

**OCHRONA DANYCH  
OSOBOWYCH  
KONTROLA I POSTĘPOWANIE  
W SPRAWIE NARUSZENIA PRZEPISÓW**  
**Poradnik ze wzorami**

Mirosław Gumularz, Patrycja Kozik

---

---

---

# OCHRONA DANYCH OSOBOWYCH

## KONTROLA I POSTĘPOWANIE W SPRAWIE NARUSZENIA PRZEPISÓW

### Poradnik ze wzorami

Mirosław Gumularz, Patrycja Kozik

---

---

Zamów książkę w księgarni internetowej

**proinfo.pl**  
księgarnia internetowa

*Stan prawny na 1 stycznia 2019 r.*

Wydawca  
*Monika Pawłowska*

Redaktor prowadzący  
*Hanna Kolenkiewicz*

Opracowanie redakcyjne i łamanie  
*Violet Design*

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.

The logo for 'prawolubni' features the word 'prawolubni' in a lowercase, serif font. A small heart symbol is positioned above the 'i'. Below the text is a decorative horizontal line with a wavy, wave-like pattern.

SZANUJMY PRAWO I WŁASNOŚĆ  
Więcej na [www.legalnakultura.pl](http://www.legalnakultura.pl)  
POLSKA IZBA KSIĄŻKI

© Copyright by  
Wolters Kluwer Polska Sp. z o.o., 2019

ISBN 978-83-8160-395-9

Dział Praw Autorskich  
01-208 Warszawa, ul. Przyokopowa 33  
tel. 22 535 82 19  
e-mail: [ksiazki@wolterskluwer.pl](mailto:ksiazki@wolterskluwer.pl)  
[www.wolterskluwer.pl](http://www.wolterskluwer.pl)  
księgarnia internetowa [www.profinfo.pl](http://www.profinfo.pl)

# SPIS TREŚCI

Wykaz skrótów .....	15
---------------------	----

## Część I Podziały danych osobowych objętych kontrolą

1. Dane osobowe wrażliwe (szczególne kategorie danych), dane o karalności oraz dane osobowe zwykłe .....	19
2. Dane osobowe podane, zaobserwowane, pochodne oraz wywnioskowane .....	21
3. Dane uporządkowane oraz nieuporządkowane .....	23
3.1. Ogólne informacje .....	23
3.2. Uporządkowanie a ustrukturyzowanie .....	29
4. Dane identyfikowalne oraz nieidentyfikowalne .....	30
4.1. Dwie normy wynikające z art. 11 RODO .....	30
4.2. Artykuł 11 RODO a definicja danych osobowych .....	31
4.3. Krótkotrwałe i długotrwałe przetwarzanie danych .....	38

## Część II Pytania i odpowiedzi

1. Czym jest RODO? .....	41
2. Jakie sankcje administracyjne i karne mogą grozić za naruszenie RODO? .....	42
3. Jakich kategorii danych dotyczy kontrola/postępowanie? .....	44
4. Kiedy przepisy RODO nie będą miały zastosowania? .....	48

5. Jakie podmioty podlegają kontroli / mogą być adresatem decyzji w ramach postępowania w sprawie naruszenia przepisów o ochronie danych osobowych? .....	49
6. Kiedy prowadzona jest kontrola, a kiedy prowadzi się postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych? .....	51
7. Czy do kontroli uzupełniającej stosuje się przepisy Kodeksu postępowania administracyjnego (w tym przepisy gwarancyjne)? .....	56
8. Jaka jest relacja pomiędzy przepisami o kontroli w RODO a przepisami prawa przedsiębiorców? .....	58
9. Jak należy rozumieć pojęcie naruszenia przepisów o ochronie danych osobowych? .....	61
10. Jakie są tryby kontroli? Czy kontrole mogą być niezapowiedziane? .....	62
11. Jakie są obowiązki kontrolowanego w trakcie kontroli i co grozi za ich naruszenie? .....	66
12. Czy można kwestionować wszczęcie kontroli lub inne czynności w toku kontroli? .....	67
13. Czy można kwestionować wszczęcie postępowania administracyjnego lub inne czynności w jego toku? .....	68
14. Jaka jest relacja zasady rozliczalności do obowiązku zebrania materiału dowodowego przez organ nadzorczy (art. 77 k.p.a.)? ....	69
15. Jak ustalić moment wszczęcia postępowania administracyjnego? .....	73
16. Jakie dokumenty inicjują kontrolę? .....	73
17. Czy i jak chroniona jest tajemnica przedsiębiorstwa? .....	76
18. Czy i w jakim zakresie Prezes UODO może mieć dostęp do tajemnic prawnie chronionych w toku kontroli i postępowania administracyjnego, na przykładzie poszczególnych tajemnic? .....	80
19. Jakie są konsekwencje naruszenia wymogów co do treści upoważnienia do kontroli? .....	81
20. Czy kontrola może być realizowana wyłącznie w zakresie upoważnienia? .....	82
21. Czy pracownicy kontrolowanego administratora/podmiotu przetwarzającego podlegają kontroli? .....	83

