RODO
PRZEWODNIK
ZE WZORAMI

redakcja Maciej Gawroński

Aleksander P. Czarnowski, Marcin Dominiak
Aleksandra Gawron, Maciej Gawroński
Michał Kibil, Katarzyna Kloc, Katarzyna Kunda
Patrycja Naklicka, Zuzanna Piotrowska, Paweł Punda
Michał Sztąberek, Magdalena Wojtas

RODO 2018

Wolters Kluwer

RODO
PRZEWODNIK
ZE WZORAMI

redakcja Maciej Gawroński

Aleksander P. Czarnowski, Marcin Dominiak
Aleksandra Gawron, Maciej Gawroński
Michał Kibil, Katarzyna Kloc, Katarzyna Kunda
Patrycja Naklicka, Zuzanna Piotrowska, Paweł Punda
Michał Sztąberek, Magdalena Wojtas

Wolters Kluwer

WARSZAWA 2018

Stan prawny na 10.03.2018 r. z uwzględnieniem zmian wprowadzonych rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. (ogólne rozporządzenie o ochronie danych, Dz.Urz. UE L 119, s. 1) wchodzącym w życie z dniem 25.05.2018 r.

Wydawca
Monika Pawłowska

Redaktor prowadzący
Joanna Tchorek

Opracowanie redakcyjne
Grażyna Polkowska-Nowak

Łamanie
Fotoedytor

ISBN 978-83-8124-637-8

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

Część B
Wzory dokumentów

Wzory rejestrów

WYKAZ SKRÓTÓW

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. WE L 281, s. 31)
dyrektywa 2016/680	– dyrektywa 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89)
EKPC	– Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie 4.11.1950 r. (Dz.U. z 1993 r. poz. 284 ze zm.)
GDPR	– EU General Data Protection Regulation
k.c.	– ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2017 r. poz. 459 ze zm.)
Konstytucja RP	– ustawa z 2.04.1997 r. – Konstytucja Rzeczypospolitej Polskiej (Dz.U. poz. 483 ze zm.)
k.p.	– ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2018 r. poz. 108 ze zm.)
KPP	– Karta praw podstawowych UE (Dz.Urz. UE C 202 z 2016 r., s. 389)
pr. bank.	– ustawa z 29.09.1997 r. – Prawo bankowe (Dz.U. z 2017 r. poz. 1876 ze zm.)

rozporządzenie 2016/679, RODO	– 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)
TFUE	– Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47)
TUE	– Traktat o Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 13)
u.o.d.o.	– ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.)
u.r.	– ustawa z 29.09.1994 r. o rachunkowości (Dz.U. z 2018 r. poz. 395 ze zm.)
u.s.i.o.z.	– ustawa z 28.04.2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2017 r. poz. 1845 ze zm.)
wyrok C-131/12 Google Spain	– wyrok z 13.05.2014 r., C-131/12, Google Spain SL i Google Inc. v. Agencia Española de Protección de Datos (AEPD) i Mario Costeja González, EU:C:2014:317

Część A

KOMPENDIUM RODO

Rozdział I

ZGODNOŚĆ PODSTAWOWA

1. RODO – unijna „ustawa" o ochronie danych osobowych

1.1. RODO – nowa „ustawa" o ochronie danych osobowych

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) – RODO – to w dużym skrócie **nowa „ustawa" o ochronie danych osobowych**.

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych w Unii Europejskiej (motyw 1 RODO). Stanowią o tym: art. 8 ust. 1 Karty praw podstawowych UE (Dz.Urz. UE C 202 z 2016 r., s. 389) oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47), zgodnie z którymi każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

Unia Europejska uznała, że w celu realizacji i gwarancji prawa do prywatności i ochrony danych na terenie Unii konieczne jest określenie stabilnych, spójnych ram ochrony danych osobowych oraz zdecydo-

wanego ich **egzekwowania**. Dotychczas problemem było właśnie egzekwowanie (wymuszanie) stosowania przepisów o ochronie danych osobowych.

1.2. Przedmiot i cel RODO

1.2.1. Uwagi wstępne

Formalnie RODO utrzymuje dotychczasowe zasady ochrony danych osobowych obowiązujące na terenie Unii Europejskiej (w tym w Polsce na podstawie „starej" ustawy z 29.08.1997 r. o ochronie danych osobowych, Dz.U. z 2016 r. poz. 922 ze zm.), natomiast nieco je uszczegóławia, dodaje uprawnienia osobom fizycznym i wprowadza surowe kary.

