# RODO DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW

**redakcja Dominik Lubasz**

Karolina Alama, Roman Bieda, Witold Chomiczewski
Mirosław Gumularz, Damian Karwala, Patrycja Kozik
Dominik Lubasz, Beata Marek, Marcin Maruta
Dariusz Szostek, Marcin Wielisiej, Mariola Więckowska
Katarzyna Witkowska-Nowakowska

**RODO 2018**

Wolters Kluwer

# RODO DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW

**redakcja Dominik Lubasz**

Karolina Alama, Roman Bieda, Witold Chomiczewski
Mirosław Gumularz, Damian Karwala, Patrycja Kozik
Dominik Lubasz, Beata Marek, Marcin Maruta
Dariusz Szostek, Marcin Wielisiej, Mariola Więckowska
Katarzyna Witkowska-Nowakowska



Wolters Kluwer

WARSZAWA 2018

*Stan prawny na 5 kwietnia 2018 r.*

Wydawca
*Monika Pawłowska*

Redaktor prowadzący
*Joanna Ołówek*

Opracowanie redakcyjne
*Grażyna Polkowska-Nowak*

Łamanie
*Andytex*

*Poszczególne rozdziały napisali:*

*Karolina Alama, Marcin Maruta – rozdz. 6*
*Roman Bieda – rozdz. 5*
*Witold Chomiczewski – rozdz. 2 podrozdz. 2.1, 2.3–2.7, rozdz. 3 podrozdz. 3.3*
*Mirosław Gumularz – rozdz. 10 podrozdz. 10.1*
*Mirosław Gumularz, Patrycja Kozik – rozdz. 2 podrozdz. 2.2, rozdz. 3 podrozdz. 3.2*
*Damian Karwala – rozdz. 8*
*Dominik Lubasz – słowo wstępne, rozdz. 1 podrozdz. 1.1–1.3, rozdz. 2 podrozdz. 2.8, rozdz. 3 podrozdz. 3.4*
*Beata Marek – rozdz. 7 podrozdz. 7.1, 7.2, rozdz. 10 podrozdz. 10.2*
*Dariusz Szostek – rozdz. 4*
*Marcin Wielisiej – rozdz. 7 podrozdz. 7.3–7.6*
*Mariola Więckowska – rozdz. 3 podrozdz. 3.1*
*Katarzyna Witkowska-Nowakowska – rozdz. 1 podrozdz. 1.4, rozdz. 9*



ISBN 978-83-8124-609-5

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

| | | |
|---|---|---|
| dyrektywa 95/46/WE | – | dyrektywa 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 (Dz.Urz. UE L 281, s. 31–50) |
| dyrektywa 2013/37/UE | – | dyrektywa Parlamentu Europejskiego i Rady 2013/37/UE z 26.06.2013 r. zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.Urz. UE L 175, s. 1–8) |
| k.c. | – | ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2017 r. poz. 459) |
| k.p. | – | ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2018 r. poz. 108) |
| projekt ustawy | – | projekt ustawy z dnia … 2018 r. o ochronie danych osobowych (projekt w wersji skierowanej do Sejmu dnia 5.04.2018 r.) |
| r.d.p.d.o. | – | rozporządzenie 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, rozporządzenie 2016/679 | – | 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) (Dz.Urz. UE L 119, s. 1–88) |
| rozporządzenie eIDAS | – | rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.06.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz. UE L 257, s. 73–114) |
| u.o.d.o. | – | ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.) |

## Inne

| | | |
|---|---|---|
| ABI | – | administrator bezpieczeństwa informacji |
| BGB | – | Bürgerliches Gesetzbuch |
| DPIA | – | *Data Protection Impact Assessment* (in. OSOD) |

| | |
|---|---|
| DPO, IOD | – inspektor ochrony danych (*data protection officer*) |
| EOG | – Europejski Obszar Gospodarczy |
| M. Praw. | – Monitor Prawniczy |
| OSOD | – ocena skutków dla ochrony danych |

# SŁOWO WSTĘPNE

25.05.2018 r. to data wyznaczająca cezurę w systemie ochrony danych osobowych w Europie. Od tego dnia rozpoczyna obowiązywanie jednolicie w całej Unii Europejskiej rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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).

