**Nowoczesne Systemy Zarządzania**
Zeszyt 14 (2019), nr 2 (kwiecień-czerwiec)
ISSN 1896-9380, s. 13-27

Instytut Organizacji i Zarządzania
Wydział Cybernetyki
Wojskowa Akademia Techniczna
w Warszawie

**Modern Management Systems**
Volume 14 (2019), No. 2 (April-June)
ISSN 1896-9380, pp. 13-27

Institute of Organization and Management
Faculty of Cybernetics
Military University of Technology

# Zarządzanie danymi osobowymi w przedsiębiorstwie

# Personal data management in the enterprise

**Janusz Rybiński**
Wojskowa Akademia Techniczna
Wydział Cybernetyki

**Abstrakt.** Działalność przedsiębiorstw jest regulowana wieloma przepisami prawa, z których w ostatnim okresie na pierwszy plan wysuwają się te dotyczące danych osobowych. Wprowadzenie RODO spowodowało, że ochrona danych osobowych nabrała nowego wymiaru i to niezależnie od pozostałych uwarunkowań prowadzenia działalności gospodarczej. W artykule przedstawiono próbę przybliżenia przepisów z zakresu ochrony danych osobowych, które dla wielu przedsiębiorców stanowią poważne wyzwanie. Ponadto skupiono się na problemach praktycznego funkcjonowania tych norm prawnych, które z założenia mają poprawić stan ochrony danych osobowych znajdujących się w dyspozycji przedsiębiorców nie tylko w naszym kraju.
**Słowa kluczowe:** dane osobowe, ochrona danych osobowych.

**Abstract.** The activity of enterprises is regulated by many legal provisions, from which personal data have been of the highest importance recently. The introduction of the GDPR meant that the protection of personal data has acquired a new dimension, regardless of the other conditions of doing business. The article presents an attempt to approximate the provisions on the protection of personal data, which are a serious challenge for many entrepreneurs. In addition, the focus was also on the problems of the practical functioning of these legal norms, which are intended to improve the protection of personal data at the disposal of entrepreneurs not only in our country.
**Keywords:** personal data, personal data protection.

## Wstęp

Działalność gospodarcza współczesnego przedsiębiorstwa jest regulowana wieloma przepisami prawa, z których w ostatnim czasie na pierwszym planie są te dotyczące danych osobowych. Wprowadzenie do naszego systemu prawnego nowelizacji ochrony danych osobowych w postaci RODO całkowicie zmieniło pogląd na ten problem. Ochrona faktycznie dotyczy wszystkich osób fizycznych, a także przedsiębiorców, stowarzyszeń i innych podmiotów, którzy dane osobowe posiadają, przetwarzają i korzystają z nich. Jednak to w przypadku przedsiębiorców dane osobowe stanowią podstawę prowadzenia działalności i są przedmiotem szczególnej troski. Dane pracowników, klientów, dostawców i innych osób związanych z firmą stanowią cenny zasób i zawsze powinny być przedmiotem szczególnej troski i w związku z tym ochrony.

System ochrony danych osobowych wykształcił się w Polsce po zmianach ustrojowych w 1989 r. Nowelizowano akty prawne, zmieniono także Konstytucję RP w celu stworzenia spójnych przepisów odpowiadających nowej sytuacji społeczno-ekonomicznej, w jakiej znalazł się nasz kraj. W związku z tym celem tego opracowania jest przedstawienie zmian w zakresie ochrony danych osobowych, a także przybliżenie przepisów, które już dzisiaj są standardem nie tylko w naszym kraju. Przepisy, które w Polsce obowiązują od 25 maja 2018 r., nie zawsze są interpretowane w sposób zgodny z intencją ustawodawcy. W związku z tym w miarę możliwości zostanie również pokazany aspekt praktyczny ich funkcjonowania.

Zmiana zasad ochrony danych osobowych w warunkach społeczeństwa informacyjnego, wszechobecnego Internetu, portali społecznościowych, dostępu do mediów społecznościowych coraz młodszych użytkowników nie budzi większych zastrzeżeń. Praktycznie wszyscy użytkownicy Internetu są zainteresowani ochroną swoich danych osobowych, podobnie jak klienci banków, sieci komórkowych i innych podmiotów, które dysponują naszymi danymi osobowymi. Problem zaczyna się wtedy, gdy dotyczy to nadinterpretacji prawa, jego stosowania niezgodnie z intencją ustawodawcy i innych wypaczeń z tego zakresu.

