

RODO

OCHRONA DANYCH OSOBOWYCH W STOSUNKACH PRACY

Edyta Jagiełło-Jaroszewska, Daria Jarmużek
Paulina Zawadzka-Filipczyk

RODO 2018

RODO

OCHRONA DANYCH OSOBOWYCH W STOSUNKACH PRACY

Edyta Jagiełło-Jaroszewska, Daria Jarmużek
Paulina Zawadzka-Filipczyk



Wolters Kluwer

WARSZAWA 2018

Stan prawny na 25 maja 2018 r.

Wydawca

Magdalena Stojek-Siwińska

Redaktor prowadzący

Adam Choiński

Opracowanie redakcyjne i łamanie

JustLuk

Poszczególne rozdziały przygotowały:

Edyta Jagiełło-Jaroszewska: rozdz. V, VI, XI

Daria Jarmużek: rozdz. IV, VII, VIII

Paulina Zawadzka-Filipczyk: rozdz. I–III, IX, X

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 978-83-8124-577-7

Dział Praw Autorskich

01-208 Warszawa, ul. Przykopowa 33

tel. 22 535 82 19

e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

Wykaz skrótów	11
Rozdział I	
Zagadnienia wstępne	15
1.1. Idea zmiany stanu prawnego w zakresie ochrony danych osobowych	15
1.2. Ochrona danych osobowych – podstawy prawne	17
1.2.1. RODO	20
1.2.2. Przepisy krajowe	25
1.3. Słowniczek RODO – podstawowe definicje	28
Rozdział II	
Zasady przetwarzania danych osobowych	41
2.1. Katalog podstawowych zasad ochrony danych	41
2.2. Konceptje <i>privacy by design</i> i <i>privacy by default</i>	47
2.3. Na czym polega rewolucyjność RODO?	48
Rozdział III	
Podstawy przetwarzania danych osobowych przez pracodawcę	50
3.1. Przesłanki dopuszczalności przetwarzania danych	50
3.1.1. „Zwykłe” dane osobowe	54
3.1.2. Dane osobowe wrażliwe	56
3.2. Zgoda pracownika na przetwarzanie danych	58

Rozdział IV

Zakres dopuszczalnego gromadzenia i przetwarzania danych osobowych pracowników przez pracodawcę	70
4.1. Ochrona danych osobowych kandydata	
w procesie rekrutacji	70
4.1.1. Jakie dane osobowe kandydata można przetwarzać? ...	71
4.1.2. Inne dane osobowe kandydata niż wskazane	
w Kodeksie pracy	75
4.1.3. Polecenia rekrutacyjne	79
4.1.4. Obowiązki pracodawcy w procesie rekrutacji	80
4.1.5. Dane osobowe kandydata a zakończenie rekrutacji ...	83
4.2. Ochrona danych osobowych pracownika	
w toku zatrudnienia	84
4.2.1. Rozpowszechnianie wizerunku pracownika	
w sieci wewnętrznej	87
4.2.2. Publikacja danych pracownika i jego zdjęcia	
w Internecie	88
4.2.3. Dane biometryczne	89
4.2.4. Monitoring	93
4.3. Ochrona danych osobowych pracownika po zakończeniu zatrudnienia	101
4.4. Ochrona danych osobowych w przypadku pracy tymczasowej	107
4.5. Ochrona danych osobowych w przypadku zatrudnienia cywilnoprawnego	108

Rozdział V

Obowiązki pracodawcy jako administratora danych	110
5.1. Ocena ryzyka oraz środki techniczne i organizacyjne zapewniające bezpieczeństwo zgromadzonych danych	110
5.2. Dokumentacja wewnętrzna dotycząca ochrony danych osobowych	123
5.2.1. Polityka ochrony danych	124
5.2.2. Rejestr czynności przetwarzania	125
5.2.3. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu	129

5.2.4. Dokumentacja naruszeń ochrony danych osobowych	135
5.2.5. Zawiadamianie osób, których dane dotyczą, o naruszeniu ochrony danych	136
5.2.6. Ocena skutków dla ochrony danych	141
5.2.7. Uprzednie konsultacje z organem nadzorczym	148
5.3. Wyznaczenie inspektora ochrony danych	152
5.4. Powierzanie przetwarzania danych osobowych usługodawcom pracodawcy	163
5.5. Przetwarzanie danych osobowych w ramach grupy przedsiębiorstw	173
5.6. Transfery danych osobowych w ramach EOG i do państw trzecich	176
5.7. Nadawanie upoważnień do przetwarzania danych osobowych	195

