

OCHRONA DANYCH OSOBYCH

Kontrola i postępowanie w sprawie naruszenia przepisów

Poradnik ze wzorami

Mirostaw Gumularz, Patrycja Kozik

EDYTOWALNE WZORY
NA STRONIE INTERNETOWEJ

WYDANIE

2

OCHRONA DANYCH OSOBYCH

Kontrola i postępowanie w sprawie naruszenia przepisów

Poradnik ze wzorami

Mirosław Gumularz, Patrycja Kozik

Zamów książkę w księgarni internetowej

proinfo.pl
księgarnia internetowa

WYDANIE

2

Materiały uzupełniające na stronie:
[www.ochrona-danych-osobowych-naruszenia-
przepisow.wolterskluwer.pl](http://www.ochrona-danych-osobowych-naruszenia-przepisow.wolterskluwer.pl)
będą dostępne do 30 czerwca 2024 r.

W razie problemów
ze znalezieniem zdrapki
z kodem aktywacyjnym
prosimy o kontakt
tel. 801 04 45 45

PIKTOGRAMY

wskazują ważne elementy
książki i ułatwiają
ich odnalezienie



Ważne



Przykłady



Podstawa prawna
Kontekst prawny



Pytania
Zadania



Rozwiązania
Odpowiedzi



Stanowisko stron
Pogląd



Orzecnictwo



Literatura



Historia



Nowe przepisy



Wiadomości dodatkowe



Informacje powiązane
Odesłanie

Stan prawny na 1 marca 2022 r.

Wydawca
Monika Pawłowska

Redaktor prowadzący
Livia Śpiewak

Opracowanie redakcyjne
Violet Design Wioletta Kowalska

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

prawoLubni

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegając przystępujących 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.

Szanujmy prawo i własność
Więcej na www.legalnakultura.pl
Polska Izba Książki

© Copyright by Wolters Kluwer Polska Sp. z o.o., 2022

ISBN 978-83-8286-233-1
2. wydanie

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 728 313 462
e-mail: PL-ksiazki@wolterskluger.com

księgarnia internetowa 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	21
2. Dane osobowe podane, zaobserwowane, pochodne oraz wywnioskowane	23
3. Dane uporządkowane oraz nieuporządkowane	26
3.1. Ogólne informacje	26
3.2. Uporządkowanie a ustrukturyzowanie	32
4. Dane identyfikowalne oraz nieidentyfikowalne	33
4.1. Dwie normy wynikające z art. 11 RODO	33
4.2. Artykuł 11 RODO a definicja danych osobowych	34
4.3. Krótkotrwałe i długotrwałe przetwarzanie danych	45

Część II

Pytania i odpowiedzi

1. Czym jest RODO?	49
2. Jakie sankcje administracyjne i karne mogą grozić za naruszenie RODO?	50
3. Czy administracyjne kary pieniężne mogą być nakładane tylko za naruszenie RODO?	54
4. Jakich kategorii danych dotyczy kontrola/postępowanie?	56
5. Kiedy przepisy RODO nie będą miały zastosowania?	61

6. Jakie inne przepisy dotyczące ochrony danych osobowych mogą mieć zastosowanie?	65
7. Czy przepisy implementujące dyrektywę policyjną przewidują możliwość przeprowadzenia kontroli przez Prezesa UODO?	66
8. Czy można otrzymać administracyjną karę pieniężną za naruszenie przepisów implementujących dyrektywę policyjną?	67
9. Jakie sankcje karne mogą grozić za naruszenie przepisów implementujących dyrektywę policyjną?	68
10. Jakie podmioty podlegają kontroli/mogą być adresatem decyzji w ramach postępowania w sprawie naruszenia przepisów o ochronie danych osobowych?	68
11. Jak należy rozumieć pojęcie kontroli?	70
12. Kiedy prowadzona jest kontrola, a kiedy prowadzi się postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych?	71
13. Czy do kontroli uzupełniającej stosuje się przepisy Kodeksu postępowania administracyjnego (w tym przepisy gwarancyjne)?	78
14. Jaka jest relacja pomiędzy przepisami o kontroli w RODO a przepisami prawa przedsiębiorców?	81
15. Czy przepisy RODO utrudniają walkę z pandemią COVID-19 i jako takie nie powinny być podczas niej stosowane?	84
16. Czy pandemia koronawirusa zmieniła sposób prowadzenia kontroli?	85
17. Czy pandemia koronawirusa wpłynęła na bieg terminów w toczących się postępowaniach?	87
18. Jakie podmioty kontrolował Prezes UODO w ubiegłych latach?	90
19. Jak należy rozumieć pojęcie naruszenia przepisów o ochronie danych osobowych?	93
20. Jakie są tryby kontroli? Czy kontrole mogą być niezapowiedziane?	94
21. Jakie są obowiązki kontrolowanego w trakcie kontroli i co grozi za ich naruszenie?	98
22. Czy można otrzymać administracyjną karę pieniężną za samo udaremnianie lub utrudnianie kontroli?	100
23. Czy nałożenie administracyjnej kary pieniężnej za udaremnianie lub utrudnianie kontroli wyklucza możliwość nałożenia takiej kary także za naruszenie innych przepisów RODO?	103