22. Czy można odpowiadać dyscyplinarnie za naruszenia przepisów dotyczących ochrony danych osobowych? .....	84
23. Jak długo może być prowadzona kontrola? .....	86
24. Kto prowadzi kontrolę? .....	87
25. Kto może brać udział w kontroli? Czy można prowadzić kontrolę pod nieobecność kontrolowanego? .....	87
26. Czy sektor publiczny objęty jest także kontrolą? .....	89
27. Czy można prowadzić kontrolę u procesora (podmiotu przetwarzającego)? .....	89
28. Jakie uprawnienia ma kontrolujący? .....	91
29. Jaka jest rola osoby, której dane dotyczą, w ramach kontroli i postępowania? .....	91
30. W jaki formalny sposób dochodzi do zakończenia kontroli? .....	93
31. W jaki sposób można kwestionować treść protokołu kontroli? .....	96
32. Czy protokół kontroli i materiał dowodowy kontroli stają się automatycznie częścią materiału dowodowego w postępowaniu administracyjnym? .....	97
33. Czy czynności w toku kontroli są utrwalane jedynie w protokole? .....	98
34. Czy wadliwość czynności w toku kontroli może mieć wpływ na postępowanie administracyjne? .....	99
35. Kto jest stroną w postępowaniu administracyjnym? .....	99
36. Kiedy postępowanie administracyjne może być umorzone? .....	101
37. Jakie są rodzaje rozstrzygnięć co do istoty sprawy w ramach postępowania w przedmiocie naruszenia przepisów o ochronie danych osobowych? .....	102
38. Jakie są skutki doręczenia decyzji Prezesa UODO? .....	103
39. Jaki środek przysługuje w postępowaniu administracyjnym w przypadku niezafatwienia sprawy w terminie? .....	104
40. Czy decyzja Prezesa UODO w postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych jest natychmiastowo wykonalna? .....	106
41. Jak można kwestionować (skarżyć) decyzję Prezesa UODO? .....	107
42. Czy niekorzystny wyrok WSA można zakwestionować? .....	108

---

43. Czy do postępowania w sprawie naruszenia przepisów o ochronie danych osobowych stosuje się reguły dotyczące milczącego załatwienia sprawy? .....	109
44. Jakie są podstawy wyłączenia kontrolera/ pracownika organu prowadzącego postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych? .....	110
45. Jakie są administracyjne kary pieniężne w sektorze prywatnym, a jakie w sektorze publicznym? .....	110
46. Jakie są kryteria miarkowania kary w ramach decyzji kończącej postępowanie? .....	113
47. Czy można nałożyć karę pieniężną bez postępowania/ decyzji? .....	115
48. Czy administracyjne kary pieniężne ulegają przedawnieniu? .....	116
49. W jakim terminie należy zapłacić karę? .....	117
50. Czy można starać się o rozłożenie kary na raty, odroczenie terminu płatności lub o ulgę w jej wykonaniu? .....	118
51. Jaka jest wysokość opłaty w przypadku skargi do WSA na decyzję Prezesa UODO? .....	119
52. Relacje pomiędzy kontrolą/postępowaniem w sprawie naruszenia przepisów o ochronie danych osobowych a postępowaniem cywilnym .....	120
53. Jaka jest rola inspektora ochrony danych w toku kontroli i postępowania w sprawie naruszenia przepisów o ochronie danych osobowych? .....	122
54. Jaka jest rola pełnomocników profesjonalnych w toku kontroli i postępowania w sprawie naruszenia przepisów o ochronie danych osobowych? .....	123
55. Jakiego przepisy znajdują zastosowanie do kontroli i postępowania administracyjnego wszczętych przed 25.05.2018 r.? .....	124
56. Czy organy nadzorcze z poszczególnych państw członkowskich mogą prowadzić wspólne postępowania? .....	127
57. Czy wiadomo u kogo będzie prowadzona kontrola w 2019 roku? .....	128

