Studia i Materiały, 2/2017 (25), cz. 2: 106–118
ISSN 1733-9758, © Wydział Zarządzania UW
DOI 10.7172/1733-9758.2017.25.10

# Wyzwania dla ochrony danych osobowych w obrocie gospodarczym przed wejściem w życie Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO)

*Zuzanna Sumińska*[*], *Igor Postuła*[**]

*Artykuł dotyczy problematyki ochrony danych osobowych w działalności gospodarczej. Autorzy analizują problemy definicji i zakresu podmiotowego ochrony danych osobowych oraz dylematu związanego z pogodzeniem ochrony danych osobowych i jawności danych przedsiębiorcy. Analiza i rozważania koncentrują się także na problematyce przetwarzania danych osobowych w relacji pracodawca–pracownik oraz ochrony danych osobowych w Internecie. Autorzy, odnosząc się do mającego wejść w życie w maju 2018 r. Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO), wskazują wyzwania dotyczące analizowanych problemów oraz nowe rozwiązania, które mają na celu ułatwienie zarządzania danymi osobowymi oraz ich skuteczną ochronę.*

**Słowa kluczowe:** bezpieczeństwo, ochrona i przetwarzanie danych osobowych, przedsiębiorca.

Nadesłany: 10.09.17 | Zaakceptowany do druku: 29.12.17

## Challenges for the protection of personal data in the economic turnover before the entrance into force of the General Data Protection Regulation (GDPR)

*This article concerns personal data protection issues in business. The authors analyze problems regarding definition and scope of personal data protection together with the dilemma associated with reconciliation of it with the transparency of entrepreneur's data. The analysis and considerations are also focused on the issue of personal data processing in the employer-employee relationship and the protection of personal data on the Internet. Referring to the General Data Protection Regulation (GDPR), that is to be implemented in May 2018, the authors indicate challenges with regards to the analyzed problems and new solutions that aim at facilitating the management of personal data and their effective protection.*

**Keywords:** security, protection and processing of personal data, entrepreneur.

Submitted: 10.09.17 | Accepted: 29.12.17

**JEL:** K2

[*] **Zuzanna Sumińska**, mgr – Wydział Zarządzania Uniwersytetu Warszawskiego.
[**] **Igor Postuła**, dr hab. – Uniwersytet Warszawski, Wydział Zarządzania.
*Adres do korespondencji*: Uniwersytet Warszawski, Wydział Zarządzania UW, ul. Szturmowa 1/3, 02-678 Warszawa; e-mail: ipostula@wz.uw.edu.pl.

## 1. Wprowadzenie

Ochrona prywatności jednostki jest zaliczana do podstawowych praw człowieka i jako fundamentalne prawo w większości współczesnych systemów prawnych podlega ochronie. Zagwarantowane jest ono w prawie międzynarodowym, europejskim oraz polskim i w ujęciu normatywnym zakłada swobodę jednostki w kształtowaniu jej życia prywatnego bez ingerencji osób trzecich (Prynciak, 2010, s. 211).

W obecnych czasach każdy jest uwikłany w ciąg przeróżnych aktywności wymagających gromadzenia danych osobowych. Gromadzone są one głównie w bazach informatycznych, a nieumieszczenie ich tam uniemożliwia funkcjonowanie jednostki. Jako przykład można podać funkcjonujący w Polsce Powszechny Elektroniczny System Ewidencji Ludności (PESEL) będący centralnym zbiorem danych gromadzącym informacje identyfikujące tożsamość oraz status administracyjno-prawny osób fizycznych. Dodatkowo, decydując się na prowadzenie działalności gospodarczej, osoba fizyczna musi liczyć się z ograniczeniem tej ochrony z uwagi na obowiązujące powszechnie prawo do informacji publicznej.

