

*Patrycja Kozik, Mirosław Gumularz*

# Rozdział I. Zakres przedmiotowy regulacji RODO – rozumienie danych osobowych i ich przetwarzania w kontekście marketingu i sprzedaży

## 1. Zagadnienia wstępne

Z punktu widzenia zakresu przedmiotowego regulacji RODO (czyli tego, czego RODO dotyczy) podstawowe znaczenie ma art. 2 RODO oraz definicja danych osobowych i przetwarzania danych osobowych, zawarta w art. 4 RODO. Stosownie do art. 2 ust. 1 RODO jego regulacje znajdują zastosowanie do:

- 1) przetwarzania danych osobowych w sposób tradycyjny (np. teczki papierowe), gdy dane są przetwarzane w zbiorach danych (uporządkowanych zestawieniach) lub mają w nich być przetwarzane;
- 2) przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany (np. w systemach IT), niezależnie od tego, czy przetwarzane są w zbiorach danych (uporządkowanych zestawieniach)<sup>1</sup>.

Nieco inaczej określono przedmiot regulacji w California Consumer Privacy Act of 2018, dotyczącej przetwarzania danych osobowych (prawo kalifornijskie wzorowane na RODO, stanowiące w związku z tym ciekawy materiał porównawczy): „przetwarzanie” oznacza operację lub zestaw operacji na danych osobowych lub ich zestawach, niezależnie od

---

<sup>1</sup> Tak np. *P. Voigt, A. von dem Bussche, The EU General Data Protection Regulation (GDPR). A Practical Guide, Switzerland 2017, s. 9–10.*

tego, czy przetwarzanie ma charakter zautomatyzowany<sup>2</sup>. W świetle tej definicji to, czy dochodzi do przetwarzania danych osobowych w sposób zautomatyzowany, czy w sposób tradycyjny (w zbiorach danych lub poza nimi), nie ma znaczenia jako kryterium definiujące zakres przedmiotowy regulacji. Najwyraźniej uznano, że wskazane kryteria: zautomatyzowanego przetwarzania oraz zbioru danych nie są na tyle precyzyjne, aby uznać je za prawnie doniosłe. Niemniej jednak, na te dwa elementy należy zawsze zwracać uwagę przy ocenie czy, dana operacja na danych osobowych podlega regulacji RODO. Przedstawione powyżej elementy, w szczególności treść art. 2 RODO przesądzają, że przy ustalaniu, czy dojdzie do zastosowania RODO w danej sytuacji biznesowej, należy w uproszczeniu<sup>3</sup> ocenić, czy:

- 1) dochodzi do przetwarzania danych osobowych,
- 2) przetwarzanie ma charakter zautomatyzowany (choćby częściowo) czy niezautomatyzowany,
- 3) jeżeli przetwarzanie ma charakter niezautomatyzowany – czy dane są lub będą być przetwarzane w zbiorze.

Zgodnie z art. 4 pkt 6 RODO zbiór danych oznacza uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany, czy rozproszony funkcjonalnie lub geograficznie<sup>4</sup>.

Stosownie do art. 4 pkt 2 RODO przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.

W konsekwencji przetwarzanie oznacza każde działanie, którego przedmiotem są dane osobowe, niemniej – jak wskazano wyżej – nie każde przetwarzanie danych osobowych będzie podlegało RODO. Aby RODO znalazło zastosowanie do przetwarzania danych, do którego będzie dochodziło w sposób niezautomatyzowany (tradycyjny), powinny one stanowić część zbioru (uporządkowanego według kryteriów zestawu danych). Precyzuje to motyw 15 RODO, który stanowi, że aby zapobiec poważnemu ryzyku obchodzenia

---

<sup>2</sup> „»Processing« means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means”.

<sup>3</sup> O wyłączeniach z zakresu stosowania RODO zob. art. 2 ust. 2 RODO.

<sup>4</sup> W wyroku TS z 10.7.2018 r. (C-25/17, Legalis) zdefiniowano pojęcie zbioru danych (dotyczyło to jeszcze poprzednich przepisów dyrektywy 95/46, niemniej była ona zbliżona do tej zawartej w RODO), wskazując, że ochrona osób fizycznych musi odnosić się zarówno do automatycznego przetwarzania danych, jak i ręcznego przetwarzania; zakres tej ochrony nie może w swym skutku być zależny od zastosowanych technik, ponieważ w przeciwnym razie wystąpiłoby poważne ryzyko obchodzenia zasad; niemniej odnośnie do ręcznego przetwarzania danych, niniejsza dyrektywa obejmuje jedynie zbiory danych, nie zaś niezorganizowane zbiory; w szczególności zawartość zbiorów musi być zorganizowana według określonych kryteriów dotyczących osób fizycznych, zapewniających łatwy dostęp do danych; zgodnie z definicją zawartą w art. 2 lit. c poszczególne państwa członkowskie mogą określić różne kryteria określania części składowych zorganizowanego zestawu danych oraz różne kryteria dostępu do takiego zestawu; zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są zorganizowane według określonych kryteriów nie powinny w żadnych okolicznościach wchodzić w zakres niniejszej dyrektywy.

prawa, ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik. 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 RODO.

Definicję danych osobowych zawiera art. 4 pkt 1 RODO. Zgodnie z nim dane osobowe oznaczają wszelkie 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:

- 1) imię i nazwisko,
- 2) numer identyfikacyjny,
- 3) dane o lokalizacji,
- 4) identyfikator internetowy,
- 5) jeden czynnik bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Powyższą definicję precyzuje motyw 26 RODO, zgodnie z którym: zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), 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, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas, potrzebne do jej zidentyfikowania oraz uwzględnić zarówno technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny. Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Przepisy RODO nie dotyczą więc przetwarzania takich anonimowych informacji, w tym przetwarzania do celów statystycznych lub naukowych<sup>5</sup>.