## **Część III**

### **Jak przygotować się do kontroli?**

#### **Rozdział I**

**Kategorie obowiązków: wymogi bezpośrednie i metawymogi . . . . . 133**

#### **Rozdział II**

**Jak zapewnić i udokumentować zgodność . . . . . 136**

1. Zapewnienie rozliczalności w ramach przygotowania do kontroli – wprowadzenie . . . . . 136
2. Rozliczalność na gruncie ustawy o ochronie danych osobowych z 1997 r. . . . . 138
3. Rozliczalność w RODO . . . . . 139
4. Znaczenie rozliczalności w aspekcie kontroli . . . . . 140
5. Zakres rozliczalności . . . . . 140
6. Realizacja rozliczalności . . . . . 141
7. Inne przykłady realizacji rozliczalności . . . . . 143
8. Dokumentowanie w ramach rozliczalności . . . . . 145
9. Dokumentowanie naruszeń ochrony danych osobowych . . . . . 146
10. Obowiązki dokumentacyjne związane z realizacją obowiązków informacyjnych oraz praw podmiotów danych . . . . . 147
11. Obowiązki dokumentacyjne związane z korzystaniem z podmiotu przetwarzającego . . . . . 148
12. Rejestrowanie czynności przetwarzania . . . . . 150
13. Ocena skutków i uprzednie konsultacje . . . . . 151
14. Inne obowiązki dokumentacyjne . . . . . 152
15. Obowiązki dokumentacyjne w RODO a dotychczasowe dokumenty . . . . . 154
16. Rozliczalność w opiniach i wytycznych Europejskiej Rady Ochrony Danych . . . . . 156
17. Podsumowanie . . . . . 158

#### **Rozdział III**

**Ocena ryzyka . . . . . 159**

1. Ocena ryzyka w RODO . . . . . 159
  - 1.1. Normatywny kontekst analizy ryzyka w RODO (kiedy ocena ryzyka jest wymagana?) . . . . . 159



1.2. Ogólny wymóg monitorowania ryzyka dla praw lub wolności (art. 24 ust. 1 RODO) .....	160
1.3. Ocena ryzyka w fazie projektowania (art. 25 ust. 1 RODO) .....	160
1.4. Ocena ryzyka pod kątem obowiązku prowadzenia rejestru czynności (art. 30 ust. 5 RODO) .....	161
1.5. Ocena ryzyka w ramach oceny środków służących bezpieczeństwu (art. 32 ust. 1–2 RODO) .....	161
1.6. Ocena ryzyka w ramach oceny incydentów bezpieczeństwa danych osobowych pod kątem obowiązku zgłaszania naruszenia ochrony danych osobowych organowi nadzorcemu (art. 33 ust. 1 RODO) .....	162
1.7. Ocena ryzyka w ramach oceny potrzeby zawiadamiania osoby, której dane dotyczą, w przypadku incydentu (art. 34 ust. 1 RODO) .....	162
1.8. Ocena ryzyka w ramach oceny skutków dla ochrony danych osobowych (art. 35 ust. 1 RODO) .....	162
1.9. Ocena ryzyka a funkcjonowanie inspektora ochrony danych (art. 39 ust. 2 RODO) .....	163
1.10. Założenia wstępne .....	164
2. Ramy analizy ryzyka .....	167
2.1. Ryzyko naruszenia praw lub wolności .....	167
2.2. Przykłady ryzyk .....	169
2.3. Etapy oceny ryzyka .....	173
2.4. Zagrożenie a ryzyko .....	176
2.4.1. Waga zagrożenia a waga ryzyka .....	180
2.4.2. Prawdopodobieństwo zagrożenia i prawdopodobieństwo ryzyka .....	182
2.5. Obiektywność oceny .....	186
2.6. Kryteria postępowania z ryzykiem .....	187
2.7. Rola podmiotu przetwarzającego .....	191
3. Ocena skutków dla ochrony danych i uprzednie konsultacje .....	194
3.1. Ocena skutków – wstęp .....	194
3.2. Kiedy ocena skutków może być wymagana? .....	195
3.3. Powiązanie oceny ryzyka i oceny skutków .....	200

3.4. Kiedy należy się konsultować z organem nadzorczym? .....	209
3.5. Elementy dokumentacyjne oceny skutków .....	210
3.6. Ocena ryzyka a inspektor ochrony danych .....	211
4. Podsumowanie .....	212

