. Zasady dochodzenia roszczeń w postępowaniu sądowym	400
7. Właściwość sądu	400
8. Wymiana informacji pomiędzy sądem a organem nadzorczym	401
9. Zawieszenie postępowania sądowego	403
10. Umorzenie postępowania sądowego	404

Rozdział XXVIII

Odpowiedzialność karna w świetle ustawy o ochronie

danych osobowych – <i>Aneta Frydrych-Romańska</i>	405
1. Wprowadzenie	405
2. Odpowiedzialność karnoprawna przewidziana w art. 107 u.o.d.o.	407
2.1. Bezprawne przetwarzanie danych osobowych	407
2.2. Niedopuszczalność przetwarzania danych	408
2.3. Przetwarzanie danych przez podmiot nieuprawniony	409
2.4. Wymiar odpowiedzialności	409
3. Przesłstwo udaremniania lub utrudniania kontroli przestrzegania przepisów o ochronie danych osobowych ...	411
4. Przesłstwo naruszenia obowiązku dostarczenia organowi nadzorczemu informacji niezbędnych do ustalenia podstawy wymiaru administracyjnej kary pieniężnej lub dostarczenia danych uniemożliwiających ustalenie podstawy jej wymiaru	413

Rozdział XXIX

Warunki i tryb certyfikacji w świetle ustawy o ochronie

danych osobowych – <i>Karolina Przybysz</i>	415
1. Wprowadzenie	415
2. Pojęcie certyfikacji na gruncie przepisów RODO	416
3. Korzyści płynące z poddania się certyfikacji	420
4. Podmiot certyfikujący	423
5. Warunki i tryb udzielania akredytacji podmiotowi certyfikującemu w świetle ustawy o ochronie danych osobowych	426

6. Warunki i tryb dokonywania certyfikacji w świetle ustawy o ochronie danych osobowych 433

Rozdział XXX

Kodeksy postępowania – Karolina Przybysz 442

1. Wprowadzenie 442
2. Pojęcie kodeksu postępowania na gruncie przepisów RODO 443
3. Cel stosowania kodeksów i płynące z tego korzyści 445
4. Procedura zatwierdzania kodeksu postępowania i akredytacji na gruncie RODO 448
 - 4.1. Podmioty uczestniczące w tworzeniu i stosowaniu kodeksów postępowania 448
 - 4.2. Zakres przedmiotowy kodeksów postępowania 450
 - 4.3. Procedura zatwierdzenia kodeksu postępowania 452
 - 4.4. Monitorowanie zatwierdzonych kodeksów postępowania 454
5. Procedura zatwierdzenia kodeksu postępowania i akredytacji na gruncie ustawy o ochronie danych osobowych 457
6. Kodeksy postępowania w Polsce 461

Rozdział XXXI

Wyjątek dziennikarski – Paulina Wirska 464

1. Wprowadzenie 464
2. Przetwarzanie danych osobowych przez sztuczną inteligencję przy współtworzeniu tekstów dziennikarskich 465
3. Istota wyjątku dziennikarskiego 467
4. Prawa podstawowe w kontekście działalności dziennikarskiej i medialnej w prawie unijnym 468
5. Wybrane orzecznictwo Trybunału Sprawiedliwości oraz Europejskiego Trybunału Praw Człowieka dotyczące ograniczania wolności słowa i wolności mediów 470
6. Rola kodeksów dziennikarskich oraz samoregulacji mediów jako narzędzi ochrony praw i wolności 471
7. „Prawo do bycia zapomnianym” oraz wpływ technologii na prywatność i ochronę danych osobowych 472

8. Równowaga praw i wolności w kontekście działalności dziennikarskiej i medialnej: wolność słowa, wolność mediów oraz prawo do prywatności i ochrony danych osobowych	475
9. Wyjątek dziennikarski w kontekście ochrony danych osobowych	478
10. Wyjątek dziennikarski w Polsce	479
11. Podsumowanie	488
Bibliografia	491
Spis rysunków, tabel i wykresów	499
Autorzy	501

SŁOWO WSTĘPNE

W dniu 25.05.2023 r. minęło pięć lat od momentu, w którym rozpoczęliśmy stosowanie przepisów ogólnego rozporządzenia o ochronie danych. Choć sam akt prawny został uchwalony ponad dwa lata wcześniej, a europejski prawodawca przewidział stosownie długi okres na dostosowanie czynności przetwarzania do nowych przepisów, to wdrożenie regulacji rozporządzenia 2016/679 rodziło i rodzi nadal wiele wątpliwości i kontrowersji. Perspektywa pięciu lat stosowania nowych przepisów pozwala jednak bliżej przyjrzeć się wykładni, określić tendencje orzecznicze, zweryfikować skuteczność wytycznych oraz innych form *soft law* w obszarze ochrony danych osobowych, a także przeanalizować stosowane w tej dziedzinie praktyki. Zbliżający się w przyszłym roku komisyjny przegląd regulacji RODO determinuje także krytyczne spojrzenie na regulacje oraz próbę wskazania mankamentów, których usunięcie konieczne byłoby w przyszłości.