---

<sup>5</sup> Warto zwrócić uwagę, że normy ISO zamiast pojęcia danych osobowych posługują się pojęciem informacji identyfikowalnych personalnie (*personally identifiable information* – PII). Przykładowo norma ISO 27018 definiuje PII jako wszelkie informacje, które:

1) mogą zostać użyte w celu identyfikacji podmiotu danych, do którego odnoszą się te informacje lub

2) są lub mogą być bezpośrednio lub pośrednio powiązane z tym podmiotem.

Trzeba przyjąć, że pomiędzy pojęciem „dane osobowe” a wskazanym pojęciem „informacje identyfikowalne personalnie” nie zachodzą istotne różnice.

Wyróżnia się przy tym następujące kategorie danych:

- 1) dane osobowe zwykle (wszelkie dane osobowe, które nie są danymi szczególnych kategorii);
- 2) dane osobowe szczególnych kategorii, tzw. dane wrażliwe – wskazane w art. 9 RODO – tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
- 3) dane osobowe dotyczące wyroków skazujących i naruszeń prawa (zob. art. 10 RODO).

Powyższe rozróżnienie ma znaczenie m.in. ze względu na odmienne podstawy przetwarzania danych wskazanych kategorii (omówionych w rozdziale XX). Zwłaszcza w kontekście marketingu należy zwrócić uwagę, że w zakresie szczególnych kategorii danych mieszczą się dane biometryczne. Zgodnie z RODO (art. 4 pkt 14) „dane biometryczne” oznaczają 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. W praktyce często wykorzystywane są systemy umożliwiające przetwarzanie danych biometrycznych, bez wyraźnego poinformowania użytkowników tych systemów (np. administratorów danych) o takiej funkcjonalności. Kwestię tę należy zawsze uwzględnić przy ocenie systemów informatycznych.

W tym miejscu należy zwrócić także uwagę, że dane speudonimizowane to w dalszym ciągu dane osobowe. Definicję pseudonimizacji zawiera art. 4 pkt 5 RODO. Zgodnie z nim pseudonimizacja oznacza 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.

Od pseudonimizacji danych należy odróżnić ich anonimizację. Nie została ona zdefiniowana w RODO, ale należy wskazać, że w przeciwieństwie do pseudonimizacji, która jest procesem odwracalnym, anonimizacja prowadzi do nieodwracalnego uniemożliwienia zidentyfikowania osoby, której dane dotyczą. Jeżeli zatem ze zbioru danych zostaną usunięte dane, które można przypisać konkretnej osobie, w tym z wykorzystaniem dodatkowych informacji, dojdzie do anonimizacji, np. w miejsce imienia i nazwiska wstawi się wyłącznie ciąg cyfr bez jakiegokolwiek klucza pozwalającego na odwrócenie dokonanej operacji (jak byłoby w przypadku pseudonimizacji). Dane zanonimizowane nie będą danymi osobowymi. Anonimizacja często będzie prowadziła do przetwarzania danych statystycznych, które – jeśli zostaną zanonimizowane w należyty sposób – nie będą stanowiły danych osobowych (np. mężczyzna, z miasta powyżej 500 000 mieszkańców, w wieku powyżej 25 lat, robi zakupy dwa razy w tygodniu). Kwestia pseudonimizacji będzie szczególnie istotna z punktu widzenia rozdziału XIV.

Od przetwarzania danych statystycznych (zagregowanych) należy odróżnić przetwarzanie danych osobowych w celu statystycznym. Definicję celu statystycznego zawiera

motyw 162 RODO. Wyrażenie „cele statystyczne” oznacza każdą operację zbierania i przetwarzania danych osobowych niezbędnych do badań statystycznych lub do opracowywania wyników statystycznych. Z kolei wyniki statystyczne mogą następnie służyć do dalszych celów, m.in. do celów badań naukowych. Wyrażenie „cel statystyczny” sugeruje, że wynikiem przetwarzania do celów statystycznych nie są dane osobowe, lecz dane zbiorcze, i że wynik ten lub te dane osobowe nie służą za podstawę środków czy decyzji dotyczących konkretnych osób fizycznych.

Z perspektywy marketingu bezpośredniego oraz sprzedaży zgłaszane są w praktyce następujące wątpliwości (omówione w dalszej części niniejszego rozdziału) dotyczące zakresu pojęcia danych osobowych, związane z próbami odpowiedzi na pytania, czy pojęcie danych osobowych obejmuje:

- 1) dane osobowe dostępne publicznie (np. firmowe strony WWW, CEIDG, KRS itp.),
- 2) dane osobowe przedsiębiorców (CEIDG),
- 3) dane osobowe członków organów jednostek organizacyjnych (np. członków zarządu spółki z o.o.),
- 4) informacje stanowiące część nazwy przedsiębiorcy (np. Jan Iksiński Budowa sp. z o.o.),
- 5) dane osobowe przedstawicieli (np. pełnomocników, prokurentów) przedsiębiorców,
- 6) dane dotyczące pracowników/współpracowników przedsiębiorców (np. dane wskazywane w umowie do kontaktu lub realizacji umowy),
- 7) dane trudno przypisywalne osobom fizycznym (np. o ruchu na stronie internetowej),
- 8) dane „wygenerowane” przez administratora danych (np. poprzez profilowanie).

## 2. Dane osobowe dostępne publicznie

Pojęcie danych dostępnych publicznie nie zostało zdefiniowane w RODO. Na gruncie poprzedniego stanu prawnego GIODO wskazywał, że są to dane, z którymi bez szczególnego nakładu sił i środków może się zapoznać nieograniczony krąg podmiotów<sup>6</sup>. Jak się wydaje, wskazana definicja zachowa swoją aktualność na gruncie przepisów RODO, które nie zawierają szczególnych regulacji w zakresie dopuszczalności przetwarzania tej kategorii danych (ani wyłączeń w odniesieniu do nich z zakresu jego zastosowania). Niezależnie od tego nie powinno budzić wątpliwości, że samo upublicznienie informacji pozostaje bez wpływu na ich uznanie za dane osobowe (jeżeli tylko będą stanowiły informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej), a w konsekwencji – na zastosowanie przepisów RODO. Okoliczność, że dane mają charakter biznesowy, np. służbowy adres e-mail pracownika opublikowany na stronie internetowej firmy, również nie ma znaczenia z punktu widzenia ich uznania za dane osobowe i stosowania do nich przepisów RODO. W tym zakresie należy odróżnić:

---

<sup>6</sup> Zob. Generalny Inspektor Ochrony Danych Osobowych, Przetwarzania danych osobowych w sektorze bankowym, [https://giodo.gov.pl/data/filemanager\\_pl/1430.pdf](https://giodo.gov.pl/data/filemanager_pl/1430.pdf) (dostęp: 12.11.2018 r.), s. 20; [https://giodo.gov.pl/1520050/id\\_art/1562/j/pl](https://giodo.gov.pl/1520050/id_art/1562/j/pl) (dostęp: 12.11.2018 r.).