## 1. Geneza systemu ochrony danych osobowych

Od 1997 r. do polskiego prawa zostało włączonych wiele aktów prawnych, które regulowały problematykę danych osobowych. Zasadniczym była ustawa, której zadaniem była ochrona danych osobowych wszystkich obywateli. Jednocześnie zapewniała ona stosowanie Dyrektywy Parlamentu Europejskiego i Rady 95/46/EC z dnia 24 października 1995 r. w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych.

Wejście w życie ww. ustawy trwale zmieniło zasady ochrony danych osobowych i wykształciło system, na który złożyło się wiele aktów wykonawczych, które łącznie regulowały kwestie prawne dotyczące ochrony danych osobowych w kraju. W ten sposób ustawowo określono wiele istotnych kwestii dotyczących ochrony, do których można zaliczyć:

- zasady przetwarzania danych osobowych osób fizycznych;
- prawa osób fizycznych, których dane osobowe są przetwarzane lub mogą być przetwarzane w zbiorach danych;
- organy ochrony danych osobowych;
- miejsce, role i zadania, jakie ma do spełnienia Generalny Inspektor Ochrony Danych Osobowych;
- zasady bezpieczeństwa danych osobowych;
- zasady i tryb zgłaszania zbiorów danych do rejestracji;
- zasady przekazywania danych osobowych do państwa trzeciego;
- zasady odpowiedzialności na gruncie tych przepisów.

Ustawa i akty prawne wydane na jej podstawie stworzyły system ochrony danych osobowych. Złożyła się na niego wymieniona już ustawa oraz akty wykonawcze do ustawy, które w sposób szczegółowy uregulowały kwestie nieunormowane lub jedynie zasygnalizowane w ustawie[1]. Przykładem może być Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ten sam obszar regulowała również późniejsza ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 r., Nr 144, poz. 1204 z późniejszymi zmianami), a także Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. z 2011 r., Nr 159, poz. 948 z późniejszymi zmianami).

Zasadniczym aktem prawnym w naszym kraju jest Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483). System prawa tworzą także: Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r., Nr 112, poz. 1198 z późniejszymi zmianami) oraz Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych (Dz.U. z 2010 r., Nr 229, poz. 1497), która weszła w życie z dniem 7 marca 2011 r.

Wydane na tej podstawie rozporządzenia to: Rozporządzenie MSWiA z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej Inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych

[1] Ustawa skonkretyzowała konstytucyjnie zagwarantowane prawo do decydowania o tym, komu, w jakim zakresie i w jakim celu przekazywane są jego dane osobowe; wyposażyła osoby, których dane są wykorzystywane, w środki służące realizacji tego prawa, jak również powołała organ – Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

(Dz.U. z 2004 r., Nr 94, poz. 923) – wydane na podstawie art. 22a ustawy oraz Rozporządzenie MSWiA z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r., Nr 229, poz. 1536) – wydane na podstawie art. 46a ustawy.

Przedstawiając genezę systemu ochrony danych osobowych, należy wymienić akty prawa międzynarodowego, ponieważ to zmiany konwencji, dyrektyw lub rozporządzeń stawały się podstawą nowelizacji przepisów krajowych. Do tego typu podstaw prawa należy zaliczyć Konwencję nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, która została sporządzona w Strasburgu (Dz.U. z 2003 r. Nr 3, poz. 25) i jest zasadniczym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia ochrony danych osobowych.

Problematykę przetwarzania danych osobowych oraz ochronę prywatności w dziedzinie telekomunikacji regulowała Dyrektywa 97/66WE Parlamentu Europejskiego i Rady z dnia 15.12.1997 r. (Dz.Urz. WE L24 z 30 stycznia 1998 r.). Natomiast Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady WE z dnia 8 czerwca 2000 r. regulowała niektóre aspekty prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku (Dz.Urz. WEL 178 z 17 lipca 2000 r.).

Wymieniając regulacje prawne, należy również pamiętać o ostatniej z nich – właśnie o Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 RODO).

