

DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH ZE WZORAMI

redakcja Mariusz Jagielski

Artur Cieřlik, Paweł Fajgielski, Mariusz Jagielski
Damian Karwała, Paulina Komorowska, Dominik Lubasz
Marta Otto, Katarzyna Palka-Bartoszek
Marlena Sakowska-Baryła, Paweł Tobiczuk

PRAWO W PRAKTYCE

DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH ZE WZORAMI

redakcja Mariusz Jagielski

Artur Cieślik, Paweł Fajgielski, Mariusz Jagielski
Damian Karwala, Paulina Komorowska, Dominik Lubasz
Marta Otto, Katarzyna Palka-Bartoszek
Marlena Sakowska-Baryła, Paweł Tobiczuk

PRAWO W PRAKTYCE

Zamów książkę w księgarni internetowej

proinfo.pl
księgarnia internetowa

Stan prawny na 1 lutego 2019 r.

Recenzent
dr Andrzej Krasuski

Wydawca
Monika Pawłowska

Redaktor prowadzący
Joanna Tchorek

Opracowanie redakcyjne i łamanie
Violet Design Wioletta Kowalska

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

Poszczególne rozdziały opracowali:

Artur Cieślik – rozdz. 3
Paweł Fajgielski – rozdz. 6
Mariusz Jagielski – rozdz. 1
Damian Karwala – rozdz. 10
Paulina Komorowska – rozdz. 4
Dominik Lubasz – rozdz. 8
Marta Otto – rozdz. 9
Katarzyna Palka-Bartoszek – rozdz. 5
Marlena Sakowska-Baryła – rozdz. 7
Paweł Tobiczuk – rozdz. 2

© Copyright by
Wolters Kluwer Polska Sp. z o.o., 2019

ISBN 978-83-8160-387-4

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

www.wolterskluger.pl
księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW	11
---------------------	----

ROZDZIAŁ 1

DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH ZGODNA Z RODO	13
1.1. Wprowadzenie	13
1.2. Podstawy prawne i zasady prowadzenia dokumentacji ochrony danych osobowych	14
1.3. Podmioty zobowiązane do opracowania dokumentacji ochrony danych osobowych	18
1.4. Zakres przedmiotowy dokumentacji ochrony danych osobowych	22
Literatura	24

ROZDZIAŁ 2

POLITYKA OCHRONY DANYCH OSOBOWYCH	25
2.1. Wprowadzenie	25
2.2. Struktura polityki	26
2.3. Zakres przedmiotowy polityki	27
2.4. Możliwe rozszerzenie treści polityki	32
2.5. Polityka w świetle dotychczasowej dokumentacji	32
2.6. Wzory	34
2.7. Instrukcja korzystania ze wzorów	55
Literatura	59

ROZDZIAŁ 3

OCENA (SZACOWANIE) RYZYKA	61
3.1. Wprowadzenie	61
3.2. Podstawy zarządzania ryzykiem w bezpieczeństwie informacji	64
3.3. Wybieranie zabezpieczeń – dobre praktyki	90
Literatura	93

ROZDZIAŁ 4

OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH	95
4.1. Zastosowanie dokumentu	95
4.2. Kontekst historyczny	96
4.3. Kiedy konieczne jest przeprowadzenie oceny skutków dla ochrony danych	96
4.4. Ocena skutków dla ochrony danych – zasady	102
4.4.1. Minimalne wymogi DPIA	103

4.4.2. Udział osób trzecich w przeprowadzaniu oceny skutków dla ochrony danych	105
4.4.2.1. Eksperti zewnętrzni	105
4.4.2.2. Osoby, których dane dotyczą	106
4.4.2.3. Podmioty przetwarzające działające w imieniu administratora	106
4.5. Ocena skutków dla ochrony danych – wzór	106
4.6. Konsekwencje DPIA. Obowiązek konsultacji z organem nadzorczym – Prezesem Urzędu Ochrony Danych Osobowych	113
4.6.1. Wniosek o uprzednie konsultacje	113
4.6.2. Przebieg i czas trwania konsultacji	114
4.6.3. Rezultat konsultacji	115
Literatura	115

