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 Tobiczyk

PRAWO W PRAKTYCE

Wolters Kluwer

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 Tobiczyk

PRAWO W PRAKTYCE

Wolters Kluwer

WARSZAWA 2019

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 Tobiczyk – rozdz. 2

ISBN 978-83-8160-387-4

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

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 elektronizacją (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

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, 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 danych[1]. 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 technologicznych[2]. 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[3].

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 sprawdzeń[4].

N! Reforma ochrony danych osobowych z 2018 r. doprowadziła do tego, że wszystkie akty normatywne, które wymagały opracowania i wdrożenia powyższych dokumentów, przestały obowiązywać[5]. Zaowocowało to istotnymi zmianami w interesującej nas dziedzinie[6]. 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 zapewniania 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 uchylającą 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

CENA 99 ZŁ (W TYM 5% VAT)