Wszystkie te wymienione i niewymienione z nazwy akty prawne regulowały problematykę ochrony naszych danych osobowych. Znalazły się tu zarówno obowiązki związane z nadzorem administratorów, którzy zarządzają danymi osobowymi, jak i zasady ich przetwarzania, przechowywania, zabezpieczania oraz rejestracji zbiorów danych, a także zasady ich przekazywania za granicę oraz odpowiedzialności karnej za naruszenia na gruncie ustawy o ochronie danych osobowych (Rybiński, 2007, s. 59).

## 2. Stan prawny po wprowadzeniu Rozporządzenia o ochronie danych osobowych

Ochrona danych osobowych w przepisach prawa pojawiła się w II połowie XX wieku, kiedy w Unii Europejskiej opracowano zasady dotyczące tej problematyki. Wcześniej nie była ona znana. Jednak na początku XX wieku, pomimo zauważenia tej problematyki, nie opracowano rozwiązania w postaci całościowych

– kompleksowych przepisów. W tym kontekście warto wymienić fragmentaryczne regulacje z późniejszego okresu, które pojawiają się w dokumentach prawnych ONZ[2].

Proces legislacyjny z zakresu ochrony danych osobowych rozpoczęła wymieniana już Dyrektywa 95/46/EC z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu danych. Następnym krokiem było przyjęcie polskiej ustawy o ochronie danych osobowych 29 sierpnia 1997 r. Propozycje całościowych zmian systemu w całej Unii Europejskiej zostały zainicjowane 4 listopada 2010 r., a 25 stycznia 2012 r. rozpoczęto dyskusję nad propozycjami kompleksowych zmian.

Przepisy tej ustawy weszły w życie z dniem 1 stycznia roku następnego. Obowiązujące aktualnie przepisy RODO uchwalono 26 kwietnia 2016 r. z terminem wejścia w życie z dniem 25 maja 2018 r. RODO dotyczy wszystkich podmiotów, które w związku z prowadzoną działalnością gospodarczą przetwarzają dane osobowe. Jednocześnie przestała obowiązywać Dyrektywa 95/46EC w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych z 1995 roku.

Wprowadzając do systemu prawa Rozporządzenie Parlamentu i Rady UE 2016/679, wprowadzono także Dyrektywę Parlamentu i Rady UE 2016/680. Stan prawny to też polska ustawa o ochronie danych osobowych z 10 maja 2018 r., a także wiele rekomendacji protokołów, wytycznych i stanowisk, tworzących system prawny w Unii Europejskiej. Wymienione akty prawa wchodzą po raz pierwszy do polskiego systemu prawa, w związku z czym wymagają bardziej precyzyjnego przedstawienia.

Rozporządzanie Parlamentu i Rady UE 2016/679 zawiera 99 artykułów i 173 motywy i składa się z 11 rozdziałów: Przepisy ogólne (art. 1-4); Zasady (art. 5-11); Prawa osoby, której dane dotyczą (art. 12-23); Administrator i podmiot przetwarzający (art. 24-43); Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych (art. 44-50); Niezależne organy nadzorcze (art. 51-59); Współpraca i spójność (art. 60-76); Środki ochrony prawnej, odpowiedzialność i sankcje (art. 77-84); Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem (art. 85-91); Akty delegowane i akty wykonawcze (art. 92-93); Przepisy końcowe (art. 94-99).

Następnym aktem prawnym jest Dyrektywa Parlamentu i Rady UE 2016/680, która zawiera 65 artykułów oraz 107 motywów i składa się z 10 rozdziałów: Przepisy ogólne (art. 1-3); Zasady (art. 4-11); Prawa osoby, której dane dotyczą (art. 12-18); Administrator i podmiot przetwarzający (art. 19-34); Przekazywanie danych

[2] Przykładem tego typu regulacji może być Rezolucja 45/95 Zgromadzenia ogólnego ONZ z dnia 26 czerwca 1985 r., która zawiera wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych. Jak wszystkie tego typu dokumenty, nie posiadały charakteru wiążącego, a jedynie stanowiły zalecenia odnośnie do gwarancji, jakie powinny być zapewnione w przepisach krajowych.

osobowych do państw trzecich lub organizacji międzynarodowych (art. 35-40); Niezależne organy nadzorcze (art. 41-49); Współpraca (art. 50-51); Środki ochrony prawnej, odpowiedzialność prawna i sankcje (art. 52-57); Akty wykonawcze (art. 58); Przepisy końcowe (art. 59-65).

