

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

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

Zamów książkę w księgarni internetowej

proinfo.pl
księgarnia internetowa

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

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegał przysługujących im praw. Książkę możesz udostępnić osobom bliskim lub osobiście znanym, ale nie publikuj jej w internecie. Jeśli cytujesz fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A jeśli musisz skopiować część, rób to jedynie na użytek osobisty.

prawolubni

SZANUJMY PRAWO I WŁASNOŚĆ
Więcej na www.legalnakultura.pl
POLSKA IZBA KSIĄŻKI

© Copyright by
Wolters Kluwer Polska Sp. z o.o., 2018

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	13
Słowo wstępne	15
Rozdział 1	
Zagadnienia ogólne, definicje oraz zasady przetwarzania danych – Dominik Lubasz, Katarzyna Witkowska-Nowakowska	17
1.1. Zagadnienia wprowadzające – Dominik Lubasz	17
1.2. Zakres zastosowania regulacji – Dominik Lubasz	19
1.3. Definicje kluczowych pojęć – Dominik Lubasz	21
1.3.1. Dane osobowe	21
1.3.2. Przetwarzanie	26
1.3.3. Administrator i podmiot przetwarzający	27
1.4. Zasady przetwarzania – Katarzyna Witkowska-Nowakowska	28
1.4.1. Zasady: legalności, rzetelności i przejrzystości	29
1.4.2. Zasada ograniczenia celu	30
1.4.3. Zasada minimalizacji danych	31
1.4.4. Zasada prawidłowości	32
1.4.5. Zasada ograniczenia przechowywania	32
1.4.6. Zasada integralności i poufności	34
1.4.7. Zasada rozliczalności	35
Rozdział 2	
Zapewnienie legalności przetwarzania – Witold Chomiczewski, Mirosław Gumularz, Patrycja Kozik	37
2.1. Zagadnienia wprowadzające – Witold Chomiczewski	37
2.2. Zgoda jako podstawa legalizująca przetwarzanie danych osobowych – Mirosław Gumularz, Patrycja Kozik	38
2.2.1. Kryteria skuteczności zgody	39
2.2.1.1. Sposób wyrażenia i jednoznaczność zgody	39
2.2.1.2. Sposób wyrażenia zgody a dane wrażliwe	40
2.2.1.3. Forma wyrażenia zgody	41

2.2.1.4. Konkretność zgody	41
2.2.1.5. Dobrowolność zgody	42
2.2.1.6. Świadomość zgody	44
2.2.2. Wymóg zapewnienia rozliczalności w zakresie zgody	45
2.2.3. Wycofanie zgody	45
2.2.4. Zgoda dziecka	45
2.2.5. Zgoda a projektowane przepisy prawa pracy	48
2.2.6. Zgoda a inne podstawy przetwarzania	49
2.2.7. Zgoda na zmianę celu przetwarzania danych	50
2.2.8. Skuteczność zgód a wytyczne Grupy Roboczej Art. 29	51
2.2.9. Pozyskiwanie zgód – wytyczne	52
2.3. Niezbędność przetwarzania do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy – <i>Witold Chomiczewski</i> ...	53
2.3.1. Wykonanie umowy	53
2.3.2. Działania przed zawarciem umowy	55
2.4. Niezbędność przetwarzania do wypełnienia obowiązku ciążącego na administratorze – <i>Witold Chomiczewski</i>	56
2.5. Niezbędność przetwarzania do ochrony żywotnych interesów podmiotu danych – <i>Witold Chomiczewski</i>	57
2.6. Niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym – <i>Witold Chomiczewski</i>	58
2.7. Niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów – <i>Witold Chomiczewski</i>	58
2.8. Dopuszczalność przetwarzania szczególnych kategorii danych osobowych – <i>Dominik Lubasz</i>	61

Rozdział 3

Obowiązki administratorów – <i>Witold Chomiczewski, Mirosław Gumularz, Patrycja Kozik, Dominik Lubasz, Mariola Więckowska</i>	63
3.1. Obowiązki bazujące na ryzyku – <i>Mariola Więckowska</i>	63
3.1.1. Uwagi ogólne	63
3.1.1.1. Podejście oparte na ryzyku	65
3.1.1.2. Ochrona danych w fazie projektowania – <i>privacy by design</i>	66
3.1.2. Ocena skutków dla ochrony danych – OSOD	67
3.1.2.1. OSOD w przypadku współadministratorów i powierzenia danych podmiotom przetwarzającym	69
3.1.2.2. Kiedy konieczne jest przeprowadzenie OSOD?	70
3.1.3. Etap 1.: Wstępna ocena skutków dla ochrony danych wraz z ogólną analizą ryzyka	72
3.1.3.1. Przykładowy szablon do etapu 1.: Wstępna ocena skutków dla ochrony danych (WOSOD)	73
3.1.3.1.1. Informacje ogólne	73