## **Część IV**

### **Tabele**

Tabela nr 1. Elementy pisemnego upoważnienia dla kontrolującego (zgodnie z art. 81 n.u.o.d.o.) .....	215
Tabela nr 2. Elementy upoważnienia kontrolującego – porównanie nowej ustawy o ochronie danych osobowych i prawa przedsiębiorców .....	217
Tabela nr 3. Kto ma / może być obecny w czasie kontroli? .....	219
Tabela nr 4. Uprawnienia kontrolującego .....	221
Tabela nr 5. Skorelowane obowiązki kontrolowanego .....	227
Tabela nr 6. Wyłączenie kontrolującego (w toku kontroli) a wyłączenie pracownika organu nadzorczego (Prezesa UODO) – porównanie .....	229
Tabela nr 7. Kontrola a czynności sprawdzające w ramach certyfikacji .....	231
Tabela nr 8. Elementy protokołu kontroli (zgodnie z art. 88 ust. 2 n.u.o.d.o.) .....	235
Tabela nr 9. Modyfikacje regulacji Kodeksu postępowania administracyjnego wprowadzone treścią nowej ustawy o ochronie danych osobowych .....	239
Tabela nr 10. Przykładowe zarzuty możliwe do podniesienia w skardze na decyzję administracyjną Prezesa UODO w ramach postępowania dowodowego prowadzonego w sprawie naruszenia przepisów nowej ustawy o ochronie danych osobowych w ramach postępowania administracyjnego .....	251
Tabela nr 11. Wybrane przepisy Kodeksu postępowania administracyjnego istotne z punktu widzenia kwestionowania rozstrzygnięć w postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych .....	253

Tabela nr 12. Środek tymczasowy – przesłanki i porównanie nowej ustawy o ochronie danych osobowych i ustawy o ochronie konkurencji i konsumentów .....	256
Tabela nr 13. Elementy decyzji administracyjnej kończącej postępowanie przed Prezesem UODO w sprawie naruszenia przepisów o ochronie danych osobowych .....	257
Tabela nr 14. Elementy skargi na decyzję/postanowienie Prezesa UODO .....	262
Tabela nr 15. Elementy skargi kasacyjnej od wyroku WSA .....	266
Tabela nr 16. Podstawowe środki ochrony prawnej na etapie kontroli i postępowania w sprawie naruszenia (kwestionowanie czynności lub braku czynności w ramach kontroli i postępowania w sprawie naruszenia przepisów o ochronie danych osobowych) .....	272
Tabela nr 17. Porównanie administratora bezpieczeństwa informacji i inspektora ochrony danych (w aspekcie kontroli i audytu wewnętrznego) .....	276
Tabela nr 18. Przykładowa tabela określająca wymóg i możliwy sposób wdrożenia .....	280
Tabela nr 19. Zestawienie przepisów dotyczących oceny ryzyka .....	308
Tabela nr 20. Ocena operacji pod kątem potrzeby dokonywania oceny skutków (przykład) .....	311
Tabela nr 21. Przykładowy formularz oceny skutków (DPIA) .....	312

## **Część V**

### **Wzory pism**

1. Wzór skargi na decyzję Prezesa UODO w przedmiocie uchylenia zastrzeżenia tajemnicy przedsiębiorstwa wraz z wnioskiem o wstrzymanie wykonalności zaskarżonej decyzji .....
2. Wzór skargi na decyzję Prezesa UODO w przedmiocie stwierdzenia naruszenia i nakazania usunięcia danych osobowych oraz powiadomienia o tym odbiorców, których dane ujawniono .....
3. Wzór skargi na decyzję Prezesa UODO w przedmiocie stwierdzenia naruszenia i nałożenia administracyjnej kary pieniężnej .....

---

4. Wzór wniosku o odroczenie terminu uiszczenia administracyjnej kary pieniężnej ze względu na ważny interes wnioskodawcy .....	333
5. Wzór skargi na postanowienie Prezesa UODO w przedmiocie odmowy odroczenia terminu uiszczenia administracyjnej kary pieniężnej .....	336
6. Wzór skargi na postanowienie Prezesa UODO w przedmiocie ograniczenia przetwarzania danych osobowych .....	339
7. Wzór skargi na decyzję Prezesa UODO w przedmiocie wymierzenia kary grzywny w wysokości 5000 zł stosownie do art. 69 n.u.o.d.o. ....	342
8. Wzór zastrzeżeń do protokołu kontroli .....	345
9. Wzór skargi na decyzję Prezesa UODO w przedmiocie odmowy udzielenia akredytacji .....	348
10. Wzór skargi na decyzję Prezesa UODO w przedmiocie cofnięcia akredytacji .....	351
11. Wzór skargi na decyzję Prezesa UODO w przedmiocie odmowy dokonania certyfikacji .....	354
12. Wzór skargi na decyzję Prezesa UODO w przedmiocie cofnięcia certyfikacji .....	357
13. Wzór skargi na decyzję Prezesa UODO w przedmiocie odmowy zatwierdzenia wiążących reguł korporacyjnych .....	359
14. Wzór skargi na decyzję Prezesa UODO w przedmiocie odmowy udzielenia zezwolenia, o którym mowa w art. 46 ust. 3 RODO .....	362
15. Wzór skargi kasacyjnej od wyroku WSA .....	364
<b>Bibliografia</b> .....	371