Kolejnym aktem prawnym jest Ustawa o ochronie danych osobowych zapewniająca stosowanie rozporządzania Parlamentu Europejskiego i Rady 2016/679, które obowiązuje w polskim porządku prawnym bezpośrednio i zawiera następujące regulacje: Ograniczenia lub wyłączenia przepisów ustawy lub RODO (art. 2-6); Inspektor ochrony danych (art. 8-11); Certyfikacja w zakresie ochrony danych osobowych, o której mowa w art. 42 RODO (art. 12-26); Kodeks postępowania (art. 40 RODO) (art. 27-33); Prezes Urzędu Ochrony Danych Osobowych (art. 34-59); Postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych (art. 60-74); Kontrola przestrzegania przepisów (art. 78-91).

Stan prawny po wprowadzeniu RODO to także wiele innych przyjętych rekomendacji, wytycznych i stanowisk. Przykładowe to:

- Protokół dodatkowy do Konwencji Rady Europy Nr 108 z dnia 28 stycznia 1981 r.;
- Skonsolidowany tekst Rozporządzenia PE i Rady (UE) 2016/679 z 27 kwietnia 2016 r.;
- Sprostowanie do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r.;
- Rekomendacja Rady Europy z dnia 1 kwietnia 2015 dotycząca ochrony danych osobowych w sektorze zatrudnienia;
- Rekomendacja R(10) z dnia 23 listopada 2010 r. dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili;
- Rekomendacja R(02) 9 z dnia 18 września 2002 r. dotycząca ochrony danych osobowych zbieranych i przetwarzanych dla celów ubezpieczeniowych;
- Rekomendacja R(87) 15 Komitetu Ministrów Rady Europy dotycząca ochrony danych osobowych wykorzystywanych w sektorze policji z 17 września 1987 roku;
- Rekomendacja R(86) 1 z dnia 23 stycznia 1986 r. dotycząca ochrony danych osobowych dla potrzeb ubezpieczenia społecznego;
- Rekomendacja R(85) 20 z dnia 25 października 1985 r. dotycząca ochrony danych osobowych wykorzystywanych dla potrzeb marketingu bezpośredniego;
- Rekomendacja R(99) 5 Komitetu Ministrów dla Państw Członkowskich dotycząca ochrony prywatności w Internecie, wytyczne w sprawie ochrony osób w zakresie gromadzenia i przetwarzania danych osobowych na „infostradach";

- Rekomendacja R(97) 18 Komitetu Ministrów dla Państw Członkowskich dotycząca ochrony danych osobowych gromadzonych i przetwarzanych dla celów statystycznych;
- Rekomendacja R(97) 5 Komitetu Ministrów dla Państw Członkowskich dotycząca ochrony danych osobowych;
- Rekomendacja R(91) 10 I Nota wyjaśniająca Komitetu Ministrów dla Państw Członkowskich dotycząca udostępniania osobom trzecim danych osobowych będących w posiadaniu instytucji publicznych;
- Rekomendacja R(91) 10 z dnia 9 września 1991 r. dotycząca ochrony danych osobowych przekazywanych osobom trzecim przez instytucje publiczne;
- Rekomendacja R(87) 15 z dnia 17 września 1987 r. dotycząca ochrony danych osobowych wykorzystywanych w sektorze policji (udo, 2019).

## 3. Wybrane regulacje Rozporządzenia o ochronie danych osobowych dotyczące przedsiębiorców

Dla istnienia organizacji, przedsiębiorstwa lub firmy, jak często się potocznie mówi, najważniejsza jest działalność, która jednoznacznie kojarzona jest z zarządzaniem. Definiowane jest ono jako zestaw działań (obejmujący planowanie i podejmowanie decyzji, organizowanie, przewodzenie i kontrolowanie) skierowanych na zasoby organizacji (ludzkie, finansowe, rzeczowe i informacyjne) i wykonywanych z zamiarem osiągnięcia jej celów w sposób sprawny i skuteczny (Griffin, 2006, s. 6).

Również zgodnie z wieloma definicjami w tym zakresie najważniejszym zasobem organizacji są jednak ludzie, którzy realizują jej cele (Piotrkowski, 2006, s. 131). Mając na uwadze te wydawałoby się oczywiste fakty dotyczące organizacji, funkcji zarządzania w kontekście zatrudnionych osób, również RODO ze swoimi regulacjami wpisuje się w ten tok myślenia. Tworząc przepisy, kierowano się właśnie wzmocnieniem podstawowych praw obywateli w epoce cyfrowej.