ROZDZIAŁ 5

REJESTR CZYNNOŚCI PRZETWARZANIA I REJESTR KATEGORII

CZYNNOŚCI PRZETWARZANIA	117
5.1. Wstęp	117
5.2. Podstawa prowadzenia rejestrów	118
5.2.1. Przepis art. 30 RODO jako formalnoprawne źródło obowiązku prowadzenia rejestrów	118
5.2.2. Wpływ ustawodawstwa krajowego na wymóg prowadzenia rejestrów wynikający z art. 30 RODO	119
5.2.3. Wyłączenie obowiązku prowadzenia rejestru dla „działalności prasowej”, wypowiedzi w ramach działalności literackiej, wypowiedzi akademickiej	121
5.2.4. Wyłączenie obowiązku prowadzenia rejestrów przez przedsiębiorcę lub podmiot zatrudniający mniej niż 250 osób	123
5.3. Prawne znaczenie rejestrów w polityce ochrony danych osobowych administratora danych osobowych lub podmiotu przetwarzającego	126
5.3.1. Prowadzenie rejestru jako realizacja wymogu przetwarzania danych osobowych zgodnie z RODO	127
5.3.2. Prowadzenie rejestru jako narzędzie wykazania przetwarzania danych osobowych zgodnie z RODO wobec organu nadzoru	127
5.4. Cel realizacji obowiązku prowadzenia rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania	128
5.5. Podmiot zobowiązany do prowadzenia rejestru	131
5.6. Dla kogo dostępne są rejestry?	134
5.7. Skąd czerpać informacje stanowiące treść rejestru?	135
5.8. Obowiązek uaktualniania rejestrów	136
5.9. Rejestr i jego forma	137
5.10. Czynności przetwarzania danych osobowych	139
5.11. Treść rejestru czynności przetwarzania	141
5.11.1. Obligatoryjna treść rejestru czynności przetwarzania; art. 30 ust. 1 RODO	141
5.11.2. Fakultatywne elementy treści rejestru czynności przetwarzania	148
5.12. Kategorie czynności przetwarzania	150
5.13. Elementy treści rejestru kategorii czynności przetwarzania	151
5.13.1. Obligatoryjne elementy treści rejestru kategorii czynności przetwarzania	151
5.13.2. Fakultatywne elementy treści rejestru kategorii czynności przetwarzania	152

5.14. Uwagi dotyczące treści zawartych w przykładowych rejestrach: czynności przetwarzania i kategorii czynności przetwarzania	152
5.15. Wzory	153
Literatura	172

ROZDZIAŁ 6

DOKUMENTACJA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH	175
6.1. Wprowadzenie	175
6.2. Naruszenie ochrony danych – pojęcie, zakres	176
6.3. Obowiązek dokumentowania naruszeń	176
6.4. Rejestr naruszeń – zawartość	179
6.5. Instrukcja wypełnienia rejestru naruszeń ochrony danych osobowych	180
Literatura	183

ROZDZIAŁ 7

DOKUMENTACJA AUDYTÓW WEWNĘTRZNYCH	185
7.1. Wprowadzenie – po co audytować?	185
7.2. Audyt wewnętrzny, sprawdzenie, kontrola	186
7.3. Wobec kogo wykazywać zgodność z RODO	188
7.4. Dokumentacja audytu wewnętrznego	189
7.5. Plan audytów wewnętrznych (sprawdzeń kontroli)	191
7.6. Audyty pozaplanowe	194
7.7. Sposób i zakres dokumentowania audytu	196
7.8. Zagadnienia audytowe	198
7.9. Raport (sprawozdanie) z audytu wewnętrznego	201
Literatura	202

ROZDZIAŁ 8

KLAUZULE WYRAŻENIA ZGÓD I KLAUZULE INFORMACYJNE	203
8.1. Zgoda na przetwarzanie danych osobowych	203
8.1.1. Wprowadzenie	203
8.1.2. Zgoda jako przesłanka legalizacyjna – zagadnienia ogólne	205
8.1.3. Wzory oświadczeń o wyrażeniu zgody	207
8.1.3.1. Wyrażenie zgody w procesie rekrutacyjnym	207
8.1.3.2. Zgoda na działania marketingowe inne niż przesyłanie informacji handlowej drogą elektroniczną oraz inne niż marketing bezpośredni na podstawie Prawa telekomunikacyjnego	208
8.1.3.3. Zgoda na otrzymywanie informacji handlowej drogą elektroniczną	209
8.1.4. Szczegółowe wymogi dotyczące zgody	210
8.1.4.1. Dobrowolność zgody	210
8.1.4.2. Konkretność zgody	212
8.1.4.3. Świadomość zgody	212
8.1.4.4. Jednoznaczność zgody	214
8.1.4.5. Wyraźność zgody	215
8.1.4.6. Forma zgody	216
8.1.4.7. Dodatkowe wymogi dotyczące pisemnej zgody	217