- 1) informacje dostępne publicznie i wynikające z rejestrów publicznych (np. CEIDG),
- 2) informacje dostępne publicznie i wynikające z innych źródeł niż rejestry publiczne (np. zakładki „kontakt” na stronach internetowych przedsiębiorców)<sup>7</sup>.

Tworzenie rejestrów publicznych jest regulowane stosownymi ustawami, np. KRSU czy CEiIDGiPIPU, których przepisy stanowią podstawę do przetwarzania (ujawniania) danych w zakresie w nich wskazanym. W związku z tym takie przetwarzanie może prowadzić do różnego rodzaju ograniczeń (np. w zakresie realizacji obowiązku informacyjnego czy prawa do bycia zapomnianym)<sup>8</sup>. Niemniej od tworzenia rejestrów publicznych (i przetwarzania danych osobowych w tym celu) przez organy państwowe, uprawnione do tego na mocy przepisów, należy odróżnić korzystanie z danych zawartych w rejestrach przez podmioty prywatne. W konsekwencji należy wskazać, że poczynione rozróżnienie – korzystanie z danych dostępnych publicznie ujętych w rejestrze publicznym i korzystanie z danych z innych źródeł – będzie w tym zakresie pozostawało bez wpływu na realizację obowiązków wynikających z RODO, o czym jest mowa w dalszej części tego rozdziału.

Przepisy RODO odnoszą się do danych dostępnych publicznie w kontekście obowiązku informacyjnego, realizowanego w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą. Stosownie do art. 14 ust. 2 lit. f RODO w celu zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych. Jak wskazuje się w doktrynie, na pierwszy plan w tym przypadku wysuwa się to, że prawodawca unijny jednoznacznie przesądza o tym, że spełnienie obowiązku informacyjnego co do zasady nie jest uzależnione od charakteru źródła danych osobowych. Zatem nawet jeśli administrator pozyskuje dane z publicznie dostępnych źródeł – a więc ogólnie rzecz ujmując: z Internetu, z książki telefonicznej, z tablic ogłoszeń zamieszczonych w sądach czy urzędach, z rejestrów publicznych prowadzonych przez organy władzy publicznej (takich jak KRS, elektroniczne księgi wieczyste i CEIDG), z których informacje są zgod-

---

<sup>7</sup> Por. California Consumer Privacy Act (CCPA) of 2018: „»Dane osobowe« nie obejmują informacji dostępnych publicznie. Przez »publicznie dostępne informacje« należy rozumieć informacje, które zgodnie z prawem są upubliczniane w ramach rejestrów federalnych, stanowych lub lokalnych – rządowych, jeżeli istnieją jakiegokolwiek warunki związane z takimi informacjami. »Publicznie dostępny« nie oznacza informacji biometrycznych zebranych przez firmę na temat konsumenta bez wiedzy konsumenta. Informacje nie są »publicznie dostępne«, jeżeli dane te są wykorzystywane do celów, które nie są zgodne z celem, dla którego dane są utrzymywane i upubliczniane w rządowych rejestrach lub dla których są publicznie utrzymywane. »Publicznie dostępny« nie obejmuje informacji dotyczących konsumentów, które są pozbawione cechy identyfikowalności lub są danymi zagregowanymi”.

Istotne jest to, że pojęcie danych osobowych (personalnych) na gruncie regulacji CCPA nie obejmuje danych upublicznionych w ramach – ujmując rzecz ogólnie – funkcjonowania rejestrów publicznych. Jednocześnie CCPA wskazuje, że w przypadku przetwarzania w innym celu (niezgodnym) niż cel dla, którego zostały upublicznione takie przetwarzanie może zostać objęte regulacją tego aktu.

<sup>8</sup> Zgodnie z art. 12 ust. 1 KRSU dane zawarte w rejestrze nie mogą być z niego usunięte, chyba że ustawa stanowi inaczej. Analogiczne postanowienie zawarto w art. 49 ust. 1 CEiIDGiPIPU. Centralna Ewidencja i Informacja o Działalności Gospodarczej umożliwia wyszukiwanie informacji również o podmiotach z niej wykreślonych. Zob. wyrok TSUE z 9.3.2017 r. (C-398/15, Legalis).

nie z prawem udostępniane, w tym publikowane w Internecie – nie może czuć się zwolniony z obowiązku informacyjnego tylko z racji tego, że dane te zostały upublicznione. Czym innym jest bowiem prowadzenie rejestrów publicznych na warunkach określonych w przepisach prawa, a czym innym – wtórne pozyskiwanie danych osobowych zawartych w tych rejestrach do celów nieznanymi podmiotowi danych<sup>9</sup>.

W konsekwencji, jeżeli administrator danych korzysta z danych pozyskanych ze źródeł powszechnie dostępnych, powinien spełnić obowiązek informacyjny wskazany w art. 14 RODO. Niemniej, w kontekście powyższego, należy zwrócić uwagę na motyw 62 RODO, objaśniający kwestie związane z wyłączeniem realizacji obowiązku informacyjnego, zawarte w art. 14 ust. 5 RODO. Motyw ten stanowi, że nałożenie obowiązku udzielenia informacji nie jest konieczne, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami, jeżeli utrwalenie lub ujawnienie danych są wyraźnie przewidziane prawem lub jeżeli poinformowanie osoby, której dane dotyczą, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Sytuacja braku możliwości lub niewspółmiernie dużego wysiłku może zachodzić w szczególności przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym. Uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia.