24. Czy można kwestionować wszczęcie kontroli lub inne czynności w toku kontroli?	104
25. Czy można kwestionować wszczęcie postępowania administracyjnego lub inne czynności w jego toku?	105
26. Jaka jest relacja zasady rozliczalności do obowiązku zebrania materiału dowodowego przez organ nadzorczy (art. 77 k.p.a.)?	107
27. Jak ustalić moment wszczęcia postępowania administracyjnego?	111
28. Jakie dokumenty inicjują kontrolę?	112
29. Czy i jak chroniona jest tajemnica przedsiębiorstwa?	114
30. Czy i w jakim zakresie Prezes UODO może mieć dostęp do tajemnic prawnie chronionych w toku kontroli i postępowania administracyjnego?	118
31. Jakie są konsekwencje naruszenia wymogów co do treści upoważnienia do kontroli?	119
32. Czy kontrola może być realizowana wyłącznie w zakresie upoważnienia?	120
33. Czy pracownicy kontrolowanego administratora/podmiotu przetwarzającego podlegają kontroli?	121
34. Czy można odpowiadać dyscyplinarnie za naruszenia przepisów dotyczących ochrony danych osobowych?	122
35. Jak długo może być prowadzona kontrola?	124
36. Kto prowadzi kontrolę?	126
37. Kto może brać udział w kontroli? Czy można prowadzić kontrolę pod nieobecność kontrolowanego?	126
38. Czy sektor publiczny objęty jest także kontrolą?	127
39. Czy można prowadzić kontrolę u procesora (podmiotu przetwarzającego)?	128
40. Jakie uprawnienia ma kontrolujący?	129
41. Jakie uprawnienia kontrolującego przewidują przepisy wdrażające dyrektywę policyjną?	130
42. Jaka jest rola osoby, której dane dotyczą, w ramach kontroli i postępowania?	131
43. W jaki formalny sposób dochodzi do zakończenia kontroli?	134
44. W jaki sposób można kwestionować treść protokołu kontroli?	137
45. Czy protokół kontroli i materiał dowodowy kontroli stają się automatycznie częścią materiału dowodowego w postępowaniu administracyjnym?	138

46. Czy czynności w toku kontroli są utrwalane jedynie w protokole?	139
47. Czy wadliwość czynności w toku kontroli może mieć wpływ na postępowanie administracyjne?	140
48. Kto jest stroną w postępowaniu administracyjnym?	141
49. Kiedy postępowanie administracyjne może być umorzone?	142
50. Jakie są rodzaje rozstrzygnięć co do istoty sprawy w ramach postępowania w przedmiocie naruszenia przepisów o ochronie danych osobowych?	144
51. Jakie są uprawnienia Prezesa UODO na gruncie ustawy wdrażającej dyrektywę policyjną?	146
52. Co grozi za brak wykonania decyzji Prezesa UODO?	148
53. Jakie są skutki doręczenia decyzji Prezesa UODO?	149
54. Jaki środek przysługuje w postępowaniu administracyjnym w przypadku niezalatwienia sprawy w terminie?	149
55. Czy decyzja Prezesa UODO w postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych jest natychmiastowo wykonalna?	151
56. Jak można kwestionować (skarżyć) decyzję Prezesa UODO?	152
57. Czy niekorzystny wyrok WSA można zakwestionować?	155
58. Czy do postępowania w sprawie naruszenia przepisów o ochronie danych osobowych stosuje się reguły dotyczące milczącego załatwienia sprawy?	156
59. Jakie są podstawy wyłączenia kontrolera/pracownika organu prowadzącego postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych?	156
60. Jakie są administracyjne kary pieniężne w sektorze prywatnym, a jakie w sektorze publicznym?	157
61. Jakie są kryteria miarkowania kary w ramach decyzji kończącej postępowanie?	159
62. Jak Prezes UODO ustala podstawę wymiaru administracyjnej kary pieniężnej?	162
63. Czy można nałożyć karę pieniężną bez postępowania/decyzji?	163
64. Czy administracyjne kary pieniężne ulegają przedawnieniu?	164
65. W jakim terminie należy zapłacić karę?	165
66. Czy można starać się o rozłożenie kary na raty, odroczenie terminu płatności lub o ulgę w jej wykonaniu?	166

67. Jaka jest wysokość opłaty w przypadku skargi do WSA na decyzję Prezesa UODO?	167
68. Relacje pomiędzy kontrolą/postępowaniem w sprawie naruszenia przepisów o ochronie danych osobowych a postępowaniem cywilnym	168
69. Jaka jest rola inspektora ochrony danych w toku kontroli i postępowania w sprawie naruszenia przepisów o ochronie danych osobowych?	170
70. Jaka jest rola inspektora ochrony danych na gruncie przepisów wdrażających dyrektywę policyjną?	171
71. Jaka jest rola pełnomocników profesjonalnych w toku kontroli i postępowania w sprawie naruszenia przepisów o ochronie danych osobowych?	172
72. Jakie przepisy znajdują zastosowanie do kontroli i postępowania administracyjnego wszczętych przed 25.05.2018 r.?	173
73. Czy organy nadzorcze z poszczególnych państw członkowskich mogą prowadzić wspólne postępowania?	176
74. Jakie podmioty były ujęte w dotychczasowych planach kontroli?	177
75. Jakie podmioty są ujęte w planie kontroli na 2022 r.?	180

Część III

Jak przygotować się do kontroli?