Rozdział VI

Prawa przysługujące pracownikowi, którego dane dotyczą

6.1. Zakres informacji podawanych osobie, której dane są zbierane	199
6.2. Dostęp do danych	208
6.3. Prawo do sprostowania danych	215
6.4. Prawo do usunięcia danych	217
6.5. Prawo do ograniczenia przetwarzania	222
6.6. Prawo do sprzeciwu	225

Rozdział VII

Postępowanie w sprawie naruszenia przepisów o ochronie

danych osobowych

7.1. Zasady prowadzenia postępowania kontrolnego	229
7.1.1. Organ prowadzący postępowanie	229
7.1.2. Jednoinstancyjność postępowania	230
7.1.3. Prawo organizacji do udziału w postępowaniu	233
7.1.4. Odpowiednie stosowanie procedury administracyjnej	237
7.1.5. Wszczęcie postępowania kontrolnego	238

7.2. Prawa i obowiązki pracodawcy w postępowaniu o naruszenie przepisów o ochronie danych osobowych	239
7.2.1. Obowiązek przedstawienia tłumaczenia dokumentu sporządzonego w języku obcym	239
7.2.2. Prawo do zastrzeżenia tajemnicy przedsiębiorstwa ...	240
7.2.3. Zobowiązanie do ograniczenia przetwarzania danych osobowych	244
7.3. Konsekwencje stwierdzenia naruszeń	248

Rozdział VIII

Kontrola pracodawcy w zakresie realizacji obowiązków

dotyczących ochrony danych osobowych	254
8.1. Zasady przeprowadzania postępowania kontrolnego	254
8.1.1. Organ prowadzący kontrolę	254
8.1.2. Rodzaje kontroli	259
8.2. Przebieg postępowania kontrolnego	261
8.2.1. Czas trwania kontroli PUODO	261
8.2.2. Upoważnienie do przeprowadzenia kontroli	262
8.3. Prawa i obowiązki kontrolującego w toku postępowania kontrolnego	265
8.3.1. Prawo wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń	265
8.3.2. Prawo wglądu do dokumentów	266
8.3.3. Prawo przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych	267
8.3.4. Prawo żądania złożenia pisemnych lub ustnych wyjaśnień oraz prawo wezwania i przesłuchania w charakterze świadka	268
8.3.5. Prawo zlecania sporządzania ekspertyz i opinii	269
8.3.6. Prawo korzystania z pomocy Policji	269
8.3.7. Prawo utrwalania przebiegu kontroli przy pomocy urządzeń rejestrujących obraz lub dźwięk	272
8.3.8. Prawo do przesłuchania pracownika kontrolowanego	274

8.4. Prawa i obowiązki pracodawcy w toku postępowania kontrolnego	275
8.4.1. Obowiązek zapewnienia warunków i środków niezbędnych do przeprowadzenia kontroli	275
8.4.2. Obowiązek sporządzenia kopii wydruków i potwierdzenia ich za zgodność z oryginałem	276
8.4.3. Obowiązek sporządzenia kopii informacji znajdujących się na nośnikach	277
8.4.4. Prawo do zgłaszania własnych wniosków dowodowych	277
8.4.5. Prawo do uczestniczenia w czynnościach kontrolnych	279
8.4.6. Prawo do uczestniczenia w przesłuchaniu świadków i zadawania im pytań	280
8.5. Protokół kontroli	282
8.6. Konsekwencje stwierdzenia naruszeń	284

Rozdział IX

Odpowiedzialność pracodawcy za naruszenie ochrony

danych osobowych	286
9.1. Odpowiedzialność cywilna	286
9.1.1. Odpowiedzialność odszkodowawcza na podstawie RODO	289
9.1.2. Odpowiedzialność cywilna na podstawie przepisów o ochronie danych	291
9.2. Odpowiedzialność administracyjna	292
9.3. Odpowiedzialność karna	303

Rozdział X

Wzory pism	307
10.1. Zgoda kandydata na przetwarzanie danych osobowych w procesie rekrutacji	307
10.2. Zgoda pracownika na rozpowszechnianie wizerunku	309
10.3. Cofnięcie zgody pracownika na przetwarzanie danych osobowych	311

Rozdział XI

Checklista realizacji obowiązków pracodawcy w zakresie wdrożenia RODO	312
--	------------

Bibliografia	315
---------------------------	------------

O autorach	319
-------------------------	------------

WYKAZ SKRÓTÓW

Akty prawne

- d.u.o.d.o. – ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.) – ustawa nie obowiązuje z wyjątkiem art. 1, 2, art. 3 ust. 1, art. 4–7, 14–22, 23–28, 31 oraz rozdziałów 4, 5 i 7*
- 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, ze zm.)
- Konstytucja RP – Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. poz. 483 ze zm.)
- k.p. – ustawa z 26.06.1974 r. – Kodeks pracy (Dz.U. z 2018 r. poz. 917 ze zm.)