8.1.4.8. Wycofanie zgody	218
8.1.4.9. Ciężar dowodu – rozliczalność	219
8.2. Klauzule informacyjne	220
8.2.1. Wprowadzenie	220
8.2.2. Obowiązki informacyjne – zagadnienia ogólne	221
8.2.3. Wzory klauzul informacyjnych	222
8.2.3.1. Klauzula rekrutacyjna	222
8.2.3.2. Klauzula kontrahencka	226
8.2.3.3. Klauzula kliencka	229
8.2.3.4. Klauzula newsletterowa	231
8.2.4. Szczegółowe wymogi dotyczące realizacji obowiązków informacyjnych	234
8.2.4.1. Typy obowiązków informacyjnych	234
8.2.4.2. Zakres obowiązków informacyjnych	235
8.2.4.3. Sposób realizacji obowiązków informacyjnych	239
8.2.4.4. Termin realizacji obowiązków informacyjnych	241
8.2.4.5. Aktualizacja informacji	242
8.2.4.6. Wyłączenia spod obowiązku realizacji	243
Literatura	246

ROZDZIAŁ 9

PRZETWARZANIE DANYCH OSOBOWYCH W KONTEKŚCIE ZATRUDNIENIA	247
9.1. Upoważnienie do przetwarzania danych osobowych	247
9.1.1. Wprowadzenie	247
9.1.2. Wzór upoważnienia do przetwarzania danych osobowych	251
9.1.3. Praktyczne wskazówki	253
9.2. Ewidencja osób upoważnionych do przetwarzania danych	255
9.2.1. Wprowadzenie	255
9.2.2. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych	256
9.2.3. Praktyczne wskazówki	257
9.3. Umowa powierzenia przetwarzania danych osobowych	258
9.3.1. Wprowadzenie	258
9.3.2. Wzór umowy powierzenia przetwarzania danych osobowych	263
9.3.3. Wskazówki praktyczne	268
9.4. Klauzula informacyjna dotycząca przetwarzania danych osobowych	269
9.4.1. Wprowadzenie	269
9.4.2. Wzór klauzuli informacyjnej dotyczącej przetwarzania danych osobowych	270
9.4.3. Wskazówki praktyczne	273
9.5. Monitoring wizyjny	274
9.5.1. Wprowadzenie	274
9.5.2. Wzór informacji o monitoringu wizyjnym	278
9.5.3. Praktyczne wskazówki	279
9.6. Monitoring poczty elektronicznej pracownika	280
9.6.1. Wprowadzenie	280
9.6.2. Wzór informacji o funkcjonowaniu monitoringu poczty elektronicznej	282
9.6.3. Praktyczne wskazówki	283
Literatura	284

ROZDZIAŁ 10

TRANSFER DANYCH OSOBOWYCH DO PAŃSTW TRZECICH	285
10.1. Wprowadzenie	285
10.2. Podstawy dopuszczalnego transferu danych osobowych oraz kolejność ich stosowania	286
10.3. Kontekst historyczny, najważniejsze zmiany	289
10.4. Umowy transferowe oparte o klauzule modelowe	291
10.5. Zgoda na transfer danych oraz obowiązek informacyjny	293
10.6. Wzory	295
10.7. Instrukcja korzystania ze wzorów	320
Literatura	322
O AUTORACH	325

WYKAZ SKRÓTÓW

Akty prawne

- k.c.** – ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2018 r. poz. 1025 ze zm.)
- Konstytucja RP** – Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)
- k.p.** – ustawa z 26.08.1974 r. – Kodeks pracy (Dz.U. z 2018 r. poz. 917 ze zm.)
- k.p.a.** – ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2018 r. poz. 2096 ze zm.)
- KPP** – Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE 2016 C 202, s. 391)
- k.s.h.** – ustawa z 15.09.2000 r. – Kodeks spółek handlowych (Dz.U. z 2017 r. poz. 1577 ze zm.)
- o.p.** – ustawa z 29.08.1997 r. – Ordynacja podatkowa (Dz.U. z 2018 r. poz. 800 ze zm.)
- pr. pras.** – ustawa z 26.01.1984 r. – Prawo prasowe (Dz.U. z 2018 r. poz. 1914)
- pr. tel.** – ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2018 r. poz. 1954 ze zm.)
- r.d.p.d.o.** – rozporządzenie 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 osobowych (Dz.U. Nr 100, poz. 1024)
- RODO** – 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) (Dz.Urz. UE L 119, s. 1, ze sprost.)
- r.p.k.z.p.** – rozporządzenie Rady Ministrów z 19.12.1992 r. w sprawie pracowniczych kas zapomogowo-pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy (Dz.U. Nr 100, poz. 502)
- r.t.s.r.z.** – rozporządzenie Ministra Administracji i Cyfryzacji z 11.05.2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. poz. 745)
- TFUE** – Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE 2016 C 202, s. 47)
- u.e.r.FUS** – ustawa z 17.12.1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U. z 2018 r. poz. 1270 ze zm.)