# WYKAZ SKRÓTÓW

## Akty prawne

- dyrektywa 95/46** – dyrektywa 95/46/WE 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, ze zm.)
- k.c.** – ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2018 r. 1025 ze zm.)
- k.k.** – ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2018 r. poz. 1600 ze zm.)
- k.p.a.** – ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2018 r. poz. 2096)
- n.u.o.d.o.** – ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. poz. 1000 ze zm.)
- o.p.** – ustawa z 29.08.1997 r. – Ordynacja podatkowa (Dz.U. z 2018 r. poz. 800 ze zm.)
- p.p.s.a.** – ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2018 r. poz. 1302 ze zm.)
- pr. przed.** – ustawa z 6.03.2018 r. – Prawo przedsiębiorców (Dz.U. 646 ze zm.)
- r.w.s.z.p.** – rozporządzenie Rady Ministrów z 16.12.2003 r. w sprawie wysokości oraz szczegółowych zasad pobierania wpisu w postępowaniu przed sądami administracyjnymi (Dz.U. Nr 221, poz. 2193 ze zm.)
- 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, ze zm.)
<b>u.f.p.</b>	– ustawa z 27.08.2009 r. o finansach publicznych (Dz.U. z 2017 r. poz. 2077 ze zm.)
<b>u.i.d.p.</b>	– ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 ze zm.)
<b>u.o.d.o.</b>	– ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.)
<b>u.o.k.k.</b>	– ustawa z 16.02.2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2018 r. poz. 798 ze zm.)
<b>u.s.d.g.</b>	– ustawa z 2.07.2004 r. o swobodzie działalności gospodarczej (Dz.U. z 2017 r. poz. 2168 ze zm.) – uchylona

## Inne

<b>CNIL</b>	– Commission Nationale de l’Informatique et des Libertés
<b>ENISA</b>	– Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (EU Agency for Network and Information Security)
<b>EROD</b>	– Europejska Rada Ochrony Danych; dawniej Grupa Robocza Art. 29
<b>GIODO</b>	– Generalny Inspektor Ochrony Danych Osobowych
<b>ICO</b>	– International Commissioner’s Office
<b>IOD</b>	– inspektor ochrony danych
<b>NSA</b>	– Naczelny Sąd Administracyjny
<b>ONSAiWSA</b>	– Orzecznictwo Naczelnego Sądu Administracyjnego i Wojewódzkich Sądów Administracyjnych
<b>Prezes UODO</b>	– Prezes Urzędu Ochrony Danych Osobowych (także jako Prezes Urzędu)
<b>UODO</b>	– Urząd Ochrony Danych Osobowych
<b>WSA</b>	– wojewódzki sąd administracyjny

## 23. Jak długo może być prowadzona kontrola?

Zgodnie z art. 89 n.u.o.d.o.:

„1. Kontrolę prowadzi się nie dłużej niż 30 dni od dnia okazania kontrolowanemu lub innej osobie wskazanej w przepisach imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość. Do terminu nie wlicza się terminów przewidzianych na zgłoszenie zastrzeżeń do protokołu kontroli lub podpisanie i doręczenie protokołu kontroli przez kontrolowanego.

2. Terminem zakończenia kontroli jest dzień podpisania protokołu kontroli przez kontrolowanego albo dzień dokonania wzmianki, o której mowa w art. 88 ust. 8”.

Powyższe oznacza, że niezależnie od terminów kontroli wpisanych w imiennym upoważnieniu do kontroli (art. 81 n.u.o.d.o.) nie powinna ona trwać dłużej niż 30 dni od dnia okazania kontrolowanemu lub innej osobie wskazanej w przepisach imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość.



Uwaga!

Artykuł 55 pr. przed. określa maksymalne terminy trwania kontroli w jednym roku kalendarzowym.