Rozdział I

Kategorie obowiązków: wymogi bezpośrednie i metawymogi	183
---	------------

Rozdział II

Jak zapewnić i udokumentować zgodność?	187
1. Zapewnienie rozliczalności w ramach przygotowania do kontroli – wprowadzenie	187
2. Rozliczalność na gruncie ustawy o ochronie danych osobowych z 1997 r.	189
3. Rozliczalność w RODO	190
4. Znaczenie rozliczalności w aspekcie kontroli	191
5. Zakres rozliczalności	191
6. Realizacja rozliczalności	192
7. Inne przykłady realizacji rozliczalności	193

8. Dokumentowanie w ramach rozliczalności	195
9. Dokumentowanie naruszeń ochrony danych osobowych	196
10. Obowiązki dokumentacyjne związane z realizacją obowiązków informacyjnych oraz praw podmiotów danych	198
11. Obowiązki dokumentacyjne związane z korzystaniem z podmiotu przetwarzającego	199
12. Rejestrowanie czynności przetwarzania	200
13. Ocena skutków i uprzednie konsultacje	202
14. Inne obowiązki dokumentacyjne	203
15. Obowiązki dokumentacyjne w RODO a dotychczasowe dokumenty	204
16. Rozliczalność w opiniach i wytycznych Europejskiej Rady Ochrony Danych	206
17. Podsumowanie	208

Rozdział III

Ocena ryzyka	209
1. Ocena ryzyka w RODO	209
1.1. Normatywny kontekst analizy ryzyka w RODO (kiedy ocena ryzyka jest wymagana?)	209
1.2. Ogólny wymóg monitorowania ryzyka dla praw lub wolności (art. 24 ust. 1 RODO)	210
1.3. Ocena ryzyka w fazie projektowania (art. 25 ust. 1 RODO)	210
1.4. Ocena ryzyka pod kątem obowiązku prowadzenia rejestrów czynności (art. 30 ust. 5 RODO)	211
1.5. Ocena ryzyka w ramach oceny środków służących bezpieczeństwu (art. 32 ust. 1–2 RODO)	211
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)	212
1.7. Ocena ryzyka w ramach oceny potrzeby zawiadomienia osoby, której dane dotyczą, w przypadku incydentu (art. 34 ust. 1 RODO)	212
1.8. Ocena ryzyka w ramach oceny skutków dla ochrony danych osobowych (art. 35 ust. 1 RODO)	212

1.9. Ocena ryzyka a funkcjonowanie inspektora ochrony danych (art. 39 ust. 2 RODO)	213
1.10. Założenia wstępne	214
2. Ramy analizy ryzyka	217
2.1. Ryzyko naruszenia praw lub wolności	217
2.2. Przykłady ryzyk	218
2.3. Etapy oceny ryzyka	223
2.4. Zagrożenie a ryzyko	225
2.4.1. Waga zagrożenia a waga ryzyka	229
2.4.2. Prawdopodobieństwo zagrożenia i prawdopodobieństwo ryzyka	231
2.5. Obiektywność oceny	236
2.6. Kryteria postępowania z ryzykiem	236
2.7. Rola podmiotu przetwarzającego	240
3. Ocena skutków dla ochrony danych i uprzednie konsultacje	242
3.1. Ocena skutków – wstęp	242
3.2. Kiedy ocena skutków może być wymagana?	243
3.3. Powiązanie oceny ryzyka i oceny skutków	248
3.4. Kiedy należy się konsultować z organem nadzorczym?	251
3.5. Elementy dokumentacyjne oceny skutków	252
3.6. Ocena ryzyka a inspektor ochrony danych	253
4. Podsumowanie	253

Część IV

Tabele

Tabela nr 1. Elementy pisemnego upoważnienia dla kontrolującego (zgodnie z art. 81 u.o.d.o.)	257
Tabela nr 2. Elementy upoważnienia kontrolującego – porównanie ustawy o ochronie danych osobowych i Prawa przedsiębiorców	259
Tabela nr 3. Kto ma/może być obecny w czasie kontroli?	260
Tabela nr 4. Uprawnienia kontrolującego	263
Tabela nr 5. Skorelowane obowiązki kontrolowanego	270
Tabela nr 6. Wyłączenie kontrolującego (w toku kontroli) a wyłączenie pracownika organu nadzorczego (Prezesa UODO) – porównanie	271