3.1.3.1.2. Osoba odpowiedzialna za OSOD	73
3.1.3.1.3. Opis zmiany	73
3.1.3.1.4. Charakter danych	74
3.1.3.1.5. Typ, zakres i operacje na danych	75
3.1.3.1.6. Prawa podmiotów danych	76
3.1.3.1.7. Czy zmiana będzie wymagała dostosowania Regulaminu Firmy? Jeśli tak, krótko opisz, jakiej	77
3.1.3.1.8. Kryteria przeprowadzenia OSOD	77
3.1.3.1.9. Decyzja dotycząca ryzyka	78
3.1.3.1.10. Akceptacja osoby odpowiedzialnej za ochronę danych / inspektor ochrony danych	79
3.1.3.2. Podsumowanie	79
3.1.4. Etap 2.: Analiza zmiany i jej wpływu na prywatność	79
3.1.4.1. Identyfikacja zagrożeń i ich potencjalnego wpływu na prywatność	80
3.1.4.2. Przykładowa tabela obszarów analizy wpływu na prywatność ..	81
3.1.5. Etap 3.: Analiza ryzyka i działań zapobiegawczych	85
3.1.5.1. Szacowanie poziomu ryzyka	87
3.1.5.2. Postępowanie z ryzykiem	89
3.1.5.3. Przykładowa lista kontrolna dla oceny ryzyka i możliwych sposobów jego ograniczenia	91
3.1.6. Etap 4.: Przygotowanie raportu końcowego wraz ze strategią postępowania z ryzykiem	94
3.1.7. Etap 5.: Monitoring wdrożenia	95
3.1.8. Korzyści z OSOD	95
3.1.9. Zakończenie	96
3.2. Upřednie konsultacje – <i>Mirosław Gumularz, Patrycja Kozik</i>	97
3.2.1. Uwagi ogólne	97
3.2.2. Typowe sytuacje, które mogą prowadzić do obowiązku dokonania upřednich konsultacji	98
3.2.3. Istotne kryteria dokonywania upřednich konsultacji w wytycznych Grupy Roboczej Art. 29	98
3.2.4. Elementy konsultacji	100
3.2.5. Na kim ciąży obowiązek dokonania upřednich konsultacji?	100
3.2.6. Działania organu nadzorczego	101
3.2.7. Przepisy szczególne mogące dotyczyć upřednich konsultacji	102
3.2.8. Sankcje	102
3.3. Notyfikowanie naruszeń ochrony danych osobowych – <i>Witold Chomiczewski</i>	102
3.3.1. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu	103
3.3.2. Zawiadamianie podmiotów danych o naruszeniach ochrony danych osobowych	104

3.4. Obowiązki dokumentacyjne – <i>Dominik Lubasz</i>	106
3.4.1. Rejestr czynności przetwarzania	108
3.4.1.1. Zakres danych w rejestrze czynności	108
3.4.1.2. Zwolnienie z obowiązku prowadzenia rejestrów dla MŚP	113
3.4.2. Rejestr kategorii czynności przetwarzania	113
3.4.3. Polityki ochrony danych	114
3.4.4. Pozostałe obowiązki dokumentacyjne	116

Rozdział 4

Wymogi w zakresie formy w ogólnym rozporządzeniu – <i>Dariusz Szostek</i>	117
4.1. Zagadnienia wprowadzające	117
4.2. Źródła prawa w odniesieniu do formy	117
4.3. Forma dotycząca zgody	118
4.4. Dowód na fakt uzyskania zgody	121
4.5. Wymogi dotyczące formy dla poszczególnych oświadczeń	123
4.6. Forma umowy o powierzenie	124

Rozdział 5

Inspektor ochrony danych – <i>Roman Bieda</i>	126
5.1. Zagadnienia wprowadzające	126
5.2. Wyznaczenie inspektora ochrony danych (IOD)	127
5.2.1. Uwagi ogólne	127
5.2.2. Obligatoryjne wyznaczenie IOD	128
5.2.3. Wymagane kwalifikacje zawodowe IOD	134
5.2.4. Podstawy zatrudnienia IOD	137
5.2.5. Notyfikacja oraz publikacja danych IOD	137
5.2.5.1. Publikacja danych kontaktowych IOD	137
5.2.5.2. Przekazanie danych IOD osobom, których dane dotyczą	138
5.2.5.3. Zawiadomienie organu nadzorczego o danych kontaktowych IOD	139
5.2.5.4. Zamieszczenie danych IOD w tzw. rejestrze czynności przetwarzania danych (rejestrze kategorii czynności przetwarzania)	140
5.3. Zadania inspektora ochrony danych	140
5.3.1. Uwagi ogólne	140
5.3.2. Podstawowe (obligatoryjne) zadania IOD	141
5.3.3. Informowanie administratora i podmiotu przetwarzającego o obowiązkach wynikających z przepisów o ochronie danych oraz doradzanie w tym zakresie (art. 39 ust. 1 lit. a RODO)	141
5.3.4. Monitorowanie przestrzegania przepisów o ochronie danych osobowych (art. 39 ust. 1 lit. b RODO)	142
5.3.5. Ocena skutków dla ochrony danych (art. 35, art. 39 ust. 1 lit. c RODO)	143