Powyższe wyłączenie znajdzie zastosowanie do ujawniania danych w rejestrach publicznych (co zostało przewidziane stosownymi ustawami), a także do korzystania z danych osobowych zawartych w rejestrach publicznych przez inne podmioty niż uprawnione do ich tworzenia na podstawie przepisów, w szczególności jeżeli wykażą one, że poinformowanie osoby, której dane dotyczą, jest niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Przesłanka ta została zliberalizowana w porównaniu do poprzedniego stanu prawnego, który przewidywał możliwość powoływania się na wyłączenie z realizacji obowiązku informacyjnego jedynie wtedy, gdy dane są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie obowiązku wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania (art. 25 ust. 2 pkt 3 OchrDanychU97).

### Ważne

Niezależnie od samego obowiązku informacyjnego przesądzenie, że dochodzi do przetwarzania danych osobowych (ze źródeł publicznie dostępnych), będzie wiązało się z koniecznością realizacji wszystkich zasad przetwarzania danych osobowych, w szczególności zasady zgodności z prawem przetwarzania, przejawiającej się w obowiązku posiadania podstawy prawnej do przetwarzania tak pozyskanych danych.

<sup>9</sup> M. Sakowska-Baryła (red.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Legalis/el. 2018, komentarz do art. 14.

### 3. Dane osobowe jednoosobowych przedsiębiorców

Należy zwrócić uwagę, że definicja danych osobowych odnosi się od osób fizycznych – bez względu na rolę, jaką odgrywają (czy są konsumentami, przedsiębiorcami, czy pracownikami itd.). Co istotne, w prawie cywilnym pojęcie konsumenta (np. w ramach umowy sprzedaży zawieranej online) odnosi się do relacji z przedsiębiorcą. Konsumentem nie można być w relacji z innym konsumentem (osobą dokonującą transakcji poza swoją działalnością gospodarczą lub zawodową). Natomiast takiego ograniczenia (co do zasady) nie ma w przepisach o ochronie danych. Regulacje RODO dotyczą każdego przetwarzania danych osobowych osób fizycznych. Nie można jednak zapominać o art. 2 ust. 2 lit. c RODO, zgodnie z którym RODO nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze.

Okoliczność, że osoba fizyczna prowadzi działalność gospodarczą, nie oznacza jednak pozbawienia dotyczących jej informacji przymiotu danych osobowych (np. oznaczenie przedsiębiorcy, tj. firma w rozumieniu przepisów KC czy numer NIP osoby fizycznej), a w konsekwencji – braku obowiązku stosowania do nich przepisów RODO. Wyłączenie w tym zakresie było zawarte w SwobDziałGospU. Przepis art. 39b SwobDziałGospU stanowił, że do jawnych danych i informacji udostępnianych przez CEIDG nie stosuje się przepisów OchrDanychU97, z wyjątkiem przepisów art. 14–19a i 21–22a oraz rozdziału 5 OchrDanychU97. Obowiązująca od 30.4.2018 r. CEiIDGiPIPU, która obecnie określa zasady funkcjonowania Centralnej Ewidencji i Informacji o Działalności Gospodarczej, nie zawiera analogicznego wyłączenia. Co więcej, takie wyłączenie w odniesieniu do osób fizycznych byłoby niezgodne z przepisami RODO<sup>10</sup>. W tym miejscu należy zwrócić uwagę na motyw 14 RODO, który wskazuje, że ochrona zapewniana RODO powinna mieć zastosowanie do osób fizycznych – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych. Regulacje RODO nie dotyczą 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.

W trakcie prac nad OchrDanychU pojawiła się wątpliwość związana z tym, czy na gruncie motywu 14 RODO jego przepisy znajdują zastosowanie do osób fizycznych prowadzących działalność gospodarczą. Doprowadziło to do zadania Komisji Europejskiej pytania w tym przedmiocie. Komisja Europejska wskazała, że jeżeli w polskim porządku prawnym osoby fizyczne prowadzące działalność gospodarczą nie są osobami prawnymi, lecz fizycznymi, czyli nie mają charakteru spółek, to znaczy, że w pełni podlegają nowym przepisom o ochronie danych osobowych<sup>11</sup>.

<sup>10</sup> Zob. G. Sibiga, Dostosowywanie prawa polskiego do ogólnego rozporządzenia o ochronie danych, Warszawa 2016, <http://michalboni.pl/mboni/wp-content/uploads/2016/11/Opinia.pdf> (dostęp: 12.11.2018 r.), s. 22.

<sup>11</sup> Zob. <https://www.pb.pl/firma-kowalski-wylaczona-z-RODO-902931> (dostęp: 12.11.2018 r.); <https://przetwarzanie.danych.pl/warszawa/porady/osoby-fizyczne-prowadzace-dzialalnosc-gospodarcza-pod-ochrona-RODO> (dostęp: 12.11.2018 r.).



Wobec powyższego dane ewidencyjne<sup>12</sup> jednoosobowych przedsiębiorców, zawarte w CEiDG, będą stanowiły dane osobowe objęte zakresem zastosowania RODO. Zgodnie z art. 5 ust. 1 CEiIDGiPIPU są to następujące dane:

- 1) imię i nazwisko przedsiębiorcy, numer PESEL, o ile taki posiada, oraz data urodzenia, o ile nie posiada numeru PESEL,
- 2) dodatkowe określenia, które przedsiębiorca włącza do firmy, o ile przedsiębiorca takich używa,
- 3) oznaczenie „w spadku”, jeżeli został ustanowiony zarząd sukcesyjny,
- 4) numer identyfikacyjny REGON przedsiębiorcy, o ile taki posiada,
- 5) numer identyfikacji podatkowej (NIP) przedsiębiorcy, o ile taki posiada, oraz informacje o jego unieważnieniu lub uchyleniu,
- 6) informacja o obywatelstwie przedsiębiorcy,
- 7) adres do doręczeń oraz – jeżeli przedsiębiorca takie miejsce posiada – adres stałego miejsca wykonywania działalności gospodarczej; dane dotyczące adresu są zgodne z oznaczeniami kodowymi przyjętymi w krajowym rejestrze urzędowym podziału terytorialnego kraju, o ile to w danym przypadku możliwe,
- 8) inne niż wymienione w pkt 7 dane kontaktowe przedsiębiorcy, w szczególności adres poczty elektronicznej, adres strony internetowej, numer telefonu, o ile dane te zostały zgłoszone przez przedsiębiorcę we wniosku o wpis do CEiDG,
- 9) przedmiot wykonywanej działalności gospodarczej według PKD na poziomie podklasy, w tym jeden przedmiot przeważającej działalności.