Tabela nr 7. Kontrola a czynności sprawdzające w ramach certyfikacji	274
Tabela nr 8. Elementy protokołu kontroli (zgodnie z art. 88 ust. 2 u.o.d.o.)	278
Tabela nr 9. Modyfikacje regulacji Kodeksu postępowania administracyjnego wprowadzone przez ustawę o ochronie danych osobowych	281
Tabela nr 10. Przykładowe zarzuty możliwe do podniesienia w skardze na decyzję administracyjną Prezesa UODO w ramach postępowania dowodowego prowadzonego w sprawie naruszenia przepisów ustawy o ochronie danych osobowych w ramach postępowania administracyjnego	295
Tabela nr 11. Wybrane przepisy Kodeksu postępowania administracyjnego istotne z punktu widzenia kwestionowania rozstrzygnięć w postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych	296
Tabela nr 12. Środek tymczasowy – przesłanki i porównanie ustawy o ochronie danych osobowych i ustawy o ochronie konkurencji i konsumentów	300
Tabela nr 13. Elementy decyzji administracyjnej kończącej postępowanie przed Prezesem UODO w sprawie naruszenia przepisów o ochronie danych osobowych	302
Tabela nr 14. Elementy skargi na decyzję/postanowienie Prezesa UODO	307
Tabela nr 15. Elementy skargi kasacyjnej od wyroku WSA	312
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)	319
Tabela nr 17. Porównanie administratora bezpieczeństwa informacji i inspektora ochrony danych (w aspekcie kontroli i audytu wewnętrznego)	324
Tabela nr 18. Przykładowa tabela określająca wymóg i możliwy sposób wdrożenia	328
Tabela nr 19. Zestawienie przepisów dotyczących oceny ryzyka	361
Tabela nr 20. Ocena operacji pod kątem potrzeby dokonywania oceny skutków (przykład)	364

Tabela nr 21. Przykładowy formularz oceny skutków (DPIA)	365
Tabela nr 22. Kontrola RODO a DODO – różnice wynikające z wyłączeń na gruncie art. 6 u.o.d.z.p.	370

Część V

Wzory pism

1. Wzór skargi na decyzję Prezesa UODO w przedmiocie uchylecia zastrzeżenia tajemnicy przedsiębiorstwa wraz z wnioskiem o wstrzymanie wykonalności zaskarżonej decyzji	375
2. Wzór skargi na decyzję Prezesa UODO w przedmiocie stwierdzenia naruszenia i nakazania usunięcia danych osobowych oraz powiadomienia o tym odbiorców, których dane ujawniono	382
3. Wzór skargi na decyzję Prezesa UODO w przedmiocie stwierdzenia naruszenia i nałożenia administracyjnej kary pieniężnej	386
4. Wzór wniosku o odroczenie terminu uiszczenia administracyjnej kary pieniężnej ze względu na ważny interes wnioskodawcy	389
5. Wzór skargi na postanowienie Prezesa UODO w przedmiocie odmowy odroczenia terminu uiszczenia administracyjnej kary pieniężnej	392
6. Wzór skargi na postanowienie Prezesa UODO w przedmiocie ograniczenia przetwarzania danych osobowych	394
7. Wzór skargi na decyzję Prezesa UODO w przedmiocie wymierzenia kary grzywny w wysokości 5000 zł stosownie do art. 69 u.o.d.o.	396
8. Wzór zastrzeżeń do protokołu kontroli	399
9. Wzór skargi na decyzję Prezesa UODO w przedmiocie odmowy udzielenia akredytacji	401
10. Wzór skargi na decyzję Prezesa UODO w przedmiocie cofnięcia akredytacji	403
11. Wzór skargi na decyzję Prezesa UODO w przedmiocie odmowy dokonania certyfikacji	405
12. Wzór skargi na decyzję Prezesa UODO w przedmiocie cofnięcia certyfikacji	407

13. Wzór skargi na decyzję Prezesa UODO w przedmiocie odmowy zatwierdzenia wiążących reguł korporacyjnych	409
14. Wzór skargi na decyzję Prezesa UODO w przedmiocie odmowy udzielenia zezwolenia, o którym mowa w art. 46 ust. 3 RODO	411
15. Wzór skargi kasacyjnej od wyroku WSA	413
Bibliografia	419

Część I

**PODZIAŁY DANYCH OSOBOWYCH
OBJĘTYCH KONTROLĄ**

1. Dane osobowe wrażliwe (szczególne kategorie danych), dane o karalności oraz dane osobowe zwykłe



Przepisy RODO wyróżniają następujące kategorie danych osobowych:


- 1) szczególne kategorie danych osobowych;
- 2) dane osobowe dotyczące wyroków skazujących i czynów zabronionych;
- 3) inne kategorie danych osobowych (dane osobowe zwykłe).