u.KRS	– ustawa z 20.08.1997 r. o Krajowym Rejestrze Sądowym (Dz.U. z 2018 r. poz. 986 ze zm.)
u.n.z.a.	– ustawa z 14.07.1983 r. o narodowym zasobie i archiwach (Dz.U. z 2018 r. poz. 217 ze zm.)
u.o.d.o.	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. poz. 1000 ze zm.)
u.o.d.o. z 1997 r.	– ustawa z 27.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.); nie obowiązuje
u.p.d.o.f.	– ustawa z 26.07.1991 r. o podatku dochodowym od osób fizycznych (Dz.U. z 2018 r. poz. 1509 ze zm.)
u.s.u.s.	– ustawa z 13.10.1998 r. o systemie ubezpieczeń społecznych (Dz.U. z 2019 r. poz. 300 ze zm.)
u.z.s.o.	– ustawa z 10.01.2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektroniczną (Dz.U. poz. 357)
u.ZFŚS	– ustawa z 4.03.1994 r. o zakładowym funduszu świadczeń socjalnych (Dz.U. 2018 r. poz. 1316 ze zm.)
u.z.z.	– ustawa z 23.05.1991 r. o związkach zawodowych (Dz.U. z 2019 r. poz. 263 ze zm.)


Urzędy, instytucje, organizacje

GIODO	– Generalny Inspektor Ochrony Danych Osobowych
IOD	– inspektor ochrony danych
KODO	– koordynator ochrony danych osobowych
PUODO	– Prezes Urzędu Ochrony Danych Osobowych
UODO	– Urząd Ochrony Danych Osobowych
ZFŚS	– zakładowy fundusz świadczeń socjalnych
ZUS	– Zakład Ubezpieczeń Społecznych

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, czyli tzw. 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 danych¹. 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 też 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


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

środka 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 technologicznych². 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 RODO³.

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:

² 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.

³ 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 sprawdzeń⁴.

N! Reforma ochrony danych osobowych z 2018 r. doprowadziła do tego, że wszystkie akty normatywne, które wymagały opracowania i wdrożenia powyższych dokumentów, przestały obowiązywać⁵. Zaowocowało to istotnymi zmianami w interesującej nas dziedzinie⁶. 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. Idzie też o to, by ograniczyć przypadki tworzenia dokumentów zbędnych, takich, które w kontekście skali i sposobu przetwarzania danych przez dany podmiot nie są użyteczne.

⁴ Art. 36b u.o.d.o. oraz § 3 ust. 3 i § 5 ust. 2 rozporządzenia Ministra Administracji i Cyfryzacji z 11.05.2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. poz. 745).

⁵ 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.

⁶ 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.

Mariusz Jagielski – doktor habilitowany nauk prawnych, adiunkt w Katedrze Prawa Konstytucyjnego Wydziału Prawa i Administracji Uniwersytetu Śląskiego w Katowicach; od 2018 r. pełnomocnik rektora UŚ ds. ochrony danych osobowych, w latach 2011–2016 prodziekan WPIA UŚ. Zajmuje się ochroną danych osobowych, prawem konstytucyjnym i prawami człowieka. Prowadzi zajęcia z przedmiotów ochrona danych osobowych i dokumentacja ochrony danych osobowych dla studentów oraz szkolenia z tego zakresu dla kadry zarządzającej i pracowników przedsiębiorstw oraz organów administracji rządowej i samorządowej.

Prezentowana książka zawiera liczne przykłady, które pomogą czytelnikowi w zrozumieniu wymagań dotyczących 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.

Zarówno część opisowa, jak i wzory zostały opracowane na podstawie najnowszych przepisów z dziedziny ochrony danych osobowych (nie tylko RODO) i uwzględniają wytyczne i interpretacje ostatnio wydane przez polskie i europejskie organy ochrony danych osobowych.

W opracowaniu omówiono m.in. następujące zagadnienia:

- politykę ochrony danych osobowych,
- ocenę (szacowanie) ryzyka,
- rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania,
- dokumentację naruszeń ochrony danych osobowych,
- dokumentację audytów wewnętrznych,
- wzory zgód i klauzul informacyjnych,
- dokumentację pracowniczą, w tym wzór umowy powierzenia danych,
- obowiązkową dokumentację w przypadku monitoringu.

Książka została napisana przez autorów zajmujących się ochroną danych osobowych, zarówno naukowo, jak i mających doświadczenie praktyczne w zakresie funkcjonowania podmiotów przetwarzających dane osobowe.



9788381603874 W01P01

ISBN 978-83-8160-387-4



9 788381 603874

ZAMÓWIENIA:

INFOLINIA 801 04 45 45, FAX 22 535 80 01

ZAMOWIENIA@WOLTERSKLUWER.PL

WWW.PROFINFO.PL