* Art. 175 u.o.d.o.: „Traci moc ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723) z wyjątkiem art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziałów 4, 5 i 7, które zachowują moc w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie, w terminie do dnia wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającą decyzję ramową Rady 2008/977/WSiW (Dz. Urz. UE L 119 z 04.05.2016, str. 89)”.

k.p.a.	– ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2017 r. poz. 1257 ze zm.)
k.w.	– ustawa z 20.05.1971 r. – Kodeks wykroczeń (Dz.U. z 2018 r. poz. 618 ze zm.)
nowela z 10.01.2018 r.	– ustawa z 10.01.2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją (Dz.U. poz. 357)
projekt u.z.n.u.	– projekt z 23.05.2018 r. ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, https://legislacja.rcl.gov.pl/projekt/12302951/katalog/12457732#12457732
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.)
u.o.d.o.	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. poz. 1000)
u.z.n.k.	– ustawa z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2018 r. poz. 419)

Czasopisma i publikatory

Dz.U.	– Dziennik Ustaw
Dz.Urz. UE	– Dziennik Urzędowy Unii Europejskiej
HUDOC	– baza orzeczeń Europejskiego Trybunału Praw Człowieka, dostępna na stronie internetowej ETPC: echr.coe.int
ONSA	– Orzecznictwo Naczelnego Sądu Administracyjnego
ONSAiWSA	– Orzecznictwo Naczelnego Sądu Administracyjnego i Wojewódzkich Sądów Administracyjnych
OSNP	– Orzecznictwo Sądu Najwyższego – Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych

Inne

EOG	– Europejski Obszar Gospodarczy
ETPC	– Europejski Trybunał Praw Człowieka
GIODO	– Generalny Inspektor Ochrony Danych Osobowych
Grupa Robocza	– Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie
Art. 29	Przetwarzania Danych Osobowych
IOD	– inspektor ochrony danych
NSA	– Naczelny Sąd Administracyjny
PIP	– Państwowa Inspekcja Pracy
PUODO	– Prezes Urzędu Ochrony Danych Osobowych
SN	– Sąd Najwyższy
UOKiK	– Urząd Ochrony Konkurencji i Konsumentów
ZUS	– Zakład Ubezpieczeń Społecznych

Rozdział I

ZAGADNIENIA WSTĘPNE

1.1. Idea zmiany stanu prawnego w zakresie ochrony danych osobowych

Wyciąg z przepisów

Motyw 2 RODO

(...) Niniejsze rozporządzenie ma na celu przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także do pomyślności ludzi.

Motyw 4 RODO

Przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości. Prawo do ochrony danych osobowych nie jest prawem bezwzględny; należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności (...).

Motyw 10 RODO

Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych (...).

Ujęta w ramy normatywne ochrona danych osobowych w niektórych państwach europejskich ma już niemal 40 lat, a zapoczątkowała ją Konwencja nr 108 Rady Europy z 28.01.1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2003 r. poz. 25), która weszła w życie 1.10.1985 r.¹ Pierwotnie Komisja Europejska postulowała jedynie wobec państw członkowskich UE ratyfikację tej konwencji, jednak wobec rozbieżności w uregulowaniach krajowych organy unijne podjęły inicjatywę stworzenia odrębnych regulacji wspólnotowych w zakresie ochrony danych osobowych². Ich efektem była dotychczas obowiązująca dyrektywa 95/46/WE, która została uchylona ze skutkiem od 25.05.2018 r. (czyli z datą, od której bezpośrednio skuteczne staje się RODO).