Warto podkreślić, że przepisy normujące zagadnienia ochrony danych osobowych to nie tylko RODO, ale również krajowe przepisy sektorowe czy unijne punktowe regulacje związane z różnymi aspektami przetwarzania danych osobowych. O ile rozporządzenie 2016/679 nie zmieniło się od momentu uchwalenia przepisów, o tyle w polskim porządku prawnym wprowadzono szereg nowych przepisów oddziałujących znacząco na zagadnienia związane z ochroną danych osób fizycznych. Nowe przepisy regulują praktyczne i kluczowe z perspektywy wielu administratorów kwestie, między innymi profilowanie, pracę zdalną czy badanie trzeźwości.

Wreszcie czynnikiem wpływającym na wzrost znaczenia zagadnień związanych z ochroną danych osobowych była pandemia COVID-19. Gwałtowna cyfryzacja, zamiana modelu pracy, w szczególności przejście do modelu pracy zdalnej, ujawniły, jak istotne są odpowiedni dobór narzędzi, zaadresowanie nowych wyzwań, zagrożeń i podatności oraz wdrożenie adekwatnych środków technicznych i organizacyjnych.

Wszystkie te aspekty zainspirowały zespół Autorów do opracowania niniejszej publikacji. W jej ramach podjęliśmy próbę zaprezentowania przepisów o ochronie danych osobowych z uwzględnieniem praktycznych aspektów ich stosowania. Publikacja została podzielona na dwie części – poświęconą zagadnieniom ogólnym oraz szczególnym problemom i obszarom przetwarzania danych osobowych. W każdej z części przybliżyliśmy syntetycznie zapatrywania doktryny oraz poglądy prezentowane w orzecznictwie, wzbogacając je o liczne przykłady i podkreślając najistotniejsze wnioski.

Każdy z Autorów jest członkiem zespołu *Privacy & Data Protection* w kancelarii Lubasz i Wspólnicy, zaś sama publikacja stanowi efekt doświadczeń zgromadzonych przez Autorów, którzy na co dzień zajmują się praktycznym wdrażaniem przepisów o ochronie danych osobowych. Liczne wyróżnienia w branżowych rankingach, dorobek naukowy i publikacyjny oraz słowa uznania od Klientów pozwalają nam wierzyć, że wiedza, jaką dzielimy się w tej książce, będzie cenna i przydatna dla każdego z Czytelników.

*Dominik Lubasz
Adam Szkuřat*

Łódź, czerwiec 2023 r.

Rozdział I

REGULACJE PRAWNE OCHRONY DANYCH OSOBOWYCH

1. Wprowadzenie

Z perspektywy osób zajmujących się ochroną danych osobowych, ale przede wszystkim z punktu widzenia administratorów, data 25.05.2018 r. jest kluczowa dla ustalenia, jakie przepisy, a w ślad za tym – jakie obowiązki i zadania, znajdą zastosowanie w istniejących i planowanych procesach przetwarzania danych osobowych. Z tym dniem rozpoczęto – po dwuletnim okresie przygotowawczym – stosowanie przepisów rozporządzenia 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)¹. Ogólna dyrektywa sformułowana w motywie 171 RODO przewiduje, że przetwarzanie, które w dniu wejścia w życie rozporządzenia, tj. dnia 24.05.2016 r., już się toczy, powinno w terminie dwóch lat od wejścia rozporządzenia w życie zostać dostosowane do jego przepisów.

¹ Dz.Urz. UE L 119, s. 1, ze zm.

2. Rola rozporządzenia 2016/679

Ogólne rozporządzenie o ochronie danych zastąpiło obowiązującą wcześniej dyrektywę 95/46/WE, a w konsekwencji również ustawę o ochronie danych osobowych z 1997 r., wprowadzając odmienny, proaktywny model ochrony, **oparty na podejściu bazującym na ryzyku** (*risk-based approach*). W ramach reformy prawa ochrony danych osobowych prawodawca odszedł od sztywnych ram regulacyjnych i precyzyjnego wskazania obowiązków, jakim powinien sprostać administrator. Były one charakterystyczne dla polskiej ustawy o ochronie danych osobowych z 1997 r. oraz rozporządzeń wykonawczych do niej, w tym zwłaszcza dla rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych².