Tak samo należy traktować dane jednoosobowych przedsiębiorców zawarte np. na ich stronach internetowych, fakturach czy w umowach handlowych, których są stroną.

## 4. Dane osobowe wynikające z Krajowego Rejestru Sądowego

W przeciwieństwie do CEiDG, w którym zawarte są wyłącznie dane osobowe osób fizycznych, w KRS zawarte są przede wszystkim dane dotyczące jednostek organizacyjnych, w tym osób prawnych. Zgodnie z art. 3 KRSU rejestr obejmuje podmioty, na które przepisy ustaw nakładają obowiązek uzyskania wpisu do KRS. W art. 36 KRSU wymieniono podmioty, które podlegają wpisaniu do rejestru przedsiębiorców KRS. Są to przede wszystkim spółki prawa handlowego (spółki jawne, spółki partnerskie, spółki komandytowe, spółki komandytowo-akcyjne, spółki z ograniczoną odpowiedzialnością oraz spółki akcyjne)<sup>13</sup>.

Choć dane takich podmiotów, zawarte w KRS (np. numer KRS, siedziba spółki z ograniczoną odpowiedzialnością), nie będą stanowiły danych osobowych, należy mieć na względzie, że w KRS znajdują się także dane osób pełniących różne funkcje, wynikające

---

<sup>12</sup> Dane informacyjne, wskazane w art. 5 ust. 2 CEiIDGiPIPU, także będą stanowiły dane osobowe osoby fizycznej prowadzącej działalność gospodarczą.

<sup>13</sup> Pełny katalog jest zawarty w art. 36 KRSU. Z uwagi na charakter niniejszego opracowania omówiono dane odnoszące się do spółek prawa handlowego.

z przepisów prawa, w ramach współpracy z podmiotami wpisanymi do KRS. Mianowicie ujawnieniu w KRS podlegają również:

- 1) oznaczenie wspólników spółki jawnej,
- 2) oznaczenie partnerów spółki partnerskiej,
- 3) oznaczenie wspólników spółki komandytowej,
- 4) oznaczenie komplementariuszy spółki komandytowo-akcyjnej,
- 5) oznaczenie wspólników posiadających samodzielnie lub łącznie z innymi co najmniej 10% kapitału zakładowego spółki z ograniczoną odpowiedzialnością oraz ilość posiadanych przez tych wspólników udziałów i łączną ich wysokość,
- 6) w przypadku gdy spółka akcyjna ma tylko jednego akcjonariusza – jego oznaczenie, a także wzmianka, że jest on jedynym akcjonariuszem spółki (art. 38 pkt 9 lit. h i pkt 9a lit. i KRSU),
- 7) oznaczenie organu uprawnionego do reprezentowania podmiotu oraz osób wchodzących w jego skład, ze wskazaniem sposobu reprezentacji, a w przypadku gdy w spółkach osobowych nie ma takiego organu – wskazanie wspólników uprawnionych do reprezentowania spółki, a także sposobu reprezentacji (art. 39 pkt 1 KRSU),
- 8) dane dotyczące prokurentów oraz rodzaju prokury (art. 39 pkt 3 KRSU).

Wskazanego oznaczenia osób dokonuje się zgodnie z art. 35 pkt 1 KRSU, czyli poprzez zamieszczenie w rejestrze ich nazwisk i imion oraz identyfikatorów nadanych w systemie ewidencji ludności, tj. numerów PESEL.

Wydawałoby się, że przedstawione kategorie informacji z założenia należy kwalifikować jako dane osobowe. Taka ocena jednak może budzić wątpliwości w kontekście powołanego wyżej motywu 14 RODO, wskazującego, że RODO nie obejmuje 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. Nie jest jasne, jak należy rozumieć pojęcie danych dotyczących osób prawnych, w tym danych kontaktowych osób prawnych. Jak trafnie wskazuje *J. Byrski*, możliwe są trzy wykładnie:

- 1) przez dane kontaktowe osoby prawnej rozumie się wyłącznie adres, e-mail, numer telefonu lub inne oznaczenia kontaktowe osoby prawnej,
- 2) chodzi dodatkowo o dane dotyczące osób fizycznych ujawnione i upublicznione (nie zaś wszystkie dane z rejestru publicznego), na podstawie przepisów prawa, w odpowiednim rejestrze publicznym (np. dane osobowe w rejestrze przedsiębiorców KRS),
- 3) mogą to być dodatkowo dane osobowe osoby fizycznej wyznaczonej do kontaktów w imieniu osoby prawnej, niekoniecznie ujawnione w rejestrze publicznym<sup>14</sup>.

Inni przedstawiciele doktryny, z jednej strony, wskazują, że nie ulega wątpliwości, że informacje o osobach fizycznych pełniących funkcje w organach osób prawnych odnoszą się nie tylko do osób prawnych, w których imieniu dana osoba fizyczna podejmuje czynności, lecz także do osób fizycznych. Jeżeli więc została spełniona przesłanka identyfikowalności osoby na podstawie ocenianych informacji, co w większości przypadków będzie

---

<sup>14</sup> Zob. <https://biznes.gazetaprawna.pl/artykuly/1177006,zgoda-na-przetwarzanie-danychw-ceidg-a-rodod.html>.

stanowiło zasadę, to informacje te należy uznać za dane osobowe. Z drugiej – stwierdzają, że zakresem wyłączenia zastosowania RODO do osób prawnych (w związku z motywem 14 RODO) powinny być objęte wszystkie dane osobowe gromadzone w KRS, a służące do oznaczenia takiego podmiotu. Wskazują przy tym, że przetwarzanie informacji o osobach fizycznych sprawujących funkcję organów osób prawnych nie może być uznane za działanie bezprawne dopóki, dopóty przetwarzanie takie odbywa się wyłącznie w celu i zakresie niezbędnym do prawidłowej identyfikacji tych osób jako pełniących funkcję organów osób prawnych<sup>15</sup>.