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest w Europie jednym z **praw podstawowych**, czego gwarancję stanowią zapisy art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 389), jak również art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47). W związku z aneksją do UE Polska wdrożyła standardy unijne w zakresie ochrony danych osobowych w drodze ustawy z 29.08.1997 r. o ochronie danych osobowych. Należy dodać, że ustawa ta obecnie nie obowiązuje, z wyjątkiem art. 1, 2, 3 ust. 1, art. 4–7, 14–22, 23–28, 31 oraz rozdziałów 4, 5 i 7, w pozostałym zakresie została zastąpiona nową ustawą z 10.05.2018 r. o ochronie danych osobowych.

Gwałtowny rozwój technologiczny i globalizacja, jak również znaczne zwiększenie transgranicznych przepływów danych osobowych, w tym pomiędzy podmiotami publicznymi i prywatnymi, przyniosły jednakże całkowicie nowe wyzwania w dziedzinie ochrony danych osobowych. Powstała potrzeba stworzenia stabilniejszych i spójniejszych ram ochrony danych osobowych w UE oraz zdecydowanego ich egzekwowania. Ponadto niezbędne stało się wzmocnienie u osób

¹ Konwencja nr 108 Rady Europy w Polsce obowiązuje od 1.09.2002 r.

² W. Gogłóza, *Prawo do prywatności – studium komparatystyczne*, <https://wgogloza.files.wordpress.com/2007/12/prywatnosc1.pdf> (dostęp: 20.06.2018 r.).

fizycznych, podmiotów gospodarczych i organów publicznych większego poczucia pewności prawa i jego stosowania w praktyce. Celem aktualnej reformy europejskich przepisów o ochronie danych osobowych jest zatem **zapewnienie w UE spójnego i równorzędnego we wszystkich państwach członkowskich stopnia ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych – co z kolei umożliwi swobodny przepływ danych osobowych w UE, zniesie przeszkody w prowadzeniu działalności gospodarczej na szczeblu UE oraz w zakresie konkurencji, jak również ułatwi organom wykonywanie obowiązków nałożonych na nie prawem UE.**

Twórcom polskich regulacji ukierunkowanych na zapewnienie skutecznego stosowania RODO w naszej przestrzeni prawnej, oprócz wdrożenia przepisów unijnych, przyświeca równocześnie cel w postaci zapewnienia efektywniejszego od obowiązującego obecnie systemu ochrony danych osobowych. Priorytetem jest w szczególności **przyspieszenie trwających postępowań** w sprawach dotyczących zasad naruszenia ochrony danych osobowych w Polsce³. Ustawodawca polski kończy prace nad projektem ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 (dalej jako projekt u.z.n.u.)⁴.

1.2. Ochrona danych osobowych – podstawy prawne

Wyciąg z przepisów

Artykuł 1 RODO

1. W niniejszym rozporządzeniu ustanowione zostają przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.

³ Ocena skutków regulacji projektu u.o.d.o., <http://www.legislacja.gov.pl/projekt/12302951> (dostęp: 3.12.2017 r.).

⁴ Tekst projektu i uzasadnienia dostępny pod adresem: <https://legislacja.rcl.gov.pl/projekt/12302951/katalog/12457732#12457732> (dostęp: 25.06.2018 r.).

2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.
3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Artykuł 88 RODO

1. Państwa członkowskie mogą zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem, w szczególności do celów rekrutacji, wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy lub klienta oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.
2. Przepisy te muszą obejmować odpowiednie i szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, w szczególności pod względem przejrzystości przetwarzania, przekazywania danych osobowych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy.
3. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych na mocy ust. 1, a następnie niezwłocznie o każdej dotyczącej ich późniejszej zmianie.

Artykuł 94 RODO

1. Dyrektywa 95/46/WE zostaje uchylona ze skutkiem od dnia 25 maja 2018 r. (...)

Artykuł 99 RODO

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po publikacji w *Dzienniku Urzędowym Unii Europejskiej*.
2. Niniejsze rozporządzenie ma zastosowanie od dnia 25 maja 2018 r. Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Motyw 14 RODO

Ochrona zapewniana niniejszym rozporządzeniem powinna mieć zastosowanie do osób fizycznych – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych. Niniejsze rozporządzenie nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej.

Motyw 15 RODO

(...) Ochrona osób fizycznych powinna mieć zastosowanie do zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych. Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów nie powinny być objęte zakresem niniejszego rozporządzenia.

Motyw 18 RODO

Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, czyli bez związku z działalnością zawodową lub handlową. Działalność osobista lub domowa może między innymi polegać na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności. Niniejsze rozporządzenie ma jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej.