W przepisach nie określono skutków przekroczenia maksymalnego terminu trwania kontroli. Jak wskazuje się w doktrynie, stosując wnioskowanie *per analogiam* z regulacji Kodeksu postępowania administracyjnego, wypada stwierdzić, że wskazany termin ma charakter procesowy, a wobec tego jego upływ nie pozbawia kontrolującego prawa do prowadzenia postępowania. Nie są to bowiem terminy prawa materialnego, które powodowałyby pozbawienie organu kompetencji do prowadzenia postępowania kontrolnego. Oznacza to w praktyce, że poczynione ustalenia oraz zebrane dowody w okresie następującym po przekroczeniu maksymalnego terminu kontroli nadal stanowią ważną podstawę dla dokonania ustaleń faktycznych w sprawie oraz wszczęcia



ewentualnego postępowania administracyjnego w przedmiocie naruszenia przepisów o ochronie danych osobowych. Niewątpliwie jednak przekroczenie przez kontrolujących wymiarów czasowych określonych art. 89 n.u.o.d.o. stanowi zachowanie naruszające prawo, które może stać się podstawą odpowiedzialności odszkodowawczej administracji publicznej na podstawie przepisów art. 417 k.c. Ponadto tego rodzaju postępowanie kontrolujących może stać się podstawą dla aktualizacji wobec nich odpowiedzialności dyscyplinarnej<sup>43</sup>.

## 24. Kto prowadzi kontrolę?

Zgodnie z art. 79 ust. 1 n.u.o.d.o. kontrolę przeprowadza upoważniony przez Prezesa Urzędu:

- pracownik Urzędu,
- członek lub pracownik organu nadzorczego państwa członkowskiego Unii Europejskiej w przypadku, o którym mowa w art. 62 RODO.

Jak się wskazuje w piśmiennictwie, brak jest podstawy prowadzenia kontroli osobiście przez Prezesa Urzędu lub jego zastępcę<sup>44</sup>.

Zob. pytanie 25 poniżej oraz część IV, tabela nr 3.

## 25. Kto może brać udział w kontroli? Czy można prowadzić kontrolę pod nieobecność kontrolowanego?

Osoby prowadzące kontrolę wskazane w pytaniu 24 powyżej to rzecz jasna nie jedyne osoby biorące udział w kontroli. Uczestników kontroli możemy przy tym podzielić na:

- obligatoryjnych – oprócz osób prowadzących kontrolę będą to:

<sup>43</sup> P. Gorzko [w:] *Ustawa...*, red. M. Gumularz, K. Koziół, P. Kozik, s. 419.

<sup>44</sup> P. Litwiński [w:] P. Litwiński, P. Barta, D. Dörre-Kolasa, *Ustawa...*, s. 212.

- kontrolowany lub osoba przez niego upoważniona (art. 83 n.u.o.d.o.), z zastrzeżeniem ust. 3 tego przepisu, zgodnie z którym w razie nieobecności kontrolowanego lub osoby przez niego upoważnionej upoważnienie do przeprowadzenia kontroli oraz legitymacja służbowa lub dokument potwierdzający tożsamość mogą być okazane:
  - 1) osobie czynnej w lokalu przedsiębiorstwa w rozumieniu art. 97 k.c. lub
  - 2) przywołanemu świadkowi, jeżeli jest funkcjonariuszem publicznym w rozumieniu art. 115 § 13 k.k., niebędącemu pracownikiem Urzędu albo osobą, o której mowa w art. 80 ust. 1 n.u.o.d.o.

Jak wskazuje P. Gorzko, pomimo że ustawodawca mówi jedynie o okazaniu dokumentów, należy wnioskować, że ustawodawca dopuścił możliwość wykonywania czynności kontrolnych w obecności innego pracownika kontrolowanego lub przywołanego świadka, tj. prowadzenia kontroli pomimo nieobecności kontrolowanego przedsiębiorcy lub osoby upoważnionej do reprezentowania przedsiębiorcy w trakcie kontroli, jako wyjątek od zasady ustanowionej w art. 83 ust. 1 n.u.o.d.o.<sup>45</sup>;

- fakultatywnych:
  - osoba posiadająca wiedzę specjalistyczną – zgodnie z art. 82 ust. 1 n.u.o.d.o. Prezes Urzędu może upoważnić do udziału w kontroli osobę posiadającą wiedzę specjalistyczną, jeżeli przeprowadzenie czynności kontrolnych wymaga takiej wiedzy (osoba ta powinna mieć upoważnienie takie jak kontrolujący, w upoważnieniu określa się zakres jej uprawnień). Upoważnienie do udziału w kontroli nie daje możliwości prowadzenia kontroli;
  - Policja – zgodnie z art. 85 ust. 1 n.u.o.d.o. Prezes Urzędu lub kontrolujący może zwrócić się do właściwego miejscowo komendanta Policji o pomoc, jeżeli jest to niezbędne do wykonywania czynności kontrolnych.