Na marginesie należy zaznaczyć, że kwestie „celu i zakresu” oraz braku „bezprawności” nie mają znaczenia dla przesądzenia, czy dojdzie do zastosowania RODO. Znaczenie we wskazanym w kontekście ma wyłącznie to, czy dojdzie do przetwarzania danych osobowych, a ewentualna ocena bezprawności przetwarzania może być poczyniona dopiero po przesądzeniu, że RODO znajdzie zastosowanie.

Z powyższego wynika, że definicja danych osobowych (uzupełniona kontekstem motywu 14 RODO) została ujęta zbyt szeroko. Niemniej – ze względu na brak odmiennego stanowiska organu nadzorczego przy wyżej wskazanych rozbieżnościach występujących z doktrynie – z ostrożności należy przyjąć, że **ujawnione w KRS dane osób fizycznych (wspólników spółek, członków zarządu itp.) będą stanowiły dane osobowe**, a nie będą mieściły się w zakresie pojęcia danych osoby prawnej. Ma to znaczenie w szczególności w kontekście obowiązku informacyjnego, którego realizacja w odniesieniu do osób ujawnionych w KRS może nastęrczać trudności. Zasygnalizowany problem jednak nie powinien przemawiać za brakiem kwalifikacji wskazanych informacji dotyczących osób fizycznych (imię, nazwisko, numer PESEL) do danych osobowych, a raczej za ewentualnym zastosowaniem wyłączenia zawartego w art. 14 ust. 5 RODO.

## 5. Korzystanie z danych zawartych w rejestrach publicznych do celów komercyjnych

Jak zaznaczono wyżej, należy odróżnić tworzenie rejestrów publicznych przez organy państwowe, działające na podstawie stosownych przepisów, od komercyjnego wykorzystania danych zawartych w rejestrach przez podmioty prywatne. W doktrynie podkreśla się, że istnienie komercyjnych baz danych, opartych na niezanonimizowanych danych pochodzących z rejestrów publicznych, nasuwa pytania dotyczące zakresu i zasad udostępniania danych osobowych z rejestrów publicznych oraz zgodności ich ponownego wykorzystywania z zasadą związania celem, która stanowi jedną z podstawowych zasad ochrony danych osobowych<sup>16</sup>. Wskazuje się również, że wcześniej do wielu formalnie jawnych rejestrów dostęp był faktycznie ograniczony ze względu na to, że był on możliwy jedynie w siedzibie sądu lub organu administracji publicznej. Publikowanie danych reje-

---

<sup>15</sup> P. Litwiński (red.), P. Barta, M. Kawecki, Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Legalis/el. 2018, komentarz do art. 4.

<sup>16</sup> A. Gryszczyńska (red.), Rejestry publiczne. Jawność i interoperacyjność, Warszawa 2016, s. 28.

strowych w sieci Internet powoduje niemal nieograniczony do nich dostęp, co umożliwia powiązanie tak opublikowanych informacji z informacjami pochodzącymi z innych źródeł i tworzenie profili osobowych, a w konsekwencji rodzi negatywne konsekwencje dla osób, których dane dotyczą. Publikowanie danych osobowych może także potencjalnie odrywać je od kontekstu, w którym zostały zebrane, i nadawać im inne niż pierwotne znaczenia, często zaskakujące osoby, których dane dotyczą<sup>17</sup>.

Powyższe zagadnienie w kontekście zapewnienia legalności przetwarzania było przedmiotem analizy NSA pod rządami OchrDanychU97. Zgodnie ze stanowiskiem NSA dane osób fizycznych (wspólników, członków zarządu itd.) wpisane do KRS (imię, nazwisko, numer PESEL, pełniona funkcja, data urodzenia) są danymi osobowymi, a zasady ich przetwarzania (zbierania, przekazywania, utrwalania, udostępniania i zmieniania) reguluje KRSU. Przepis art. 8 KRSU, wskazujący na jawność rejestru, nie upoważnia do przetwarzania danych osobowych zawartych w KRS w dowolnych celach.

### Orzecznictwo

---

Decydując się na umieszczenie swoich danych w KRS, przedsiębiorcy mają zaufanie, że ich dane będą ujawniane i wykorzystywane tylko w taki sposób, na jaki zezwala KRSU. [...] Ustawodawca nie może bowiem dopuścić do tego, że ochrona danych osobowych znajdujących się w KRS nie będzie ograniczona wobec podmiotów, które będą chciały wykorzystać te dane w innych celach i na innych zasadach niż dopuszcza to KRSU. Wówczas dopuszczono by także do sytuacji, w której dane z KRS mogłyby być w nieograniczony sposób wykorzystywane, bez woli osób w nich ujętych, w celu utworzenia bazy danych dla prowadzenia kampanii marketingowych.

[...] cele przetwarzania danych objętych KRS, a ujawnionych w Monitorze Sądowym i Gospodarczym, nie są tożsame z celami komercyjnymi, dla których dane te przetwarza (zbiera, utrwała, udostępnia itd.) skarżąca Spółka [tworząca komercyjną bazę] (wyr. NSA z 24.1.2013 r., I OSK 1827/11, Legalis).

---

Powyższy wyrok został wydany na kanwie oceny zasadności wyłączenia realizacji obowiązku informacyjnego z powołaniem się na sytuację, w której przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której te dane dotyczą (art. 25 ust. 2 pkt 1 OchrDanychU97). Nie przesądza on jednak o zakazie korzystania z rejestrów publicznych do celów komercyjnych i tworzenia baz o takim charakterze.