W stosunku do organizacji zakładano głównie ułatwienie ich działalności na wspólnym rynku. Ważnym elementem jest także uzyskanie odpowiedzi na wiele pytań z tego zakresu, np. jak RODO reguluje podstawowe wymogi?, czy wpływa to na wizerunek przedsiębiorstwa?, jakie w związku z tym posiada obowiązki jako administrator danych?, jakie są obowiązki administratora w stosunku do osób fizycznych? Istotne kwestie to także odpowiedzialność za złamanie przepisów, która w stosunku do przedsiębiorstw jest bardzo dotkliwa, ponieważ za naruszenie postanowień RODO można nałożyć na przedsiębiorstwo kary pieniężne.

W zależności od okoliczności naruszenia, do których należą m.in.: charakter, czas i waga naruszenia, umyślność lub nieumyślność podmiotu, wdrożone u administratora środki organizacyjne oraz techniczne, czy też sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, a w szczególności to, czy i w jakim zakresie przedsiębiorca zgłosił

naruszenie, kara pieniężna jest różna. Może wynieść do 10 000 000 euro, w przypadku przedsiębiorstwa do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, lub w przypadku większych naruszeń nawet do 20 000 000 euro, w przypadku przedsiębiorstwa do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (*Gotowi na RODO*, 2018, s. 32).

W odpowiedzi na tego typu wątpliwości ukazało się kilka komentarzy na stronach internetowych lex-europa[3]. Z zamieszczonych tam informacji wynika, że Rozporządzenie o ochronie danych osobowych „ma na celu tworzenie możliwości dla firm i pobudzanie innowacyjności za pośrednictwem szeregu kroków, w tym":

- jeden zbiór ogólnounijnych przepisów – jedno ogólnounijne prawo dotyczące ochrony danych ma przynieść oszczędności w wysokości 2,3 mld euro rocznie;
- inspektor ochrony danych, odpowiedzialny za ochronę danych, zostanie wyznaczony przez władze publiczne i firmy zajmujące się przetwarzaniem danych na dużą skalę;
- kompleksowa współpraca – firmy kontaktują się tylko z jednym organem nadzorczym (w kraju UE, w którym prowadzą główną działalność);
- przepisy UE dla firm spoza UE – firmy z siedzibą poza UE stosują te same przepisy przy oferowaniu towarów i usług lub przy monitorowaniu zachowania osób w UE;
- przepisy sprzyjające innowacji – gwarancja, że zabezpieczenia chroniące dane są wbudowane w produkty i usługi od najwcześniejszego etapu rozwoju (ochrona danych w fazie projektowania oraz domyślna ochrona danych);
- technologie sprzyjające prywatności, takie jak pseudonimizacja (gdy obszary identyfikacji w danym wpisie zastępowane są jednym lub wieloma sztucznymi identyfikatorami) oraz szyfrowanie (gdy dane są kodowane w sposób umożliwiający ich odczytanie tylko osobom upoważnionym);
- usuwanie powiadomień – nowe przepisy dotyczące danych osobowych usuną większość obowiązków zawiadamiania i koszty z nimi związane. Jednym z celów rozporządzenia w sprawie ochrony danych jest usuwanie przeszkód utrudniających swobodny przepływ danych osobowych w UE. Ułatwi to rozwój przedsiębiorstw;
- ocena skutków – firmy będą przeprowadzać oceny skutków, gdy przetwarzanie danych może skutkować dużym ryzykiem naruszenia praw i swobód osób;
- rejestrowanie – MŚP nie są zobowiązane do rejestrowania czynności związanych z przetwarzaniem danych, chyba że takie przetwarzanie ma regularny charakter lub może skutkować ryzykiem naruszenia praw i swobód osób, których dane są przetwarzane (eur-lex.europa).

[3] W przypadku tych przepisów w roku ich wydania pojawiły się jedynie komentarze i oczywiście teksty dokumentów prawnych, w związku z tym platformy internetowe są jak do tej pory jedynymi źródłami, z których można czerpać wiedzę na ten temat.