Pojawienie się nowoczesnych technologii, w tym zautomatyzowanych mechanizmów przetwarzania danych osobowych, stało się impulsem do objęcia danych osobowych samodzielną ochroną. Gromadzone informacje zaczęły przybierać na wartości, a kontrola ich obiegu i treści stała się zagrożeniem dla jednostek. Pojawił się zatem problem wyznaczenia granic prywatności oraz wzmocnienia metod jej ochrony przed ingerencją osób trzecich. Jak stwierdził N. Brieskorn – celem państwa stało się ukształtowanie systemu ochrony danych osobowych w taki sposób, aby dostosować go do potrzeb człowieka i zapewnić mu możliwość swobodnego rozwoju oraz zmian (Briekskorn, 1999, s. 208–210). Współcześnie instrumenty zapewniające prawo do prywatności oraz ochrony danych osobowych są w znaczącym zakresie rozbudowane, jednak równocześnie państwa znajdują powody, aby w te prawa także ingerować.

Okazuje się więc, że swoboda dzielenia się informacjami jest pozorna, ponieważ bywa, że jesteśmy zmuszeni do wyjawienia pewnych danych osobowych, mając nadzieję, że będą one poprawnie chronione przed ingerencją osób do tego nieupoważnionych. Nie można tego jednak rozpatrywać jedynie w negatywnym świetle. Niekiedy wręcz oczekujemy, aby nasze dane pojawiły się w systemie informatycznym, co umożliwi ich szybsze przetwarzanie, chociażby po to, abyśmy nie byli zmuszeni do wypełniania setek formularzy, podając w każdym te same dane. Istotne jest jednak, aby informacje były odpowiednio zabezpieczone i niedostępne dla nieupoważnionych osób.

Mamy więc problem dwóch wartości. Z jednej strony, mamy ochronę danych osobowych związaną z powszechnym prawem do prywatności, z drugiej zaś prawo do informacji publicznej i swobodę działalności gospodarczej zapewniającej bezpieczeństwo obrotu. Jak więc pogodzić problemy na styku tych zagadnień?

Celem niniejszego artykułu jest ocena praktyki ochrony danych osobowych w odniesieniu do przedsiębiorców na podstawie analizy przepisów prawa oraz koncepcji i zagadnienień teoretycznych przedstawionych w literaturze przedmiotu. W pierwszej części artykułu autorzy skupiają się na zagadnieniach teoretycznych, w tym sygnalizują problemy związane ze zdefiniowaniem pojęcia danych osobowych wraz ze wskazaniem podmiotowego zakresu ich ochrony. W drugiej części koncentrują się na praktycznych aspektach ochrony danych osobowych przedsiębiorców omawiając problematykę zagadnienia w procesach biznesowych oraz w Internecie. Trzecia, ostatnia część została poświęcona analizie zmian przepisów dotyczących ochrony danych osobowych wchodzących w życie w maju 2018 roku.

W opracowaniu wykorzystana została głównie metoda opisowa z elementami formalno-dogmatycznymi, polegająca na analizie aktualnych tekstów prawnych z wykorzystaniem literatury i orzecznictwa. Przy omawianiu pojęcia przetwarzania danych osobowych posłużono się metodą historyczną, polegającą na porównaniu regulacji obowiązujących obecnie z regulacjami obowiązującymi wcześniej. W artykule zastosowano także metodę porównawczą na tle regulacji w innych krajach europejskich.

## 2. Pojęcie danych osobowych

Ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych w art. 6 definiuje dane osobowe jako wszelkie

informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[1]. Przepis ten, zmieniony nowelą z dnia 25 sierpnia 2001 roku, odpowiada definicji zamieszczonej w prawie unijnym[2] i konkretyzuje, że danymi osobowymi są nie tylko informacje, które służą identyfikacji konkretnej osoby, lecz także wszelkie informacje dające się z nią powiązać (dane identyfikujące).