Nowa regulacja ochrony danych opiera się na kilku podstawowych filarach: na wysokim poziomie ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, na kształtowaniu obowiązków administratorów w oparciu o podejście bazujące na ryzyku i neutralności technologicznej, a przez to uelastycznieniu, odformalizowaniu i zrelatywizowaniu wymogów zależnie m.in. od wielkości administratora, z dostrzeżeniem szczególnej sytuacji prawnej małych i średnich przedsiębiorców. Nowe podejście wymaga jednak dużo intensywniejszego zaangażowania adresatów norm w proces ich stosowania, w szczególności poprzez czynności analityczne, ocenę zakresu i sposobu realizacji obowiązków, przede wszystkim przez dobór odpowiednich środków technicznych i organizacyjnych.

W tym niełatwym zadaniu autorzy publikacji starają się pomóc, przybliżając nowe zasady przetwarzania danych osobowych, wyjaśniając przesłanki legalizacyjne, opisując i analizując nowe prawa osób, których dane są przetwarzane, i wreszcie obowiązki administratorów, ze szczególnym uwzględnieniem pozycji małych i średnich przedsiębiorców.

Staraliśmy się przedstawić regulacje rozporządzenia ogólnego o ochronie danych w możliwie najbardziej praktyczny sposób, uwzględniając wytyczne Grupy Roboczej Art. 29, stanowiska organów nadzorczych oraz prawodawcy. Mamy nadzieję, że książka ta ułatwi stosowanie ogólnego rozporządzenia o ochronie danych w praktyce MŚP.

Dziękuję za zaangażowanie znakomitemu zespołowi autorów, będących zarówno praktykami, jak i teoretykami, nie tylko prawa, o bogatym wieloaspektowym doświadczeniu!

*dr Dominik Lubasz*

Rozdział 1

# ZAGADNIENIA OGÓLNE, DEFINICJE ORAZ ZASADY PRZETWARZANIA DANYCH

## 1.1. Zagadnienia wprowadzające

W dniu 25.05.2018 r. – po dwuletnim okresie przygotowawczym – ogólne rozporządzenie o ochronie danych (RODO) zacznie być stosowane[1]. Do tego dnia administratorzy i podmioty przetwarzające dane, a także ich przedstawiciele, zarówno z sektora prywatnego, jak i publicznego, niezależnie od wielkości i przedmiotu działalności, zobowiązani są do przygotowania swoich organizacji do stosowania nowej regulacji. W rozporządzeniu 2016/679 nie zostały bowiem przewidziane żadne przepisy przejściowe, które regulowałyby sytuację prawną podmiotów zobowiązanych, przetwarzających obecnie dane osobowe i zamierzających czynić to po 25.05.2018 r. W motywie 171 RODO zawarto jedyną wskazówkę stanowiącą, że przetwarzanie, które w dniu rozpoczęcia stosowania rozporządzenia już się toczy, powinno w terminie 2 lat od wejścia rozporządzenia w życie zostać dostosowane do jego przepisów.

Rozporządzenie 2016/679 zastępuje dotychczas obowiązującą 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*). Odchodzi tym samym od sztywnych ram regulacyjnych i wyabstrahowanych od kategorii administratora, zakresu jego działania, zwłaszcza jego związku z przetwarzaniem danych osobowych i skali tego przetwarzania, które były charakterystyczne dla polskiej ustawy z 29.08.1997 r. o ochronie danych osobowych[2] i rozporządzeń wykonawczych do niej, a zwłaszcza rozporzą-

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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. 1–88.

[2] Dz.U. z 2016 r. poz. 922 ze zm.

dzenia 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[3].

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, o którym mowa w art. 24, uwzględniania ochrony danych już w fazie projektowania (*privacy by design*) w myśl art. 25 ust. 1 oraz realizacji zasady domyślnej ochrony danych (*privacy 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. Jako podstawa przyjętej konstrukcji obowiązków wskazany mechanizm jest realizowany przez analizę ryzyka, dla której jednak brak szczegółowej regulacji w analizowanym rozporządzeniu. Decyzja na temat przyjmowanej metodyki, sposobu podejścia, użytych narzędzi analitycznych, jak również samego zakresu analizy pozostawiana jest w rękach administratora.

Opisane podejście związane jest ze zdiagnozowaną potrzebą unowocześnienia regulacji ochrony danych osobowych w Unii Europejskiej, zapewnienia jej neutralności technologicznej, zniwelowania negatywnych aspektów związanych z dotychczasowym wyborem środka legislacyjnego w postaci dyrektywy o minimalnym charakterze, a wreszcie dostrzeżeniem wartości danych osobowych w gospodarce (*data driven economy*) i wpływu wykorzystania danych, w szczególności w aspekcie transgranicznym, na budowanie jednolitego rynku cyfrowego w Unii Europejskiej[4]. Sformułowano w związku z tym **podstawowe cele**, jakie przyświecają 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 –

[3] Dz.U. poz. 1024.