Szczególne kategorie danych osobowych w rozumieniu RODO to dane osobowe:

- 1) ujawniające pochodzenie rasowe lub etniczne;
- 2) ujawniające poglądy polityczne;
- 3) ujawniające przekonania religijne lub światopoglądowe;
- 4) ujawniające przynależność do związków zawodowych;
- 5) genetyczne (tj. dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej);
- 6) biometryczne (tj. dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne);
- 7) dotyczące zdrowia (tj. dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia);
- 8) dotyczące seksualności lub orientacji seksualnej osoby.

Należy zwrócić uwagę, że katalog szczególnych kategorii danych osobowych (danych wrażliwych) ma charakter zamknięty, chociaż niektóre z nich są określone w sposób bardzo ogólny, np. dane dotyczące seksualności. EROD wskazuje, że przetwarzanie szczególnych kategorii danych, np. o stanie zdrowia, może wynikać z możliwości wnioskowania tych informacji z danych zwykłych. Założenia lub wnioski dotyczące danych kategorii specjalnej, np. że dana osoba po odwiedzeniu strony głoszącej poglądy liberalne prawdopodobnie zagłosuje na daną partię, również stanowiłyby specjalną kategorię danych osobowych. Podobnie – jak wskazuje EROD – profilowanie może stworzyć specjalną kategorię danych, wnioskując z danych, które same w sobie nie są specjalną kategorią danych, ale stają się takie w połączeniu z innymi danymi. Na przykład można wywnioskować czyjś stan zdrowia na podstawie zapisów dotyczących zakupów żywności w połączeniu z danymi o jakości i wartości energetycznej żywności¹.

 Odłąbną kategorią danych są dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa². Jak wskazuje art. 10 RODO, przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 RODO można dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem UE lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw

¹ EROD, *Wtyczne 8/2020 dotyczące targetowania użytkowników mediów społecznościowych*, v. 2.0, 13.04.2021 r., nb 121, https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_pl_0.pdf (dostęp: 15.02.2022 r.).

² P. Litwiński, P. Barta, M. Kawecki [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018, art. 10, nt 3–4, przyjmują następujące rozumienie wskazanych elementów:

- 1) informacje o „naruszeniach prawa” – informacje o przypadkach popełnienia przestępstwa (naruszenia obowiązującego prawa) przez daną osobę fizyczną, ale nie stwierdzonych wyrokami sądowymi (np. informacja o nałożeniu mandatu karnego, który ukarany przyjął),
- 2) powiązane środki bezpieczeństwa – środki zabezpieczające, które zostały wskazane w art. 93a § 1 k.k.

i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

Co istotne, zgodnie z treścią art. 10 RODO przedstawione kategorie danych, tj. dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa, mogą być przetwarzane na podstawie art. 6 RODO (a nie art. 9 RODO, który dotyczy szczególnych kategorii danych osobowych). Wskazane kategorie danych mogą być przetwarzane wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem UE lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

Pozostałe kategorie danych osobowych to dane osobowe zwykłe. Dane osobowe zwykłe to wszystkie inne kategorie niż wskazane powyżej szczególne kategorie danych osobowych oraz dotyczące wyroków skazujących i czynów zabronionych.

2. Dane osobowe podane, zaobserwowane, pochodne oraz wywnioskowane



Dla zrozumienia, czym są dane osobowe, istotne jest wyróżnienie następujących kategorii³:

- 1) podane dane osobowe – dane osobowe świadomie podawane przez osoby fizyczne, np. przy wypełnianiu formularza online;
- 2) zaobserwowane dane osobowe – dane osobowe rejestrowane automatycznie, np. za pomocą plików cookies lub czujników online, lub telewizji przemysłowej umożliwiającej rozpoznanie twarzy;
- 3) pochodne dane osobowe – dane osobowe „tworzone” z innych danych w stosunkowo prosty i bezpośredni sposób, np. przy obliczaniu zdolności kredytowej klienta;

³ ICO, *Big data, artificial intelligence, machine learning and data protection*, v. 2.2, 4.09.2017 r., s. 12, <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> (dostęp: 15.02.2022 r.).

- 4) wywnioskowane dane osobowe – dane osobowe tworzone za pomocą bardziej złożonych metod analitycznych (np. poprzez odszukiwanie korelacji między zestawami danych i wykorzystanie tych korelacji do kategoryzacji lub profilowania osób, np. obliczania wyników kredytowych lub przewidywania przyszłych wyników zdrowotnych). Dane wywnioskowane są oparte na prawdopodobieństwach i w związku z tym są mniej pewne niż dane pochodne.



Pojęcie danych osobowych obejmuje wszystkie wskazane kategorie. Potwierdza to wyrok Trybunału Sprawiedliwości z 20.12.2017 r., C-434/16, Peter Nowak przeciwko Data Protection Commissioner⁴. W przedmiotowej sprawie chodziło o odpowiedź na pytania:

1. Czy informacje zapisane przez osobę przystępującą do egzaminu zawodowego w odpowiedziach lub jako odpowiedzi na arkuszu egzaminacyjnym mogą stanowić dane osobowe w rozumieniu dyrektywy 95/46/WE?
2. Jakie czynniki są istotne dla określenia, czy w danym przypadku taki arkusz egzaminacyjny stanowi dane osobowe, i jakie znaczenie należy przypisać tym czynnikom?