Definicja tego pojęcia jest ogólna, a zaliczenie informacji do kategorii danych osobowych nie jest oparte na jednym, uniwersalnym kryterium. Stworzenie wyczerpującego wykazu danych osobowych jest niemożliwe, bowiem ta sama informacja w rękach jednej osoby będzie stanowić dane osobowe, w innej już nie. Zdaniem A. Mednisa nie jest realne odgórne przypisanie charakteru osobowego żadnej kategorii danych, o czym stanowi użyty w definicji danych osobowych zwrot „wszelkie informacje". Oznacza to, że pojęcie danych osobowych obejmuje nie tylko znaki językowe, lecz także informacje przybierające inne formy, tj. filmy, zdjęcia, dane biometryczne. Nie ma przy tym znaczenia sposób wyrażenia i zapisania komunikatu, zakres i swoboda udostępniania czy metoda pozyskania (Barta i Litwiński, 2016, s. 77). Ustalenie przedmiotowego zakresu ustawowego danych osobowych budzi zatem wiele wątpliwości i jest dyskusyjne. Niezaprzeczalnie jednak, aby informacja posiadała charakter osobowy, musi spełniać łącznie trzy przesłanki – być komunikatem, dotyczyć osoby fizycznej (w Polsce ochrona danych osób prawnych regulowana jest postanowieniami kodeksu cywilnego oraz niektórymi ustawami szczegółowymi), posiadać ustalony bądź możliwy do ustalenia podmiot (nie są danymi osobowymi dane anonimowe), przy czym nieistotny jest sposób wyrażenia komunikatu ani jego prawdziwość[3]. Mniej kłopotów sprawia wskazanie danych osobowych dotyczących zidentyfikowanej już osoby. Bezsporne jest, iż danymi osobowymi będą w takim przypadku wszelkie informacje dotyczące tej, konkretnej osoby (m.in. data urodzenia, miejsce zamieszkania, nr dowodu osobistego, rozmiar buta czy ocena na dyplomie ukończenia szkoły wyższej)[4]. Problemy stwarza jednak określenie charakteru informacji umożliwiającej zidentyfikowanie osoby.

Zgodnie z art. 6 ust. 2 uodo, „osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne". Ustawa odwołuje się tutaj do pojęcia tożsamości, które nie jest jednak przez ustawę definiowane. Z tego względu konieczne jest odwołanie się do wykładni językowej tego pojęcia, zgodnie z którą tożsamość rozumie się jako „świadomość siebie, swoich cech i własnej odrębności"[5] albo jako tożsamośc osobistą, czyli „bycie tym samym człowiekiem (tą samą osobą), bycie sobą, bycie tym, za kogo się podajemy"[6]. Oznacza to zatem, że tożsamość to cechy, które stanowią o tym, kim dana osoba jest, czym różni się od innych, na co składa się nie tylko to, kim się jest obecnie, ale także to, kim się było, a nawet zamierza być w przyszłości. Z uwagi na to, że ochrona danych osobowych dotyczy także ochrony prywatności, to oczywiste jest także, iż ochrona ta dotyczy również informacji związanych z przeszłością określonego człowieka.[7]

Ustawodawca postanowił ograniczyć zakres pojęcia informacji umożliwiającej określenie tożsamości w art. 6 ust. 3 poprzez sformułowanie, że nie ma charakteru danych osobowych informacja, która do ustalenia tożsamości osoby wymaga od osoby trzeciej „nadmiernych kosztów, czasu i działań"[8]. W rozwoju technologii coraz ciężej jednak mówić o nadmiernych nakładach. Praktyka pokazała, że decydujące jest zachowanie pewnej proporcji między poniesionymi nakładami a uzyskanym rezultatem w postaci zidentyfikowanej osoby, gdyż charakter „nadmierności" jest niewątpliwie względny i zależny od sytuacji (Banyś i Łuczak, 2014, s. 20–21).