Podejście oparte na ryzyku jest kluczowe dla odczytania, zrozumienia i zrealizowania obowiązków administratora i podmiotu przetwarzającego nałożonych na nich mocą przepisów rozporządzenia 2016/679. Stało się ono istotnym elementem wielu obowiązków, w tym:

- ogólnego obowiązku zapewnienia zgodności z rozporządzeniem 2016/679, o którym mowa w jego art. 24;
- uwzględniania ochrony danych już w fazie projektowania (*data protection by design*) w myśl art. 25 ust. 1 oraz realizacji zasady domyślnej ochrony danych (*data protection by default*) zgodnie z art. 25 ust. 2;
- sporządzania określonej przepisami dokumentacji przetwarzania ujętej w ramy art. 30;
- zapewnienia bezpieczeństwa przetwarzania, w szczególności wskazanego w art. 32;
- oceny skutków przetwarzania dla ochrony danych (*data protection impact assessment*) oraz uprzednich konsultacji z organem nadzoru, o których mowa odpowiednio w art. 35 i 36.

² Dz.U. Nr 100, poz. 1024.

Jako podstawa przyjętej konstrukcji obowiązków wskazany mechanizm jest realizowany przez analizę ryzyka, dla której jednak brak szczegółowej regulacji w rozporządzeniu 2016/679. Decyzja w kwestii przyjmowanej metodyki, sposobu podejścia, użytych narzędzi analitycznych, jak również samego zakresu analizy została pozostawiona w rękach administratora.

Rysunek 1. Cechy regulacji zawartych w RODO



Źródło: opracowanie własne.

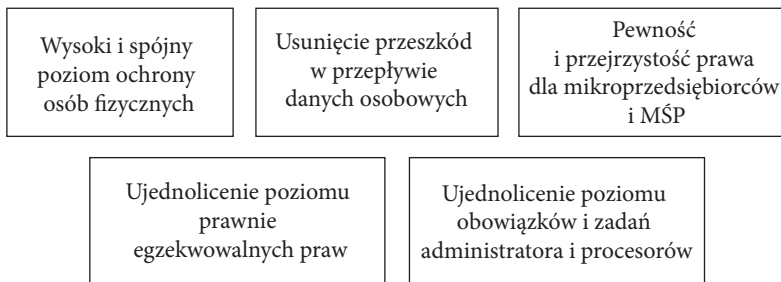
Opisane podejście jest związane ze zdiagnozowaną potrzebą unowocześnienia regulacji ochrony danych osobowych w Unii Europejskiej, zapewnienia jej neutralności technologicznej, zniwelowania negatywnych aspektów dotychczasowego wyboru środka legislacyjnego w postaci dyrektywy o minimalnym charakterze, a wreszcie – z dostrzeżeniem wartości danych osobowych w gospodarce (*data driven economy*) i wpływu wykorzystania danych, w szczególności w ujęciu transgranicznym, na budowanie jednolitego rynku cyfrowego w Unii Europejskiej.

3. Cele reformy prawa ochrony danych osobowych

W związku z tym sformułowano **podstawowe cele**, jakie przyświecają omawianej reformie. Z jednej strony jest to **wysoki poziom ochrony praw osób fizycznych**, z drugiej jednak – poszerzenie możliwości biznesowych poprzez **ułatwienie swobodnego przepływu danych osobowych na jednolitym rynku cyfrowym**.

W założeniach nowa regulacja – między innymi poprzez technologiczną neutralność – pozostawia administratorom swobodę co do wyboru metod i środków, z wykorzystaniem których będą realizować cele i zadania związane z bezpieczeństwem informacji, co stało się ostatecznie jednym z najbardziej charakterystycznych elementów tej regulacji. Zmieniono w związku z tym stosowane rozwiązania tak, by uelastyczyć podejście i zróżnicować nakładane obowiązki zależnie od warunków przetwarzania danych, podmiotów przetwarzających i skali. Miało to być także odpowiedzią na sytuację prawną oraz oczekiwania małych i średnich przedsiębiorców.

Rysunek 2. Podstawowe cele związane ze stosowaniem RODO



Źródło: opracowanie własne.

4. Zakres zastosowania RODO

Przepisy art. 2 i 3 RODO odpowiednio wyznaczają zakres przedmiotowy i zakres terytorialny zastosowania rozporządzenia.