We wskazanym orzeczeniu Trybunał Sprawiedliwości orzekł, że:

- 1) użycie w zawartej w art. 2 lit. a dyrektywy 95/46/WE definicji danych osobowych wyrażenia „wszelkie informacje” odzwierciedla przyświecający unijnemu prawodawcy zamiar przypisania temu pojęciu szerokiego zakresu znaczeniowego, nie ograniczając go do informacji wrażliwych czy też prywatnych, lecz rozszerzając go potencjalnie o informacje wszelkiego rodzaju, zarówno obiektywne, jak i subiektywne, w postaci opinii czy oceny, a jedynym warunkiem, które muszą one spełniać, jest to, aby „dotyczyły” danej osoby. Warunek ten jest zaś spełniony, gdy ze względu na swą treść, cel czy skutek dana informacja jest powiązana z daną osobą;
- 2) treść odpowiedzi egzaminacyjnych odzwierciedla poziom wiedzy i umiejętności osoby przystępującej do egzaminu w danej dziedzinie oraz, w odpowiednim przypadku, sposób jej rozumowania, wnioskowania i przyjęte przez nią krytyczne podejście. W przypadku

⁴ EU:C:2017:994.

- egzaminu pisanego odręcznie odpowiedzi te zawierają poza tym informacje odnoszące się do charakteru pisma;
- 3) w odniesieniu do naniesionych przez egzaminatora komentarzy dotyczących tych odpowiedzi należy stwierdzić, że stanowią one, tak jak udzielone na egzaminie przez przystępującą do niego osobę odpowiedzi, informacje dotyczące tej właśnie osoby. Treść tych komentarzy odzwierciedla bowiem wyrażoną przez egzaminatora opinię czy ocenę indywidualnych osiągnięć danej osoby na tym egzaminie, a w szczególności poziomu jej wiedzy i umiejętności w danej dziedzinie. To, że naniesione przez egzaminatora komentarze odnoszące się do odpowiedzi udzielonych na egzaminie przez osobę do niego przystępującą są również informacjami dotyczącymi egzaminatora, nie stoi na przeszkodzie uznaniu, że te komentarze, ze względu na ich treść, cel czy skutek, są powiązane z egzaminowaną osobą;
 - 4) ta sama informacja może dotyczyć więcej niż jednej osoby fizycznej i stanowić w odniesieniu do tych osób dane osobowe w rozumieniu art. 2 lit. a dyrektywy 95/46/WE, pod warunkiem że osoby te zostały zidentyfikowane lub są możliwe do zidentyfikowania.

Konkludując, Trybunał Sprawiedliwości na zadane pytania odpowiedział, że pojęcie danych osobowych należy interpretować w ten sposób, że odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego i ewentualne naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi stanowią dane osobowe w rozumieniu tego przepisu. Wyrok ten zachował swą aktualność także na gruncie RODO.

Co istotne, w ramach tego samego celu, w zależności czy dochodzić będzie do przetwarzania danych podanych, czy wywnioskowanych lub pochodnych, inne mogą być podstawy przetwarzania danych osobowych. Zwraça na to uwagę EROD w opinii dotyczącej mediów społecznościowych⁵. Podobnie inny może być zakres realizacji praw. Dotyczy to przykładowo prawa do przenoszenia danych. Grupa Robocza Art. 29 (obecnie EROD), w kontekście prawa do przenoszenia danych, wskazała, że można wyróżnić różne kategorie danych w zależności od ich pochodzenia, aby określić,

⁵ EROD, *Wytoczne 8/2020...*, nb 121.

administracyjne: jedno w sprawie naruszenia przepisów o ochronie danych osobowych w związku z przetwarzaniem danych osobowych bez podstawy prawnej⁸⁴, drugie w przedmiocie nałożenia na Głównego Geodetę Kraju administracyjnej kary pieniężnej za brak współpracy z Prezesem UODO w ramach wykonywania przez niego uprawnień kontrolnych⁸⁵.

Oba te postępowania zakończyły się nałożeniem na GGK administracyjnej kary pieniężnej w wysokości 100 000 zł (maksymalny wymiar kary). Ponadto w przypadku postępowania w sprawie naruszenia przepisów o ochronie danych osobowych w związku z przetwarzaniem danych osobowych bez podstawy prawnej Główny Geodeta Kraju został zobowiązany do dostosowania operacji przetwarzania danych osobowych do przepisów RODO poprzez zaprzestanie udostępniania na portalu GEO-PORTAL2 (www.geoportal.gov.pl) danych osobowych w zakresie numerów ksiąg wieczystych pozyskanych z ewidencji gruntów i budynków (prowadzonej przez starostów). Co istotne, Prezes UODO – poza możliwością stosowania egzekucji administracyjnej – na podstawie art. 83 ust. 6 RODO posiada istotne uprawnienie w postaci nałożenia administracyjnej kary pieniężnej za nieprzestrzeganie nakazu orzeczonego na podstawie art. 58 ust. 2 RODO (w tym nakazu dostosowania operacji przetwarzania danych osobowych do przepisów RODO). Oznacza to, że w przypadku niewykonania nakazu wynikającego z decyzji Prezes UODO będzie mógł nałożyć na Głównego Geodetę Kraju kolejną administracyjną karę pieniężną.