[4] D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2017, art. 1, nt 15. Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pl.pdf. Projekt dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych (COM(2012)0010 (COD)), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

m.in. 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 regulacji. Zmieniono w związku z tym optykę rozwiązań, uelastyczniając podejście i różnicując nakładane obowiązki zależnie od warunków przetwarzania danych, różnych podmiotów przetwarzających i różnej jego skali, co miało być także odpowiedzią na sytuację prawną oraz oczekiwania małych i średnich przedsiębiorców[5].

W konsekwencji wszyscy administratorzy, w tym należący do kategorii małych i średnich przedsiębiorców, choć z pewnymi wyjątkami[6], do 25.05.2018 r. zobowiązani są wdrożyć wymogi rozporządzenia 2016/679 związane zarówno z opartymi na analizie ryzyka obowiązkami, jak i z realizacją praw podmiotów danych, a po tym terminie utrzymać i aktualizować system ochrony danych zgodny z przepisami analizowanego aktu prawnego. Z tych względów konieczne jest dokonanie weryfikacji procesów, w których niezbędne jest przetwarzanie danych osobowych, oraz dokonanie analizy zgodności przetwarzania w tych procesach przez pryzmat nowych zasad i przesłanek przetwarzania danych oraz nowego katalogu praw podmiotów danych i obowiązków nakładanych na administratorów.

Mimo bowiem tego, że rozporządzenie jest aktem prawa europejskiego obowiązującym bezpośrednio we wszystkich państwach członkowskich, bez potrzeby dokonywania zabiegów implementacyjnych[7], jak w przypadku dyrektyw, to w wielu jego przepisach zostało zawarte uprawnienie dla ustawodawców krajowych uregulowania niektórych zagadnień, jak np. instytucji organu nadzorczego, wyłączeń w przypadkach wymienionych w art. 23 czy zagadnień związanych z przetwarzaniem danych osobowych pracowników[8].

## 1.2. Zakres zastosowania regulacji

Przepisy art. 2 i 3 odpowiednio wyznaczają zakres przedmiotowy i zakres terytorialny zastosowania rozporządzenia 2016/679.

[5] D. Lubasz, K. Witkowska, *Europejska reforma ochrony danych osobowych z perspektywy pełnomocnika przedsiębiorcy* [w:] *Media elektroniczne. Współczesne problemy prawne*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2016, s. 176.

[6] Zob. pkt 3.4.1.2.

[7] Rozporządzenie wywołuje pełny skutek bezpośredni, a zatem zarówno wertykalny, jak i horyzontalny, co zostało potwierdzone w wyroku TS z 14.12.1971 r., C-43/71, Politi s.a.s. v. Minister Finansów Republiki Włoskiej, CURIA.

[8] Z tych prerogatyw polskich ustawodawca planuje skorzystać – zob. projekt ustawy o ochronie danych osobowych oraz Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 (https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-niektorych-ustaw-w-zwiazku-z-zapewnieniem-stosowania-rozporzadzenia-2016-679.html).

Publikacja to przeznaczone dla małych i średnich przedsiębiorców praktyczne omówienie nowych przepisów dotyczących ochrony danych osobowych wprowadzonych przez rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. (RODO).

Autorzy szczegółowo opisują, jak przedsiębiorcy powinni przygotować się do stosowania RODO. Praktyczne wskazówki ułatwią proces wdrożenia nowych regulacji. W porównaniu z dotychczasowymi przepisami istotnie zmieniają się obowiązki administratorów danych i sposób ich wykonywania.

Z książki czytelnik dowie się m.in.:
– jakie są nowe prawa podmiotów danych, w tym prawa informacyjne, prawo do bycia zapomnianym, do przenoszenia danych czy też prawo do ograniczenia przetwarzania, co oznaczają i jak je realizować;
– jakie są nowe obowiązki nałożone na administratorów i jak się przygotować do ich wykonywania;
– jakie sankcje, nie tylko finansowe, będą groziły za naruszenie nowych przepisów.

Autorzy w opracowaniu uwzględnili ponadto projekt nowej polskiej ustawy o ochronie danych osobowych.

9788381246095 W01P01

ISBN 978-83-8124-609-5

9 788381 246095



CENA 119 ZŁ (W TYM 5% VAT)