W myśl art. 2 RODO obejmuje ono swoim zakresem zastosowania wszelkiego rodzaju przetwarzanie danych osobowych stanowiących lub mających stanowić część zbioru danych, przetwarzanych w sposób całkowicie lub tylko częściowo zautomatyzowany, a także w sposób ogólnie niezautomatyzowany. W konsekwencji regulacja ta znajduje zastosowanie do większości form przetwarzania. Równocześnie podlega ona jednak pewnym ograniczeniom poprzez sformułowane w art. 2 ust. 2 wyjątki.

Wyłączenia zastosowania rozporządzenia 2016/679 obejmują:

- 1) przetwarzanie w ramach działalności nieobjętej zakresem prawa Unii;
- 2) przetwarzanie przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;
- 3) przetwarzanie przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;
- 4) przetwarzanie przez właściwe organy 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.

Zakres terytorialny zastosowania rozporządzenia 2016/679 wyznaczony jest z kolei, zgodnie z art. 3 RODO, przez związek przetwarzania danych osobowych z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii Europejskiej, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

Dostrzegając słabości regulacji dyrektywy 95/46/WE, prawodawca unijny w art. 3 ust. 2 RODO rozszerzył zastosowanie rozporządzenia

Publikacja jest kompleksowym opracowaniem praktycznych aspektów obowiązywania przepisów o ochronie danych osobowych, w tym w szczególności ogólnego rozporządzenia o ochronie danych.

Struktura książki została podzielona na zagadnienia ogólne, odpowiadające zasadniczym kwestiom unormowanym w przepisach RODO, oraz zagadnienia szczegółowe, obejmujące wybrane obszary działalności administratora, mające swoje specyficzne regulacje na styku RODO i krajowych aktów prawnych.

Walorem publikacji jest jej praktyczny charakter i odniesienie do najbardziej aktualnych poglądów, wytycznych i tendencji orzeczniczych. Książka uwzględni zarówno bieżące orzecznictwo sądów administracyjnych i TSUE, jak i aktualną linię orzeczniczą prezentowaną przez Prezesa UODO. Autorzy – zespół Privacy & Data Protection Lubasz i Wspólnicy – Kancelarii Radców Prawnych sp.k. – podjęli się także analizy najnowszych wytycznych i opinii europejskich organów ochrony danych osobowych, takich jak Europejska Rada Ochrony Danych czy Europejski Inspektor Ochrony Danych.

Książka przeznaczona jest dla praktyków – adwokatów, radców prawnych i sędziów, jak również inspektorów ochrony danych, koordynatorów ochrony danych osobowych, osób odpowiedzialnych w organizacjach za ochronę danych osobowych. Zainteresuje też pracowników działów HR, m.in. w związku z rekrutacją, zatrudnieniem, przetwarzaniem danych w ramach pracy zdalnej oraz badaniem trzeźwości, a także osoby odpowiedzialne w organizacji lub nadzorujące zagadnienia *compliance* oraz ochronę danych osobowych, pracowników działów sprzedaży, marketingu i PR.

Dominik Lubasz – doktor nauk prawnych; radca prawny; partner zarządzający w Lubasz i Wspólnicy – Kancelarii Radców Prawnych sp.k.; ekspert Europejskiej Rady Ochrony Danych; ekspert w zakresie sztucznej inteligencji w Artificial Intelligence (AI) and Privacy Ad Hoc Working Group w EADPP; wiceprzewodniczący grupy ds. etyki i prawa – Grupy Roboczej ds. Sztucznej Inteligencji; autor wielu publikacji z zakresu ochrony danych osobowych oraz handlu elektronicznego.

Adam Szkurłat – adwokat; senior associate w Lubasz i Wspólnicy – Kancelarii Radców Prawnych sp.k.; wykładowca w Uczelni Łazarskiego oraz Polskiej Akademii Nauk; w 2023 r. wyróżniony przez ranking The Legal 500 jako Recommended Lawyer w kategorii „ochrona danych osobowych i prywatności”; autor kilkudziesięciu publikacji z zakresu ochrony danych osobowych, prawa cywilnego i prawa nowoczesnych technologii.



9 788383 287133 W01P01

ISBN 978-83-8328-713-3



9 788383 287133

ZAMÓWIENIA:

INFOLINIA: 801 04 45 45

ZAMOWIENIA@WOLTERSKLUPER.PL

WWW.PROFINFO.PL

Kup e-book i czytaj
w aplikacji Smarteca



CENA 179 ZŁ (W TYM 5% VAT)