Artykuł 47 Konstytucji RP

Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Artykuł 51 Konstytucji RP

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

1.2.1. RODO

W Polsce będącej państwem członkowskim UE prawo unijne stanowi integralną część krajowego porządku prawnego. Fundamentalnymi zasadami prawa wspólnotowego są: zasada **pierwszeństwa prawa wspólnotowego** nad prawem stanowionym przez państwa członkowskie, jak również zasada **bezpośredniego skutku prawa europejskiego**, której zakres jest różny w zależności od rodzaju aktu prawnego. Rozporządzenia unijne są zawsze w pełni i bezpośrednio stosowane w krajach UE. Oznacza to, że ich skuteczność nie wymaga żadnych dodatkowych działań legislacyjnych w państwie członkowskim.

Ważne!

W dniu 25.05.2016 r. weszło w życie 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.), które ma zastosowanie od 25.05.2018 r. **Począwszy od tej daty RODO jest stosowane w sposób bezpośredni, stając się nadrzędnym aktem prawnym regulującym problematykę ochrony danych osobowych we wszystkich państwach członkowskich UE, w tym również w Polsce.**

Do głównych celów RODO należą:

- zapewnienie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych;
- uregulowanie swobodnego przepływu danych osobowych;
- ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych.

RODO zapewnia ochronę przetwarzania danych osobowych zarówno w sposób zautomatyzowany (całkowicie lub częściowo), jak i przetwarzanie tych danych w sposób ręczny – jeżeli dane te znajdują się lub mają się znaleźć w zbiorze danych.

RODO nie ma zastosowania w przypadku przetwarzania danych osobowych:

- w ramach działalności nieobjętej zakresem prawa Unii, w szczególności w zakresie bezpieczeństwa narodowego;
- przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres wspólnej polityki bezpieczeństwa i obrony;
- przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;
- przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom;
- do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii⁵.

Uwaga!

RODO nie obejmuje również przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej.

Jeżeli chodzi o czynności osób fizycznych o czysto osobistym lub domowym charakterze, to są to takie czynności, które pozostają **bez związku z działalnością zawodową lub handlową**. Zaliczają się do nich w szczególności: korespondencja i przechowywanie adresów, podtrzymywanie więzi społecznych oraz działalność internetowa po-

⁵ W tym zakresie zastosowanie znajduje rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z 18.12.2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.Urz. WE L 8 z 2001 r., s. 1).

dejmowana w ramach takiej działalności. Do wymienionych czynności nie ma obowiązku stosowania RODO, z zastrzeżeniem jednak, że RODO znajduje zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej. Ponadto RODO znajduje zastosowanie do osób fizycznych prowadzących działalność gospodarczą.

Przykład

Adam K. prowadzący działalność gospodarczą w zakresie fotografowania zamieścił na swoim profilu w Facebooku zdjęcia z sesji świątecznej swojej rodziny, w tym swojej kuzynki Moniki S. Z treści wpisu wynikało, że ma on na celu zachęcać potencjalnych klientów Adama K. do wykupienia takiej sesji. Zdjęcia Moniki S. podpisane jej imieniem i nazwiskiem były widoczne jedynie dla osób znajdujących się w sieci kontaktów Adama K. i jednocześnie były niedostępne dla pozostałych użytkowników portalu. Monika S. zażądała natychmiastowego usunięcia zdjęć, na którym widniała jej osoba, argumentując, że nie wyraziła zgody na ich publikację.

Adam K., przetwarzając dane dotyczące wizerunku Moniki S., naruszył prawo. Przetwarzanie danych osobowych w ramach portali społecznościowych co do zasady kwalifikuje się wprawdzie jako czynność o czysto osobistym lub domowym charakterze, o ile dostęp do tych danych mają jedynie osoby wybrane przez użytkownika (a nie dane są ogólnodostępne)⁶. Opisane działania Adama K. wykraczały jednak poza działania o czysto osobistym lub domowym charakterze. Jeżeli użytkownik portalu społecznościowego działa w imieniu przedsiębiorstwa lub wykorzystuje portal głównie jako platformę służącą osiągnięciu celów komercyjnych, to wówczas wyłączenie RODO nie ma zastosowania i użytkownik musi uzyskać zgodę osoby zainteresowanej (lub wskazać inną podstawę prawną legalizującą przetwarzanie tych danych).