Rozporządzenie odnosi się do wielu kwestii, które zawierały przepisy wcześniej obowiązujące, jednak w ich zapisach znajdują się regulacje ogólnie wpisujące się w istotę przyjętych założeń. W celu określenia, które mają zastosowanie do przedsiębiorstwa, zostaną omówione najważniejsze z nich.

„Dane osobowe" oznaczają 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 (RODO, art. 40).

W praktycznym podejściu oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, czyli mamy do czynienia z osobą i możliwością jej zidentyfikowania. W definicji zawarto również element uzasadniający prawdopodobieństwo identyfikacji. Danych osobowych nie stanowią informacje: zagregowane, statystyczne, dane osoby zmarłej (motyw 27 RODO), dane osobowe osoby prawnej – przedsiębiorcy (motyw 14 RODO). Do danych osobowych wrażliwych nie należy zaliczać tych, które można nazwać danymi „drażliwymi", jak: wiek osoby, jej stan cywilny, numer konta bankowego, posiadany majątek.

Przetwarzanie z kolei oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, są to: 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 (eur-lex.europa).

Z treści tej definicji wynika kilka praktycznych wniosków. Każda osoba, która będzie przetwarzała dane osobowe, powinna zostać upoważniona do ich przetwarzania przez administratora danych osobowych (ADO). Upoważnienie należy wydać, zanim dana osoba zacznie przetwarzać dane osobowe. Osoby upoważnione do przetwarzania danych osobowych są zobowiązane do ochrony danych zarówno w trakcie trwania zatrudnienia, jak i po zwolnieniu z pracy z różnych przyczyn.

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 (eur-lex.europa). Administrator danych oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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 (eur-lex.europa).

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:

- osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią… Akapit ten nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań (RODO, art. 6).

RODO wskazuje zasady, jakimi należy się kierować, przetwarzając dane osobowe. Muszą one być:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą – „zgodność z prawem, rzetelność i przejrzystość";
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie możliwe jest jedynie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą – „ograniczenie celu";
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane – „minimalizacja danych";
- prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane – „prawidłowość";
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane – „ograniczenie przechowywania";
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych – „integralność i poufność".

Administrator jest odpowiedzialny za przestrzeganie przepisów, w tym ww. zasad, i musi być w stanie wykazać ich przestrzeganie – „rozliczalność" (RODO, art. 6).

Nieco szerzej potraktowano zasady przetwarzania szczególnych kategorii danych osobowych (RODO, art. 6). Określono, że jest to dozwolone, jednak w celu ich przetwarzania musi być spełniony jeden z poniższych warunków:

- osoba, której dane dotyczą, dała wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach;
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą;
- przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot;
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego;
- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej;
- przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych;
- przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych (RODO, art. 9).

Cały rozdział III Rozporządzenia o ochronie danych osobowych został przeznaczony na regulacje związane z prawami osób, których dane dotyczą (RODO, art. 9). W tym zakresie RODO nadało podmiotom danych następujące prawa:

- Prawo do usunięcia danych, „prawo do bycia zapomnianym" – występuje wówczas, gdy: dane osobowe nie są już niezbędne do celów, w których zostały zebrane, osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania, nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania, dane osobowe były przetwarzane niezgodnie z prawem, muszą one zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie.

- Prawo do przenoszenia danych – prawo to polega na tym, że osoba ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dotyczące jej dane osobowe, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe (przetwarzanie odbywa się na podstawie zgody, umowy lub w sposób zautomatyzowany).
- Prawo do ograniczenia przetwarzania – prawo polega na tym, że osoba, której dane są przetwarzane, może żądać od administratora ograniczenia przetwarzania jej danych osobowych, np. w przypadku, gdy przetwarzanie jest niezgodne z prawem.
- Prawo do sprostowania i uzupełnienia danych – osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych lub ich sprostowania.
- Prawo dostępu przysługujące osobie, której dane dotyczą – prawo to polega na tym, że osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są jej dane osobowe, ma prawo do uzyskania dostępu do nich oraz uzyskania takich informacji jak m.in: cele przetwarzania, kategorie odnośnych danych osobowych, informacje o odbiorcach.