24. Czy można kwestionować wszczęcie kontroli lub inne czynności w toku kontroli?

Wszczęcie kontroli nie oznacza, że doszło do naruszenia przepisów o ochronie danych. Kontrola może uprawdopodobnić naruszenie, ale ostatecznie kwestia ta zostanie rozstrzygnięta w toku postępowania

⁸⁴ Decyzja Prezesa UODO z 24.08.2020 r., DKN.5112.13.2020, <https://uodo.gov.pl/decyzje/DKN.5112.13.2020> (dostęp: 15.02.2022 r.).

⁸⁵ Decyzja Prezesa UODO z 2.07.2020 r., DKE.561.3.2020.

administracyjnego. Z zastrzeżeniem powyższych uwag dotyczących kontroli niezapowiedzianej, w praktyce nie ma środków prawnych do kwestionowania samego wszczęcia kontroli (zasadności kontroli).

25. Czy można kwestionować wszczęcie postępowania administracyjnego lub inne czynności w jego toku?

Należy przyjąć, że postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych wszczyna Prezes UODO z urzędu. W sytuacji gdy prowadzona była kontrola, wynika to wprost z art. 90 u.o.d.o. Zgodnie z tym przepisem, jeżeli na podstawie informacji zgromadzonych w postępowaniu kontrolnym Prezes Urzędu uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania, o którym mowa w art. 60 u.o.d.o. (w sprawie naruszenia przepisów o ochronie danych osobowych). Tak samo należy przyjąć w sytuacji, gdy Prezes UODO decyduje się (bez prowadzenia kontroli) od razu wszcząć postępowanie administracyjne.

Do obu wskazanych sytuacji stosuje się, poprzez art. 7 u.o.d.o., art. 61 k.p.a. Zgodnie z art. 61 § 4 k.p.a. o wszczęciu postępowania z urzędu lub na żądanie jednej ze stron należy zawiadomić wszystkie osoby będące stronami w sprawie. Co ważne, wydane na podstawie art. 61 § 4 k.p.a. zawiadomienie o wszczęciu postępowania administracyjnego nie mieści się w żadnej z wyróżnionych w art. 3 § 2 p.p.s.a. kategorii form działania administracji publicznej podlegających sądowej kontroli. Jest ono czynnością procesową stanowiącą naturalną konsekwencję wynikającą z art. 10 k.p.a. zasady zapewnienia stronom czynnego udziału w każdym stadium tego postępowania. Jedynym celem tej czynności jest więc poinformowanie strony o wszczęciu postępowania administracyjnego i umożliwienie podjęcia przez nią aktywności ukierunkowanej na obronę jej praw. W konsekwencji zawiadomienie o wszczęciu postępowania nie stanowi formy nałożenia na stronę jakiegokolwiek obowiązku bądź przyznania jej określonego prawa, czy to o charakterze materialnym, czy procesowym. Z tych też względów ustawodawca nie

przewidział możliwości jego kwestionowania ani w postępowaniu administracyjnym, ani sądowym.

W tym miejscu należy zwrócić uwagę, że zgodnie z art. 61a k.p.a.:

„§ 1. Gdy żądanie, o którym mowa w art. 61, zostało wniesione przez osobę niebędącą stroną lub z innych uzasadnionych przyczyn postępowanie nie może być wszczęte, organ administracji publicznej wydaje postanowienie o odmowie wszczęcia postępowania. Przepis art. 61 § 5 stosuje się odpowiednio.

§ 2. Na postanowienie, o którym mowa w § 1, służy zażalenie”.

W powyższym kontekście WSA w Warszawie w wyroku z 27.11.2020 r., II SA/Wa 1542/20⁸⁶, wskazała, że:

„[...] w postanowieniu wydanym w trybie art. 61a § 1 k.p.a. organ nie może formułować wniosków i ocen dotyczących meritum żądania. Instytucja odmowy wszczęcia postępowania kończy się aktem formalnym, a nie merytorycznym (por. wyrok Naczelnego Sądu Administracyjnego z dnia 18 grudnia 2015 r., sygn. akt II OSK 999/14, publ. LEX nr 1989306).