⁶ Taki pogląd wyraziła Grupa Robocza Art. 29 w opinii 5/2009 w sprawie portali społecznościowych, przyjętej 12.06.2009 r.

Ważne!

RODO znajduje zastosowanie do przetwarzania danych osobowych:

- 1) w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego na terytorium UE.

Uwaga!

Samo przetwarzanie danych osobowych nie musi odbywać się na terytorium UE.

Przykład

Pracodawca mający siedzibę w Polsce deleguje pracowników na terytorium Ukrainy. Do przetwarzania danych osobowych pracowników delegowanych znajduje zastosowanie RODO;

- 2) osób, których dane dotyczą, przebywających w UE, przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w UE, jeżeli czynności przetwarzania wiążą się z:
 - oferowaniem towarów lub usług takim osobom – niezależnie od tego, czy pociąga to za sobą płatność, lub
 - monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w UE.

Uwaga!

Do ustalenia zamiaru oferowania towarów lub usług nie wystarczy sama dostępność w UE strony internetowej administratora, podmiotu przetwarzającego, pośrednika, adresu poczty elektronicznej lub innych danych kontaktowych ani posługiwanie się językiem powszechnie stosowanym w państwie trzecim, w którym jednostkę organizacyjną ma administrator. Natomiast potwierdzeniem oczywistości takiego zamiaru mogą być: posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w UE.

Na gruncie RODO „monitorowanie zachowania” polega na obserwowaniu osób fizycznych w Internecie, a także stosowaniu technik przetwarzania danych polegających na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw.

Przykład

Polski pracownik zgłosił się za pośrednictwem platformy internetowej na bezpłatne szkolenie językowe prowadzone przez wirtualną szkołę Business English. Przy założeniu, że szkoła ta miała zamiar oferować swoje usługi polskim klientom, do przetwarzania danych osobowych pracownika znajduje zastosowanie RODO;

- 3) przez administratora niemającego jednostki organizacyjnej w UE, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Uwaga!

Stosowanie RODO nie zależy od formy, w jakiej prowadzona jest działalność danej jednostki organizacyjnej. Płyne z tego wnioszek, że RODO może znaleźć zastosowanie również do jednostek organizacyjnych będących przedstawicielstwami i oddziałami⁷.

W zakresie interpretacji RODO walor pomocniczy, w praktyce o trudnym do przecenienia znaczeniu, mają te **opinie i zalecenia Grupy Roboczej Art. 29**, które zachowują aktualność pomimo zmiany stanu prawnego. Grupa Robocza Art. 29 jest niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności, zrzeszającym organy ochrony danych z całej UE. Została powołana na podsta-

⁷ Tak P. Litwiński [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych*. Komentarz, red. P. Litwiński, Warszawa 2017, s. 155.

wie art. 29 dyrektywy 95/46/WE. Opinie i zalecenia Grupy Roboczej Art. 29 nie są prawnie wiążące i nie mają bezpośredniego skutku.

Uwaga!

Grupa Robocza Art. 29 opracowała wytyczne do RODO w zakresie: inspektorów ochrony danych, prawa do przenoszenia danych, ustalenia głównego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego oraz dotyczące oceny skutków dla ochrony danych, jak również odnośnie do zgody na przetwarzanie danych osobowych.

Po 25.05.2018 r. Grupę Roboczą Art. 29 zastąpiła **Europejska Rada Ochrony Danych**, jako nowy i niezależny organ UE, którego głównym zadaniem będzie przyczynianie się do spójnego stosowania RODO w całej Unii. Rada będzie mogła w szczególności wydawać opinie, wytyczne i zalecenia, określać najlepsze praktyki, a także przyjmować prawnie wiążące decyzje w razie sporów między organami nadzorczymi.

1.2.2. Przepisy krajowe

W Polsce ochrona danych osobowych ma swoje źródło w Konstytucji, która zapewnia każdemu prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Konstytucja gwarantuje jednocześnie prawo do ochrony danych osobowych przez:

- dopuszczalność zobowiązania do ujawniania informacji dotyczącej swojej osoby jedynie na podstawie ustawy;
- zakaz pozyskiwania, gromadzenia i udostępniania przez władze publiczne innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym;
- zapewnienie każdemu prawa dostępu do dotyczących go urzędowych dokumentów i zbiorów danych, z ewentualnymi ograniczeniami określonymi ustawą;
- zapewnienie każdemu prawa do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

Problematyka, którą RODO wprost przekazuje do uregulowania w prawie krajowym oraz w zakresie której prawodawca unijny pozostawił swobodę regulacyjną państwom członkowskim, będzie stanowiła przedmiot **nowej ustawy z 10.05.2018 r. o ochronie danych osobowych**. Ustawa ta zastępuje dotychczas obowiązującą ustawę z 29.08.1997 r. o ochronie danych osobowych i znajdzie zastosowanie do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w RODO.