5.3.6. Współpraca z organem nadzorczym oraz pełnienie funkcji „punktu kontaktowego” dla organu nadzorczego	144
5.3.7. Pełnienie funkcji „punktu kontaktowego” dla osób, których dane dotyczą	145
5.3.8. Inne zadania IOD	145
5.4. Status inspektora ochrony danych	146
5.4.1. Uwagi ogólne	146
5.4.2. Zasada niezależności IOD	146
5.4.3. Obowiązek przedsiębiorcy włączania IOD we wszystkie sprawy dotyczące ochrony danych osobowych	147
5.4.4. Obowiązek wspierania IOD przez przedsiębiorcę	148
5.4.5. Obowiązek zachowania poufności przez IOD	149

Rozdział 6

Outsourcing – powierzenie przetwarzania danych osobowych – Karolina

<i>Alama, Marcin Maruta</i>	150
6.1. Zagadnienia wprowadzające	150
6.2. Powierzenie przetwarzania danych – podstawowe pojęcia	152
6.3. Powierzenie przetwarzania – prawa i obowiązki stron	153
6.4. Obowiązki administratora w związku z powierzeniem przetwarzania danych osobowych	154
6.4.1. Uwagi ogólne	154
6.4.2. Wybór podmiotu przetwarzającego spełniającego wymagania rozporządzenia 2016/679	155
6.4.3. Wydawanie udokumentowanych poleceń	156
6.4.4. Umowa powierzenia przetwarzania danych osobowych	157
6.4.4.1. Forma umowy	157
6.4.4.2. Zakres przedmiotowy umowy powierzenia przetwarzania	159
6.4.4.3. Podpowierzenie przetwarzania danych – korzystanie z usług podprocesora	159
6.4.4.4. Obowiązek pomocy administratorowi	161
6.4.4.5. Współpraca z administratorem	162
6.4.4.6. Usunięcie lub zwrócenie danych	162
6.4.4.7. Stosunek umowy powierzenia danych do umowy głównej	162
6.5. Międzynarodowy transfer danych osobowych w kontekście powierzenia przetwarzania danych osobowych	163
6.5.1. Uwagi ogólne	163
6.5.2. Podstawy prawne transferu danych poza EOG	163
6.6. Odpowiedzialność podmiotów uczestniczących w powierzeniu przetwarzania danych osobowych	164
6.7. Rynek usług chmurowych a powierzenie przetwarzania danych osobowych	166
6.7.1. Uwagi ogólne	166

6.7.2. Zapewnienie zgodności powierzenia danych przez administratora	166
6.7.3. Prognozy w zakresie przyszłości rynku usług chmurowych	169
6.7.4. Migracja do rozwiązań chmurowych a zgodność z rozporządzeniem 2016/679	170
6.8. Obowiązki administratora i procesora w zakresie powierzenia przetwarzania danych osobowych – podsumowanie	170