Zob. część IV, tabela nr 3.

<sup>45</sup> P. Gorzko [w:] *Ustawa...*, red. M. Gumularz, K. Koziół, P. Kozik, s. 399.

## 26. Czy sektor publiczny objęty jest także kontrolą?

RODO co do zasady ma zastosowanie do wszystkich branż oraz do sektorów prywatnego i publicznego. Organy administracji publicznej podlegają przepisom RODO, jeżeli przetwarzają dane osobowe dotyczące osób fizycznych (administrator danych na gruncie RODO oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych). Jak wskazuje się w doktrynie, zakres podmiotowy kontroli będzie wyznaczany przez krąg podmiotów, do których przepisy o ochronie danych osobowych znajdują zastosowanie (adresatów ich norm). Jeżeli RODO stosuje się do podmiotów nie tylko z sektora prywatnego, lecz także publicznego, podmioty z tego sektora będą mogły być objęte kontrolą (brak jakichkolwiek wyłączeń lub ograniczeń w tym zakresie; odnośnie do ograniczeń w zakresie kar nakładanych na podmioty publiczne ustanowionych w przepisach nowej ustawy o ochronie danych osobowych na mocy art. 83 ust. 7 RODO zob. pytanie 45 poniżej). Wynika z tego, że w praktyce kontrola może być wykonywana zarówno w ministerstwie, urzędzie miasta, gminnym ośrodku pomocy społecznej, publicznej szkole, jak i w niepublicznym przedszkolu, prywatnej klinice, banku, spółdzielni, kancelarii radcowskiej czy u osoby prowadzącej biuro rachunkowe<sup>46</sup>.

## 27. Czy można prowadzić kontrolę u procesora (podmiotu przetwarzającego)?

Uprawnienia kontrolne mogą być wykonywane w stosunku do administratora danych osobowych<sup>47</sup>, ale także w odniesieniu do podmiotu przetwarzającego, tzw. procesora (niezależnie od możliwości

---

<sup>46</sup> M. Sakowska-Baryła, *Kontrolowanie przez GIODO przetwarzania danych osobowych – przestrzeganie przepisów o ochronie danych osobowych*, <http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-ee69c7aa-a3c3-4bda-880e-ad6cd30fb9a9> (dostęp: 1.01.2019 r.).

<sup>47</sup> Jeżeli chodzi o współadministrowanie w rozumieniu art. 26 RODO – w odniesieniu do każdego ze współadministrujących danymi administratorów.

audytowania go przez administratora danych w związku z powierzeniem mu danych osobowych do przetwarzania na podstawie art. 28 ust. 3 lit. h RODO). Inaczej niż pod rządami uchylonej ustawy o ochronie danych osobowych, przepisy o kontroli stosuje się do podmiotu przetwarzającego wprost, nie zaś odpowiednio.

Przepisy RODO przewidują dwie kategorie obowiązków ciążących na procesorze w związku z przetwarzaniem powierzonych danych osobowych. Pierwsza kategoria obejmuje obowiązki procesora, które powinny wynikać z umowy powierzenia zawartej z administratorem (art. 28 RODO). Do drugiej kategorii zaliczyć można samodzielne obowiązki procesora, tj. te, których bezpośrednim źródłem są przepisy RODO. Należą do niej będą następujące obowiązki:

- wyznaczenie przedstawiciela w UE, jeśli jest to niezbędne (art. 27 RODO),
- niekorzystanie z usług innego podmiotu przetwarzającego bez zgody administratora (art. 28 ust. 2 RODO),
- przetwarzanie danych wyłącznie na polecenie administratora (art. 29 RODO),
- prowadzenie rejestru kategorii czynności przetwarzania dokonywanych w imieniu administratora (art. 30 ust. 2 RODO),
- współpraca z organem nadzorczym (art. 31 RODO),
- zapewnienie bezpieczeństwa przetwarzania (32 RODO),
- niezwłoczne zgłaszanie administratorowi naruszenia ochrony danych osobowych (art. 33 ust. 2 RODO),
- powołanie inspektora ochrony danych (art. 37 ust. 1 RODO).

Z art. 83 ust. 4 RODO wynika, że administracyjnej karze pieniężnej podlega naruszenie – przez administratora i procesora – m.in. obowiązków wynikających z art. 8, 11, 25–39 oraz 42 i 43 RODO<sup>48</sup>.

Prowadzenie kontroli u procesora nie wyłącza kontroli u administratora, który powierzył mu dane do przetwarzania (i na odwrót).

