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

Wolters Kluwer

WARSZAWA 2023

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

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

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 przybliżamy 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 Szkurłat

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 osobowych[2].

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.

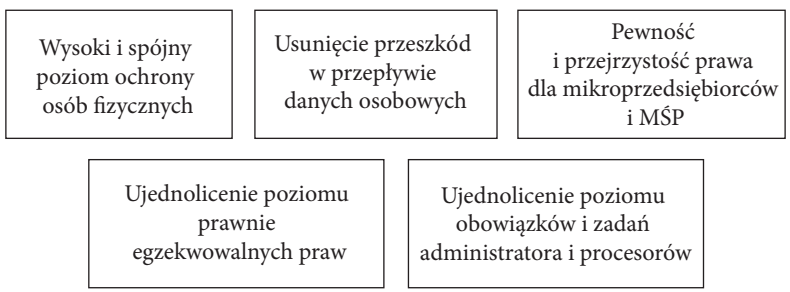
Opisane podejście jest związane ze zdiagnozowaną potrzebą unowocześnienia regulacji ochrony danych osobowych w Unii Europejskiej, zapewnienia jej neutralności technologicznej, zniwelowania negatywnych aspektów dotychczasowego wyboru środka legislacyjnego w postaci dyrektywy o minimalnym charakterze, 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 uelastycznić 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 ogóle niezautomatyzowany. W konsekwencji regulacja ta znajdzie 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 wyznaczany 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 uwzględnia 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.

9788383287133 W01P01

ISBN 978-83-8328-713-3

9 788383 287133

CENA 179 ZŁ (W TYM 5% VAT)