Rozdział 7

Prawa podmiotów danych – <i>Beata Marek, Marcin Wielisiej</i>	173
7.1. Prawa informacyjne i dostępowe – <i>Beata Marek</i>	173
7.1.1. Obowiązki informacyjne, gdy dane pozyskiwane są bezpośrednio od osoby, której dane dotyczą	174
7.1.2. Obowiązki informacyjne, gdy dane pozyskiwane są w sposób inny niż od osoby, której dane dotyczą	177
7.1.3. Dostęp do danych	179
7.2. Prawo do sprostowania danych, usunięcia i zapomnienia – <i>Beata Marek</i>	180
7.2.1. Sprostowanie danych	180
7.2.2. Usunięcie danych (prawo do bycia zapomnianym)	181
7.3. Prawo do ograniczenia przetwarzania – <i>Marcin Wielisiej</i>	183
7.3.1. Uwagi ogólne	183
7.3.2. Uprawnieni do korzystania z prawa do ograniczenia przetwarzania danych	184
7.3.3. Zakres stosowania prawa do ograniczenia przetwarzania	184
7.3.4. Kwestionowanie prawidłowości danych	185
7.3.5. Przetwarzanie niezgodne z prawem	186
7.3.6. Dane nie są już niezbędne do realizacji celu przetwarzania	188
7.3.7. Wniesienie sprzeciwu	188
7.3.8. Treść i forma komunikacji z osobą, której dane dotyczą	189
7.3.9. Realizacja ograniczenia przetwarzania	190
7.3.10. Przesłanki uzasadniające przetwarzanie danych mimo wniesionego żądania ograniczenia	191
7.3.11. Sankcje	192
7.4. Prawo do przenoszenia danych – <i>Marcin Wielisiej</i>	192
7.4.1. Uwagi ogólne	192
7.4.2. Zakres stosowania prawa do przenoszenia danych	193
7.4.3. Zakres danych objętych prawem do przenoszenia	194
7.4.4. Treść i forma komunikacji z osobą, której dane dotyczą	195
7.4.5. Przygotowanie i format danych	196
7.4.6. Realizacja prawa do przeniesienia danych	197
7.4.7. Przekazanie danych osobie, której dane dotyczą	198
7.4.8. Przekazanie danych innemu administratorowi	199

7.4.9. Sankcje	200
7.5. Prawo do sprzeciwu – <i>Marcin Wielisiej</i>	200
7.5.1. Uwagi ogólne	200
7.5.2. Przesłanki zastosowania prawa do sprzeciwu	201
7.5.3. Forma zgłoszenia sprzeciwu	202
7.5.4. Realizacja sprzeciwu	203
7.5.5. Sankcje	203
7.6. Prawa związane z profilowaniem – <i>Marcin Wielisiej</i>	204
7.6.1. Uwagi ogólne	204
7.6.2. Zakaz podejmowania automatycznych decyzji	205
7.6.3. Ograniczenia zakazu podejmowania automatycznych decyzji	206
7.6.4. Profilowanie zgodne z rozporządzeniem 2016/679	207
7.6.5. Sankcje	208
 Rozdział 8	
Transfery danych do państw trzecich – <i>Damian Karwala</i>	209
8.1. Zagadnienia wprowadzające	209
8.1.1. Ponadgraniczne transfery danych w praktyce	209
8.1.2. Krytyka dotychczasowej regulacji transferowej i ogólna ocena zmian	210
8.2. Transfery danych na podstawie decyzji Komisji Europejskiej	212
8.3. Transfery danych z wykorzystaniem odpowiednich zabezpieczeń	215
8.4. Umowy transferowe	216
8.5. Transfery danych na podstawie wiążących reguł korporacyjnych	219
8.6. Kodeksy postępowania (dobrych praktyk) oraz mechanizmy certyfikacyjne jako nowe podstawy transferowe	220
8.7. Transfery danych z użyciem odstępstw (wyjątków)	221
8.8. Zgoda osoby zainteresowanej jako podstawa transferu	221
8.9. Prawnie uzasadnione interesy eksportera danych	224
8.10. Operacje dalszych transferów danych	225
8.11. Kolejność stosowania przesłanek transferowych	225
 Rozdział 9	
Postępowanie kontrolne i sankcje – <i>Katarzyna Witkowska-Nowakowska</i>	227
9.1. Zagadnienia wprowadzające	227
9.2. Postępowanie kontrolne	228
9.3. Postępowanie w sprawie naruszenia ochrony danych osobowych	230
9.4. Administracyjne kary pieniężne	231
9.4.1. Warunki nakładania administracyjnych kar pieniężnych	231
9.4.2. Wysokość i podstawa do nałożenia kar	232
9.5. Sankcje karne	235
9.6. Uprawnienia podmiotu danych	236

Rozdział 10

Szczególne sytuacje związane z przetwarzaniem – Mirosław Gumularz, Beata Marek	239
10.1. Przetwarzanie danych osobowych w związku z zatrudnieniem – Mirosław Gumularz	239
10.2. Przetwarzanie danych w big data – Beata Marek	242
Bibliografia	247

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 (<i>data protection officer</i>)
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 stosowane¹. 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 osobowych² 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 osobowych³.

Podjęcie 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 Europejskiej⁴. 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 przedsiębiorców⁵.

W konsekwencji wszyscy administratorzy, w tym należący do kategorii małych i średnich przedsiębiorców, choć z pewnymi wyjątkami⁶, 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 implementacyjnych⁷, 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 pracowników⁸.

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 Fiansów 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 przeznaczona 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.



9 788381 246095 W01P01

ISBN 978-83-8124-609-5



9 788381 246095

ZAMÓWIENIA:

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