Skoro nie jest prowadzone postępowanie administracyjne, to za bezzasadne należało uznać podniesione w skardze zarzuty naruszenia art. 7 w zw. z art. 77 § 1 k.p.a. w zw. z art. 61a § 1 k.p.a. Jeśli bowiem organ powołuje się na oczywistość przeszkód uzasadniającą wydanie postanowienia w przedmiocie odmowy wszczęcia postępowania, to musi ona wynikać bądź z treści samego wniosku o wszczęcie postępowania, faktów powszechnie znanych lub znanych organowi z urzędu (art. 77 § 4 k.p.a.), bądź z dokumentów urzędowych, którymi dysponuje organ (za: B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Wydawnictwo C.H. Beck, Warszawa 2016 r., str. 491). Nie prowadzi on w sprawie postępowania dowodowego. To między innymi odróżnia wstępną kontrolę wpływających do organu podań, od następczej kontroli możliwości prowadzenia postępowania. Jeżeli organ poweźmie wątpliwości co do możliwości procedowania, będzie

⁸⁶ LEX nr 3121804.

potrzebował przeprowadzić w tym zakresie postępowanie dowodowe – to powinien wszcząć postępowanie, przeprowadzić je, a w razie następczego stwierdzenia przeszkody do jego kontynuacji i merytorycznego zakończenia – umorzyć je na podstawie art. 105 k.p.a. Skoro zaś organ wybrał w niniejszej sprawie możliwe rozwiązanie na podstawie art. 61a § 1 k.p.a., w ocenie Sądu słuszne, to oznacza, że nie mógł naruszyć przepisów o postępowaniu dowodowym.

W rozpoznawanej sprawie jako przesłankę zastosowania art. 61a § 1 k.p.a. organ powołał brak ustawowych kompetencji, a więc w istocie brak przesłanki materialnoprawnej do rozpatrzenia żądania skarżącej o nakazanie udostępnienia danych osobowych autorów komentarzy zamieszczonych na portalach internetowych Google oraz Facebook, naruszających jej dobra osobiste”.

26. Jaka jest relacja zasady rozliczalności do obowiązku zebrania materiału dowodowego przez organ nadzorczy (art. 77 k.p.a.)?

Do postępowania w sprawie naruszenia przepisów o ochronie danych (w związku z treścią art. 7 ust. 1 u.o.d.o.) zastosowanie znajdzie m.in. art. 77 k.p.a. Zgodnie z nim:

„§ 1. Organ administracji publicznej jest obowiązany w sposób wyczerpujący zebrać i rozpatrzyć cały materiał dowodowy.

§ 2. Organ może w każdym stadium postępowania zmienić, uzupełnić lub uchylić swoje postanowienie dotyczące przeprowadzenia dowodu. [...]”.

W powyższym kontekście należy zwrócić uwagę, że zasada rozliczalności zawarta w RODO (art. 5 ust. 2) wskazuje, że to na administratorze danych spoczywa ciężar wykazania przestrzegania przepisów RODO (odnośnie do zapewnienia rozliczalności zob. część III rozdział II „Jak zapewnić i udokumentować zgodność?”).

Pomiędzy powyższymi regułami nie zachodzi sprzeczność. W orzecnictwie przyjmuje się, że obowiązek wskazany w art. 77 § 1 k.p.a. nie

Z opracowania czytelnik dowie się m.in.:

- jakie są prawa i obowiązki podmiotów kontrolowanych;
- na co zwraca uwagę Prezes UODO w trakcie kontroli;
- jak przebiegały dotychczas prowadzone kontrole;
- co grozi za utrudnianie lub udaremnianie kontroli.

W nowym wydaniu publikacji autorzy omawiają ponadto:

- wpływ pandemii koronawirusa na prowadzenie kontroli przestrzegania przepisów dotyczących ochrony danych osobowych;
- tryb i sposób prowadzenia kontroli na gruncie przepisów ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości;
- najważniejsze decyzje Prezesa UODO i orzecznictwo zapadłe w toku przeszło trzyletniego stosowania przepisów RODO.

Książka zawiera także:

- wzory dokumentów do wykorzystania zarówno na etapie kontroli, jak i postępowania w sprawie naruszenia przepisów o ochronie danych,
- wzory skarg na decyzje i postanowienia wydawane przez Prezesa Urzędu.

Wzory dostępne w wersji elektronicznej do pobrania ze strony www.ochrona-danych-osobowych-naruszenia-przepisow.wolterskluwer.pl po wpisaniu zamieszczonego w książce kodu aktywacyjnego. Wzory można modyfikować i dostosowywać do indywidualnych potrzeb.

Mirostaw Gumularz – doktor nauk prawnych, radca prawny; były doradca społeczny ds. ochrony danych osobowych w Ministerstwie Cyfryzacji w toku prac nad RODO; audytor wewnętrzny ISO 27001 (bezpieczeństwo informacji), 27701 (zarządzanie informacją o prywatności) oraz 22301 (ciągłość działania); autor oraz współautor licznych publikacji z zakresu ochrony danych osobowych i nowych technologii.

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



9788382862331 W02P01

ISBN 978-83-8286-233-1



9 788382 862331

ZAMÓWIENIA:

INFOLINIA: 801 04 45 45

ZAMOWIENIA@WOLTERSKLUPER.PL

WWW.PROFINFO.PL

Kup e-book i czytaj
w aplikacji Smarteca



CENA 119 ZŁ (W TYM 5% VAT)