---

<sup>48</sup> Zob. także art. 58 ust. 2 oraz art. 83 ust. 2 RODO, które także odnoszą się do odpowiedzialności administratora i procesora. Co więcej, art. 28 ust. 10 RODO stanowi, że bez uszczerbku dla art. 82, 83 i 84, jeżeli podmiot przetwarzający naruszy rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

## 28. Jakie uprawnienia ma kontrolujący?

Zakres uprawnień kontrolującego jest wyczerpująco wskazany w art. 84–86 n.u.o.d.o. Ma on charakter katalogu zamkniętego, co oznacza, że kontrolujący może realizować wyłącznie uprawnienia w nim wskazane. Kontrolujący ma prawo:

- 1) wstępu w godzinach od 6:00 do 22:00 na grunt oraz do budynków, lokali lub innych pomieszczeń;
- 2) wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;
- 3) przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
- 4) żądania złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwania w charakterze świadka w zakresie niezbędnym do ustalenia stanu faktycznego;
- 5) zlecenia sporządzania ekspertyz i opinii.

Zob. szerzej część IV, tabela nr 4.

## 29. Jaka jest rola osoby, której dane dotyczą, w ramach kontroli i postępowania?

Jak zostało już wyżej wskazane, jednym z rodzajów kontroli przeprowadzanej przez Prezesa Urzędu jest kontrola doraźna, która (w przeciwieństwie do kontroli planowej) jest wszczynana w wyniku uzyskania informacji stanowiących podstawę do jej przeprowadzenia. Tego rodzaju informacje mogą pochodzić ze źródeł powszechnie dostępnych (np. z prasy) lub od osób zainteresowanych (podmiotów danych i innych osób, które poinformują organ nadzorczy o nieprawidłowościach związanych z przetwarzaniem danych). Najbardziej typowym impulsem do przeprowadzenia kontroli jest skarga osoby, której dane dotyczą, na administratora, który przetwarza jej dane, naruszając – w ocenie tej osoby – jej prawa wynikające z przepisów o ochronie danych osobowych<sup>49</sup>.

---

<sup>49</sup> P. Fajgielski, *Ogólne...*, s. 845.

**Mirosław Gumularz** – radca prawny, doktor nauk prawnych. Jako doradca społeczny ds. ochrony danych osobowych w Ministerstwie Cyfryzacji brał udział w pracach nad wdrożeniem RODO do polskiego porządku prawnego; członek Grupy Roboczej ds. Ochrony Danych Osobowych przy Ministerstwie Cyfryzacji; audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji według normy ISO 27001:2013; autor oraz współautor licznych publikacji z zakresu ochrony danych osobowych oraz nowych technologii.

**Patrycja Kozik** – radca prawny, doktorantka w Katedrze Prawa Europejskiego na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego; audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji według normy ISO 27001:2013; wykładowca na studiach podyplomowych z zakresu ochrony danych osobowych organizowanych przez Uniwersytet Marii Curie-Skłodowskiej w Lublinie, autorka licznych publikacji z zakresu szeroko pojętego prawa nowych technologii.

Książka zawiera odpowiedzi na kluczowe pytania związane z kontrolą i postępowaniem w sprawie naruszenia przepisów o ochronie danych osobowych, w tym m.in.:

- jakie podmioty mogą być kontrolowane,
- jakie są prawa i obowiązki podmiotów kontrolowanych,
- jakie relacje zachodzą między kontrolą a postępowaniem administracyjnym.

Ponadto w publikacji omówiono, jak administrator ochrony danych osobowych powinien przygotować się do kontroli, w tym jak ma wykazać zapewnienie zgodności z przepisami i obowiązkami dokumentacyjnymi wynikającymi z RODO.

Opracowanie zawiera także:

- wzory dokumentów istotnych dla administratorów danych i podmiotów przetwarzających zarówno na etapie kontroli, jak i postępowania w sprawie naruszenia przepisów o ochronie danych,
- wzory skarg na decyzje i postanowienia wydawane przez Prezesa Urzędu Ochrony Danych Osobowych na gruncie ustawy o ochronie danych osobowych.

Publikacja jest przeznaczona dla adwokatów, radców prawnych, a także administratorów, podmiotów przetwarzających i inspektorów ochrony danych. Będzie przydatna pracownikom administracji rządowej i samorządowej oraz przedsiębiorcom przetwarzającym dane osobowe.



**ZAMÓWIENIA:**

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

ISBN 978-83-8160-395-9



CENA 119 Zł (W TYM 5% VAT)