## 6. Firma przedsiębiorstwa/przedsiębiorcy jako dane osobowe

Zgodnie z art. 43<sup>1</sup> KC przedsiębiorcą jest osoba fizyczna, osoba prawna i jednostka organizacyjna, o której mowa w art. 33<sup>1</sup> § 1 KC, prowadząca we własnym imieniu działalność gospodarczą lub zawodową. Z kolei art. 43<sup>2</sup> § 1 KC wskazuje, że przedsiębiorca działa

---

<sup>17</sup> P. Drobek, Ryzyka dla ochrony danych osobowych w związku z ponownym wykorzystywaniem informacji sektora publicznego, (w:) A. Piskorz-Ryń (red.), *Jawność i jej ograniczenia. Dostęp i wykorzystywanie*, t. 5, Legalis/el. 2015.

pod firmą. Stosownie do art. 43<sup>4</sup> KC firmą osoby fizycznej jest jej imię i nazwisko. Nie wyklucza to włączenia do firmy pseudonimu lub określeń wskazujących na przedmiot działalności przedsiębiorcy, miejsce jej prowadzenia oraz innych określeń dowolnie obranych. Inaczej będzie w odniesieniu do osób prawnych – firmą osoby prawnej jest jej nazwa. Firma zawiera określenie formy prawnej osoby prawnej, które może być podane w skrócie, a ponadto może wskazywać na przedmiot działalności, siedzibę tej osoby oraz inne określenia dowolnie obrane (art. 43<sup>5</sup> § 1 i 2 KC).

Zatem firma jednoosobowego przedsiębiorcy, zawierająca imię i nazwisko (i inne określenia, np. kancelaria radcy prawnego), będzie stanowiła dane osobowe – jako informacja odnosząca się do konkretnej (możliwej do zidentyfikowania) osoby fizycznej. Takich informacji nie można uznać za dane dotyczące osoby prawnej, o których mowa w motywie 14 RODO, co (jak wyżej wskazano) wyraźnie przesądziła Komisja Europejska.

Natomiast firma (oznaczenie) osoby prawnej nie będzie stanowiła danych osobowych (np. ABC sp. z o.o.). Wątpliwości może budzić sytuacja, w której firma osoby prawnej będzie zawierać dane osoby fizycznej (Iksiński Budowa Maszyn sp. z o.o.). Jak stanowi art. 43<sup>5</sup> § 3 KC, firma osoby prawnej może zawierać nazwisko lub pseudonim osoby fizycznej, jeżeli służy to ukazaniu związków tej osoby z powstaniem lub działalnością przedsiębiorcy. Umieszczenie w firmie nazwiska albo pseudonimu osoby fizycznej wymaga pisemnej zgody tej osoby, a w razie jej śmierci – zgody jej małżonka i dzieci. Jak się wskazuje w doktrynie, celem wprowadzenia wskazanego przepisu było przede wszystkim dążenie do wyeliminowania spotykanych w praktyce przypadków nadużywania znanych nazwisk bez uzasadnienia (co prowadzi do naruszenia dóbr osobistych osób noszących te nazwiska)<sup>18</sup>. Regulacja art. 43<sup>5</sup> § 3 KC nie ma zatem nic wspólnego z przetwarzaniem danych osobowych w tym zakresie.

### Ważne

Umieszczenie nazwiska w firmie osoby prawnej nie będzie powodowało, że firma takiej osoby prawnej będzie stanowiła jej dane osobowe. Osoba prawna nie ma bowiem danych osobowych – niezależnie od tego, czy nazwisko lub inna kategoria danych znajdują się w jej firmie. Regulacje RODO nie znajdują bowiem zastosowania do danych przedsiębiorstw będących osobami prawnymi, w tym danych o firmie.

## 7. Dane osobowe pełnomocników i pracowników

W związku z prowadzeniem działalności biznesowej sprzedażowej lub marketingowej często dochodzi do przetwarzania danych pracowników kontrahentów/klientów. Można zastanawiać się, czy jeżeli do podejmowania działań biznesowych będą wykorzystywane dane o charakterze służbowym, to będzie dochodziło do przetwarzania danych osobowych, objętego zakresem stosowania RODO. Odpowiadając na to pytanie, można przy-

<sup>18</sup> M. Popiołek, komentarz do art. 43<sup>5</sup>, (w:) K. Pietrzykowski (red.), Kodeks cywilny. Komentarz art. 1–449<sup>10</sup>, t. 1, Warszawa 2013, s. 182, teza 7.

toczyć wyjaśnienia Komisji Europejskiej. Wskazała ona, że przepisy o ochronie danych mają zastosowanie wyłącznie do danych osobowych dotyczących osób fizycznych. Nie regulują przetwarzania danych dotyczących spółek ani żadnych innych osób prawnych. Niemniej informacje dotyczące jednoosobowej działalności gospodarczej mogą zawierać dane osobowe pozwalające na ustalenie tożsamości osoby fizycznej. Przepisy mają też zastosowanie do wszystkich danych osobowych dotyczących osób fizycznych w związku z ich działalnością zawodową, m.in. do danych pracowników zatrudnionych w przedsiębiorstwie/organizacji, służbowych adresów e-mail, typu: „imię.nazwisko@firma.eu”, lub numerów telefonów służbowych<sup>19</sup>.

W konsekwencji należy wskazać, że dane pracowników będących osobami kontaktowymi w ramach wykonywania umowy czy też np. dane pełnomocników osób prawnych – będących możliwymi do zidentyfikowania osobami fizycznymi – będą danymi osobowymi, podlegającymi zastosowaniu RODO, niezależnie od tego, czy będą to dane służbowe/dane przetwarzane w związku z zawieraniem umów z kontrahentem niebędącym osobą fizyczną (zob. wyr. TS z 9.3.2017 r., C-398/15, Legalis).