Z punktu widzenia administratorów danych bardzo ważne są regulacje związane z obowiązkiem informacyjnym, który RODO nałożyło na administratorów. Z treści tego aktu prawnego wynika, że obowiązek informacyjny można spełnić w formie tzw. klauzuli informacyjnej. Natomiast ten obowiązek co do zasady należy spełnić wobec każdej osoby, której dane są przetwarzane.

W przypadku pozyskiwania danych osobowych od osoby lub z innych źródeł na administratorze ciąży obowiązek poinformowania osoby m.in. o: swojej tożsamości i danych kontaktowych, danych kontaktowych inspektora ochrony danych, celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania, odbiorcach danych osobowych, prawach wynikających z RODO, a także źródłach pozyskania danych (RODO, art. 13 i 14).

Z pozostałych regulacji na uwagę zasługują obowiązki administratora i współadministratorów. W przedsiębiorstwie istnieje zasada zawarta w przepisach, że wyznacza się inspektora ochrony danych osobowych, któremu przydzielono liczne obowiązki. Rozporządzenie zwraca także dużą uwagę na właściwe formułowanie umowy powierzenia w zakresie przetwarzania danych osobowych, która również obwarowana została licznymi regulacjami. W tym zakresie warto przypomnieć, że przedsiębiorstwa miały czas na wdrożenie przepisów rozporządzenia. Faktem jest, że czas ten został wykorzystany w różny sposób. W lepszej sytuacji były większe firmy, np. Google, które „potrafiły lepiej zaadaptować się do nowych warunków niż inni gracze rynku AdTech. W wyniku tego nastąpiła większa konsolidacja branży Big Data i ograniczenie roli małych podmiotów" (Gut, 1019, s. 26-27).

Interesujące wnioski przekazała prezes Urzędu Ochrony Danych Osobowych dr Edyta Bielak-Jomaa, która oceniając pół roku funkcjonowania RODO, stwierdziła, że dokonała się „zmiana podejścia do zarządzania danymi osobowymi, uporządkowanie działań w tym zakresie, coraz częstsze korzystanie przez nas z praw, które gwarantuje nam RODO, to tylko kilka przykładów korzyści, które wynikają z rozpoczęcia stosowania nowego prawa". Ponadto wiele podmiotów (przedsiębiorców i administracja publiczna) wprowadziło cenne rozwiązania, które sprzyjają lepszej ochronie danych osobowych (uodo, 2019).

W zaleceniach dotyczących ochrony danych osobowych prezes stwierdziła, że należy jednak pracować nad doskonaleniem stosowanych rozwiązań i procedur. Warto więc skupić uwagę na pogłębianiu przepisów dotyczących danych osobowych, w tym RODO, a także korzystać ze swobody działania i elastyczności, jaką dają przepisy ogólnego rozporządzenia. Warto też uwzględniać zagrożenia, jakie dla ochrony danych osobowych niesie korzystanie z nowoczesnych technologii i Internetu, w tym przez coraz młodszych użytkowników (uodo, 2019).

## Podsumowanie

W zakresie ochrony danych osobowych w ostatnim czasie zmieniło się bardzo dużo. Najważniejszą zmianę przyniosło wejście przepisów RODO z dniem 25 maja 2018 r. Wprowadzenie tych przepisów do polskiego porządku prawnego kończy pewną epokę w tym zakresie. Najważniejszy problem to zmiana polegająca na ewolucji, a nie rewolucji. Do tej pory funkcjonował system ochrony danych osobowych, jednak zmiany zostały wprowadzone nie bez powodu. Stały się odpowiedzią na gwałtownie zmieniające się możliwości społeczeństwa informacyjnego, globalizację, dostęp do portali społecznościowych, w tym coraz młodszych użytkowników, zwiększenie zagrożeń dla bezpieczeństwa danych osobowych, Internet rzeczy (IoT) (właściwie danych) i związane z tym niebezpieczeństwa, a główny cel to przystosowanie Europy do ery cyfrowej.

Jeżeli chodzi o dokumenty, to przyjęte rozwiązania prawne wprowadzają radykalne zmiany zarówno w sensie merytorycznym, jak i formalnym (bezpośrednie zastosowanie ogólnego rozporządzania UE, bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego, nie wymaga też implementacji). W związku z tym jedynym aktem prawnym po wprowadzeniu ogólnego rozporządzenia stała się wymieniana wcześniej ustawa o ochronie danych osobowych z 10 maja tego samego roku. Jednak ustawa ma jedynie na celu regulowanie kwestii prawnych związanych z ochroną danych osobowych i zapewnienie stosowania w naszym kraju przepisów ogólnego rozporządzenia o ochronie danych osobowych – RODO.