Jeśli chodzi o przetwarzanie danych osobowych pracowników w związku z zatrudnieniem, każde państwo członkowskie może przyjąć bardziej szczegółowe przepisy niż RODO, mające zapewnić ochronę praw i wolności. Dotyczy to w szczególności regulacji w zakresie:

- rekrutacji;
- wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi;
- zarządzania, planowania i organizacji pracy;
- równości i różnorodności w miejscu pracy;
- bezpieczeństwa i higieny pracy;
- ochrony własności pracodawcy lub klienta;
- indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem;
- zakończenia stosunku pracy.

Warunkiem, jaki postawił państwom członkowskim ustawodawca unijny, jest zagwarantowanie, by regulacje te obejmowały **odpowiednie i szczegółowe środki** zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, w szczególności pod względem przejrzystości przetwarzania, przekazywania danych osobowych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy.

Ważne!

Nowa ustawa o ochronie danych osobowych weszła w życie 25.05.2018 r., natomiast projekt ustawy o zmianie niektórych

ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 jest jeszcze (na dzień oddania tekstu do druku) w fazie prac legislacyjnych.

Nowa ustawa o ochronie danych osobowych określa:

- 1) podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o jego wyznaczeniu;
- 2) warunki i tryb akredytacji podmiotu uprawnionego do certyfikacji w zakresie danych osobowych, akredytowanego przez Polskie Centrum Akredytacji, podmiotu monitorującego kodeks postępowania oraz certyfikacji;
- 3) tryb zatwierdzenia kodeksu postępowania;
- 4) organ właściwy w sprawie ochrony danych osobowych;
- 5) postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych;
- 6) tryb europejskiej współpracy administracyjnej;
- 7) kontrolę przestrzegania przepisów o ochronie danych osobowych;
- 8) odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych i postępowanie przed sądem;
- 9) odpowiedzialność karną i administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych.

Uwaga!

Jak wynika z nowej ustawy o ochronie danych osobowych, ograniczenia w stosowaniu RODO mają zastosowanie do działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych, jak również do wypowiedzi w ramach działalności literackiej lub artystycznej, a także wypowiedzi akademickiej.

Ważne!

Na mocy projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 zostaną zmodyfikowane m.in. przepisy Kodeksu pracy dotyczące danych osobowych podawanych pracodawcy przez kandydata do zatrudnienia oraz przez pracownika, jak również przepisy ustawy

z 4.03.1994 r. o zakładowym funduszu świadczeń socjalnych (Dz.U. z 2017 r. poz. 2191 ze zm.) dotyczące danych osobowych udostępnianych pracodawcy w związku z korzystaniem ze świadczeń z zakładowego funduszu świadczeń socjalnych przez osoby uprawnione (zob. rozdział IV). Z kolei na mocy nowej ustawy o ochronie danych osobowych uregulowane zostały zasady stosowania monitoringu w zakładzie pracy.

1.3. Słowniczek RODO – podstawowe definicje

Podstawowe definicje w zakresie ochrony danych osobowych określa art. 4 RODO.

1. Dane osobowe

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane osobowe zatem to **wszelkie informacje, które pozwalają ustalić w sposób bezpośredni lub pośredni tożsamość konkretnej osoby fizycznej** (odróżnić ją od wszystkich pozostałych członków grupy). Pojęcie danych osobowych obejmuje wszelkie stwierdzenia na temat osoby – informacje „obiektywne”, jak również „subiektywne”, opinie lub oceny. Informacje te nie muszą być prawdziwe ani sprawdzone. Mogą dotyczyć życia prywatnego i rodzinnego, jak również życia zawodowego, a także relacji społecznych osoby lub jej zachowań ekonomicznych. Nie ma znaczenia format tych informacji czy też rodzaj nośnika. Przy czym informacja dotyczy osoby, jeżeli jest ona na temat tej osoby (jest o tej osobie) lub choćby pośrednio się do niej odnosi.

Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo, że zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, trzeba z kolei uwzględnić wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz technologię dostępną w momencie przetwarzania danych, jak również postęp technologiczny. O tym, na ile poszczególne czynniki identyfikujące pozwalają na ostateczne ustalenie tożsamości osoby, decydują szczególne okoliczności danej sytuacji.

Przykład

Samo nazwisko „Nowak” nie pozwoli w Polsce na zidentyfikowanie osoby – czyli wyodrębnienie jej na tle pozostałych członków grupy. W ramach zakładu pracy liczącego kilkanaście osób zazwyczaj pozwoli już dość łatwo zidentyfikować osobę.

Dane osobowe to w szczególności: imię i nazwisko, adres zamieszkania, numer telefonu, numer PESEL, NIP, numer rachunku bankowego, adres mailowy, wizerunek, zdjęcie, informacje o wykształceniu i doświadczeniu zawodowym, numer rejestracyjny pojazdu. Daną osobową może być jednak także adres IP, jeśli na dłuższy okres czasu lub na stałe jest on przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi⁸.

Ważne!

Wyróżniamy dwie kategorie danych osobowych: **dane osobowe zwykłe** oraz **dane osobowe wrażliwe**, czyli dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycz-

⁸ Tak wyrok NSA z 19.05.2011 r., I OSK 1079/10, LEX nr 990136.

nej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Uwaga!

RODO nie znajduje zastosowania do danych osób zmarłych. Zasady ochrony danych osobowych nie mają też zastosowania do informacji anonimowych ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować.

2. Przetwarzanie

Przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Uwaga!

Samo żądanie danych osobowych jest czynnością faktyczną, która poprzedza zbieranie danych osobowych⁹. Nie stanowi więc ono jeszcze przetwarzania danych osobowych, a tym samym nie jest to czynność objęta działaniem RODO.

3. Ograniczenie przetwarzania

Ograniczenie przetwarzania – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Wśród metod pozwalających ograniczyć przetwarzanie danych osobowych mogą się znaleźć m.in.: czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do wybranych danych lub czasowe usunięcie opublikowanych danych ze strony internetowej. Dane osobowe, co do których ograni-

⁹ Tak wyrok NSA z 28.06.2011 r., I OSK 1264/10, LEX nr 1082607.

czono ich przetwarzanie, powinny być wyróżnione na tle innych danych, nie podlegają one dalszemu przetwarzaniu i nie mogą być zmieniane.

4. Profilowanie

Profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Ważne!

Zautomatyzowane przetwarzanie danych osobowych stanowi profilowanie, o ile wywołuje skutki prawne względem osoby lub w podobny sposób znacząco na nią wpływa.

5. Pseudonimizacja

Pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Dane spseudonimizowane to zatem takie dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej.

Uwaga!

Pseudonimizacja jest jedną z zalecanych przez RODO metod zabezpieczeń danych osobowych.

6. Zbiór danych

Zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Przykład

Typowymi zbiorami danych osobowych w zakładzie pracy są zbiór danych osobowych kandydatów do zatrudnienia oraz zbiór danych osobowych pracowników. Zbiory te mogą mieć zarówno postać tradycyjną (papierową), jak i elektroniczną.

7. Administrator

Administrator – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Administratorem danych osobowych nie jest każdy dysponent tych danych¹⁰ (w szczególności każdy pracownik, którego upoważniono do przetwarzania danych osobowych). Administratorem danych osobowych jest tylko ten, kto **faktycznie decyduje o celach i środkach ich przetwarzania**, bez względu na to, czy dane te fizycznie posiada. W przypadku danych osobowych przetwarzanych w ramach stosunku pracy wskazówką pomocną przy identyfikowaniu administratora danych jest zwyczajowa rola pracodawcy w odniesieniu do danych dotyczących jego pracowników, zwykle wiążąca się z pewną odpowiedzialnością.

Uwaga!

Jeśli chodzi o dane osobowe osób zatrudnionych (zarówno na podstawie stosunku pracy, jak i stosunku cywilnoprawnego), status administratora ma zawsze pracodawca. Nie ma znaczenia, czy pracodawca przetwarza te dane wyłącznie własnymi środkami, czy też powierza je podmiotowi zewnętrznemu (np. biuru rachunkowemu prowadzącemu księgowość czy firmie kadrowo-płacowej).

¹⁰ Tak wyrok NSA z 30.01.2002 r., II SA 1098/01, „Wokanda” 2002/7–8, s. 70.