W tym kontekście interesujące jest stanowisko brytyjskiego organu nadzorczego, tj. ICO (Information Commissioner's Office/odpowiednik polskiego UODO), zgodnie z którym informacje dotyczące osoby prawnej – a nie osoby fizycznej – nie są danymi osobowymi. W związku z tym nie stanowią danych osobowych i nie wchodzi w zakres RODO informacja o spółce z ograniczoną odpowiedzialnością lub jednostce prawnej (*legal entity*), które mogą mieć osobowość prawną odrębną od właścicieli lub dyrektorów. Podobnie informacje o organie publicznym nie są danymi osobowymi. Przepisy RODO obejmują jednak dane osobowe osób fizycznych działających jako jednoosobowi przedsiębiorcy, pracownicy, partnerzy i dyrektorzy przedsiębiorstw, jeżeli informacje odnoszą się do nich jako osób fizycznych, a nie przedstawicieli osoby prawnej (*rather than as the representative of a legal person*)<sup>20</sup>. Nazwa i firmowy adres e-mail wyraźnie odsyłają do konkretnej osoby, a zatem są danymi osobowymi. Jednak treść wiadomości e-mail nie będzie automatycznie kwalifikowana jako dane osobowe, chyba że zawiera informacje, które ujawniają coś o tej osobie lub mają na nią wpływ<sup>21</sup>.

## 8. Informacje trudno identyfikowalne

Problem z danymi trudno identyfikowalnymi (niemożliwymi do łatwego, tj. bezpośredniego przypisania do wyodrębnionej osoby fizycznej) aktualny był już na gruncie przepisów implementujących dyrektywę 95/46/WE, które zawierały definicję danych osobo-

---

<sup>19</sup> Zob. [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company\\_pl](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_pl) (dostęp: 12.11.2018 r.).

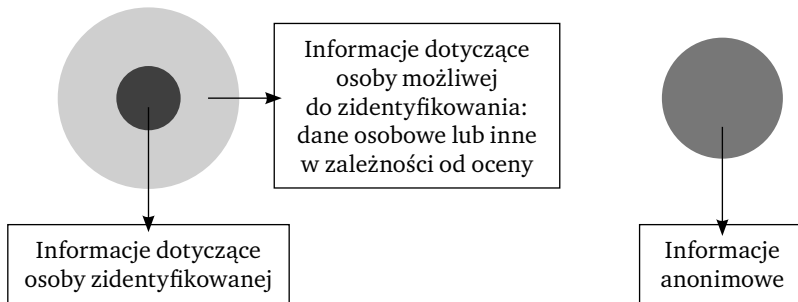
<sup>20</sup> Fragment: *rather than as the representative of a legal person* może dawać pewną podstawę do argumentacji, że w pewnych kontekstach dane osób reprezentujących osoby prawne mogą nie być kwalifikowane jako dane osobowe. Niemniej – w świetle przedstawionego stanowiska Komisji Europejskiej – takie stanowisko może być uznane za kontrowersyjne.

<sup>21</sup> Zob. ICO, What is personal data?, <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/> (dostęp: 12.11.2018 r.).

wych zbliżoną do tej z RODO. Chodzi o sytuację, gdy bez dodatkowych informacji (które musiałyby być pozyskane ze źródeł zewnętrznych dla administratora lub z wewnętrznych zasobów np. przeszukanie poszczególnych baz danych) nie istnieje możliwość przypisania danej informacji wyodrębnionej (odróżnionej od innych) osobie fizycznej.

Jak wskazano na wstępie, pojęcie danych osobowych obejmuje informacje dotyczące osób fizycznych, o różnym stopniu powiązania z tymi osobami, czyli nie tylko informacje dotyczące jednej (wyodrębnionej) osoby, np. identyfikatory typu numer PESEL czy kod genetyczny<sup>22</sup>. Pojęcie danych osobowych jest w istocie nieo określone. Na jednym biegunie – poza zakresem – znajdują się informacje anonimowe (tj. nieprzypisywane wyodrębnionej osobie fizycznej), a na drugim – informacje jednoznacznie mieszczące się w pojęciu danych osobowych (np. numer PESEL). Pomiędzy tymi biegunami jest pole szarości – wyznaczone możliwą identyfikacją osoby fizycznej. W tym obszarze mogą – ale nie muszą – znajdować się dane osobowe. Mieszczą się w nim np. dane pseudonimizowane.

**Rysunek 1.** Zakres pojęcia danych osobowych



Biorąc powyższe pod uwagę, pojawiają się następujące pytania:

- 1) czy każda informacja, która może być (choćby czysto hipotetycznie) przypisana osobie fizycznej, stanowi dane osobowe?<sup>23</sup>,
- 2) czy o przypisaniu informacji osobie fizycznej decyduje fakt, że administrator zna lub jest w stanie wskazać tę osobę?,

<sup>22</sup> Zgodnie z art. 87 RODO państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym. W takim przypadku krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje RODO.

<sup>23</sup> P. Litwiński (red.), P. Barta, M. Kawecki, Rozporządzenie UE w sprawie ochrony osób fizycznych..., komentarz do art. 4. Autorzy wskazują: „w literaturze przedmiotu znane jest zjawisko tzw. relatywizacji pojęcia danych osobowych [...], zgodnie z którym ta sama informacja może być różnie kwalifikowana z punktu widzenia definicji danych osobowych w zależności od tego, jaki podmiot tę informację przetwarza, jakimi środkami identyfikacji dysponuje, jakie jeszcze inne informacje przetwarza itp. Zjawisko to w pewnym sensie dotyczy także sytuacji, gdy ocenie prawnej podlega przetwarzanie informacji przez jeden podmiot, nie zaś przez kilka podmiotów – zwraca się bowiem uwagę na problem powstający wtedy, gdy jeden podmiot posiada dwie bazy danych, w których przetwarzane są informacje niestanowiące samodzielnie danych osobowych. Jednakże jeżeli w wyniku połączenia informacji pochodzących z tych baz danych powstanie sytuacja, w której osobę fizyczną można będzie zidentyfikować, wówczas informacje zawarte w obydwu bazach danych trzeba będzie uznać za dane osobowe”.