Mimo uspokajających wypowiedzi organów nadzorczych w praktyce RODO stanowi rewolucję w ochronie danych właśnie ze względu na kary, nowe obowiązki firm i innych podmiotów przetwarzających dane osobowe ze względu na tzw. podejście oparte na ryzyku, czyli spoczywający na wszystkich obowiązek oceny ryzyk związanych z przetwarzaniem danych osobowych i dostosowania sposobów ochrony danych do tych ryzyk, a także ze względu na wprowadzenie zasady rozliczalności – obowiązku wykazania zgodności przez obowiązanego.

§ Zgodnie z art. 1 RODO:

1. W niniejszym rozporządzeniu ustanowione zostają **przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych** osobowych.
2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich **prawo do ochrony danych osobowych**.
3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

1.2.2. Ochrona osób fizycznych

Ogólne rozporządzenie o ochronie danych jest aktem kompleksowym, który szeroko reguluje kwestię ochrony prywatności i danych osobowych (osób fizycznych), a także dotyka materii swobodnego przepływu danych osobowych w Unii Europejskiej. RODO nie dotyczy przetwarzania danych dotyczących osób prawnych, w szczególności przedsiębiorstw, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej (motyw 14).

1.2.3. Bezpośredniość

RODO jest aktem prawnym przyjętym na poziomie unijnym, ma jednak bezpośrednie zastosowanie do każdej organizacji przetwarzającej dane osobowe jako administrator danych lub podmiot przetwarzający w państwie członkowskim Unii Europejskiej.

Bezpośredniość stosowania i w konsekwencji rola „ustawy" o ochronie danych osobowych to cechy odróżniające RODO od tracącej wkrótce moc 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 (Dz.Urz. WE L 281, s. 31), która w założeniu miała harmonizować przepisy o ochronie danych osobowych w Unii Europejskiej, ale ze względu na spore różnice w implementujących ją przepisach krajowych w praktyce poziom ochrony danych osobowych i podejście do tego obszaru były dość mocno zróżnicowane.

RODO jako wspólna nowa „ustawa" o ochronie danych ma zapewnić wysoki, ujednolicony poziom ochrony danych w całej Unii Europejskiej. Dzięki swojej ogólności i wysokopoziomowości RODO pozostawia jednocześnie duży zakres swobody w podejściu, luz interpretacyjny i praktykę do wypracowania w poszczególnych państwach członkowskich.

Maciej Gawroński – radca prawny; konsultant Grupy Roboczej Art. 29 ds. projektu standardowych klauzul umownych *ad hoc* dotyczących przekazywania danych przez przetwarzającego w UE do podprzetwarzającego spoza UE; ekspert Komisji Europejskiej ds. kontraktów cloud computingowych. Zaproponował Komisji Europejskiej zasadę odpowiedzialności pozaunijnych podprocesorów, która stała się ogólną zasadą odpowiedzialności podmiotów przetwarzających, a także zasadę przenoszalności danych osobowych, konsultował zasady podpowierzenia; ekspert prawa technologii mediów i telekomunikacji rekomendowany przez Ranking Kancelarii Prawnych dziennika „Rzeczpospolita". Jest też jednym z twórców treści systemu informacji prawnej LEX Ochrona Danych Osobowych.

W książce w praktyczny sposób wyjaśniono przepisy RODO, wskazano wiele dokumentów i rozwiązań, dzięki którym czytelnik będzie mógł postępować zgodnie z tą regulacją unijną.

Autorzy wykorzystali opinie Grupy Roboczej Art. 29 oraz GIODO, normy ISO z obszaru bezpieczeństwa informacji, a także bogate doświadczenie z własnej krajowej i międzynarodowej praktyki ochrony danych osobowych, cyberbezpieczeństwa i cloud computingu, w tym prace dla Grupy Roboczej Art. 29 i Komisji Europejskiej.

W publikacji czytelnik znajdzie m.in.:
– projekt polityki ochrony danych osobowych, która obejmuje obowiązki administratora i podmiotu przetwarzającego,
– wzór umowy powierzenia danych,
– wzory klauzul informacyjnych, w których zawarto kategorie informacji,
– listy standardowych zagrożeń bezpieczeństwa informacji i potencjalnych naruszeń praw i wolności mogących wyniknąć z naruszenia ochrony danych osobowych.

Autorzy wyjaśniają również zagadnienia mogące stwarzać szczególne trudności przy stosowaniu RODO, jak np. art. 11 RODO dotyczący tak zwanych danych niezidentyfikowanych.

9788381246378 W01P01

ZAMÓWIENIA:
INFOLINIA 801 04 45 45, FAX 22 535 80 01
ZAMOWIENIA@WOLTERSKLUWER.PL
WWW.PROFINFO.PL

ISBN 978-83-8124-637-8
9 788381 246378

CENA 119 ZŁ (W TYM 5% VAT)