W stosunku do przedsiębiorców rozporządzenie wprowadza wiele zmian, do których można zaliczyć: rozszerzenie definicji pojęcia danych osobowych, tak by

uwzględniała ona możliwości rozwoju technologicznego i pojawienie się nowych form identyfikacji; pozyskiwanie zgody na przetwarzanie danych osobowych; obowiązek wyznaczania inspektora ochrony danych; podejście oparte na ryzyku; obowiązek zgłaszania naruszeń (organowi nadzorczemu, administratorowi danych) i powiadamiania podmiotu danych; wprowadzenie nieznanego wcześniej prawa do „bycia zapomnianym"; uproszczenie przepisów dotyczących międzynarodowego przekazywania danych osobowych; doprecyzowanie obowiązków podmiotów przetwarzających dane; prawo dostępu do danych, poprawiania ich, uzupełniania i przenoszenia między systemami, a także ochrony prywatności w fazie projektowania.

## BIBLIOGRAFIA

[1] Barta J., Markiewicz R., 2001, *Ochrona danych osobowych. Komentarz*, Wyd. Zakamycze.

[2] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług w społeczeństwie informacyjnym, a w szczególności handlu elektronicznego w obrębie wolnego rynku (Dz.Urz. WEL 178 z 17 lipca 2000 r.).

[3] Dyrektywa 97/66WE Parlamentu Europejskiego i Rady z dnia 15.12.1997 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w dziedzinie telekomunikacji (Dz.Urz. WE L24 z 30 stycznia 1998 r.).

[4] Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/EC) w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych (Dz.Urz. WE L 281 z 23 listopada 1995 r.).

[5] Dyrektywa Parlamentu i Rady UE 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych związanych z czynami zabronionymi i do celów wykonywania kar oraz w sprawie swobodnego przepływu takich danych.

[6] *Gotowi na RODO*, podręcznik, Wyd. Generalnego Inspektora Ochrony Danych Osobowych.

[7] Griffin R.W., 2006, *Podstawy zarządzania organizacjami*, Wydawnictwo Naukowe PWN, Warszawa.

[8] Gut M., *RODO w ekosystemie programmatic – wygrani, przegrani*, „Media & Marketing Polska", Nr 1(473).

[9] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483).

[10] Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2003 r. Nr 3, poz. 25).

[11] Piotrkowski K., 2006, *Organizacja i zarządzanie*, Wydawnictwo AlmaMer, Warszawa.

[12] Rezolucja 45/95 Zgromadzenia ogólnego ONZ z dnia 26 czerwca 1985 r., zawierająca wytyczne w sprawie uregulowania kartotek skomputeryzowanych danych osobowych.

[13] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., Nr 100, poz. 1024).

[14] Rozporządzenie MSWiA z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. z 2008 r., Nr 229, poz. 1536) – wydane na podstawie art. 46a ustawy – określa wzór zgłoszenia, który jest załącznikiem do tego rozporządzenia.

[15] Rozporządzenie MSWiA z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. z 2004 r., Nr 94, poz. 923) – wydane na podstawie art. 22a ustawy – określa wzory, o których mówi to rozporządzenie.

[16] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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).

[17] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. z 2011 r., Nr 159, poz. 948).

[18] Rybiński J., 2007, *System zarządzania innowacjami w resorcie obrony narodowej*, Wyd. WAT, Warszawa.

[19] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. Nr 144, poz. 1204 z późniejszymi zmianami).

[20] Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych (Dz.U. z 2010 r., Nr 229, poz. 1497), ustawa weszła w życie w dniu 7 marca 2011 r.

[21] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 1997 r., Nr 133, poz. 883 z późniejszymi zmianami).

[22] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r., Nr 112, poz. 1198 z późniejszymi zmianami).

[23] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).

NETOGRAFIA

[1] https://eur-lex.europa.eu/content/help/faq/intro.html?locale=pl (12.02.2019).

[2] https://uodo.gov.pl/pl/131 (12.02.2019).

[3] https://uodo.gov.pl/pl/138/589 (12.02.2019).