Istotne jest również rozróżnienie między danymi zwykłymi a szczególnie chronionymi. Ustawa wprost nie definiuje pojęcia „dane zwykłe" i „dane wrażliwe", jednak podział ten, jak wskażemy poniżej, wynika wprost z przepisów w niej zawartych i jest dla stosowania prawa bardzo istotny. Ustawodawca określił kryterium dopuszczalności przetwarzania danych osobowych w oparciu o przesłanki z art. 27 ust. 2, rozróżniając dane, które przetwarza się na zasadach ogólnych określonych w art. 23 ust. 1 (dane zwykłe) oraz takie, których przetwarzanie jest dopuszczalne, jeżeli

jest spełniona przynajmniej jedna z określonych w art. 27 ust. 2 przesłanek (dane wrażliwe; inaczej: sensytywne, szczególnie istotne). Na mocy art. 27 ust. 1 zakazano przetwarzania enumeratywnie wymienionych kategorii danych, wyłączając przypadki wskazane w ust. 2 tego artykułu. Do danych wrażliwych, wykazanych w ustawie należą dane dotyczące: pochodzenia rasowego i etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, stanu zdrowia, kodu genetycznego, nałogów, życia seksualnego, orzeczeń o ukaraniu i mandatów karnych oraz innych orzeczeń sądowych lub administracyjnych. Nie należy jednak zapominać, że dane sensytywne stanowią kategorię pojęcia danych osobowych zawartego w ustawie o ochronie danych osobowych, co oznacza, że nie można nazwać informacji wrażliwą bez wcześniejszego ustalenia jej podmiotu. Nie jest więc zabronione wykorzystywanie wyżej wymienionych informacji, gdy są anonimowe. Widać to na przykładzie licznych ankiet socjologicznych, które pomimo iż „zahaczają“ o dane szczególnie istotne, nie pozwalają na zidentyfikowanie osoby uczestniczącej w ankiecie na ich podstawie.

Jak zauważyła M. Sakowska-Baryła, koncepcja wyodrębnienia kategorii danych wymagających podwyższonego standardu ochrony jest trafna, jednak rozgraniczenie dokonane zostało z pewnym uproszczeniem, na podstawie przeciętnych odczuć i zjawisk, a nie na podstawie konkretnych przypadków, dlatego zasadność dwupodziału danych osobowych i jego przeprowadzenie może stanowić temat szerokiej dyskusji i może być kwestionowany. W niektórych sytuacjach istotniejszy od treści informacji może być bowiem kontekst jej wykorzystania (Sakowska-Baryła, 2015, s. 213).

Ustawodawca, definiując dane osobowe w art. 6 ustawy o ochronie danych osobowych nie określił zamkniętego katalogu informacji stanowiących te dane. Dlatego też przy rozstrzyganiu, czy określona informacja lub informacje stanowią dane osobowe, w większości przypadków nieuniknione jest dokonanie zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby. W świetle przepisów należy przyjąć, że nie będzie miała charakteru danych osobowych pojedyncza, bardzo ogólna informacja (do wyjątków należą numery identyfikacyjne, np. PESEL, NIP, REGON)[9]. Może ona jednak stanowić dane osobowe w połączeniu z dodatkowymi informacjami, co w konsekwencji może prowadzić do konkretnej osoby. Zastosowane przez europejskiego i krajowego prawodawcę pojęcia nieostre służą maksymalnej ochronie danych osobowych, ponieważ sformułowania zbyt konkretne czy wręcz kazuistyczne mogłyby efektywnie zawężać jej zakres.

## 3. Podmiotowy zakres ochrony danych osobowych

Zgodnie z art. 47 Konstytucji, „każdy ma prawo do ochrony prawnej życia prywatnego”. Natomiast, zgodnie z art. 51 ust. 2 Konstytucji, „władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym”. Tu należy zwrócić uwagę, że Konstytucja w tytule Rozdziału II rozróżnia pojęcia „człowiek” i „obywatel”. Z uwagi na to rozróżnienie w literaturze można znaleźć dwa podejścia dotyczące zakresu podmiotowego art. 51 ust. 2 Konstytucji. Jak twierdzi E. Kulesza, gwarancje zawarte w omawianym artykule w odniesieniu do ochrony danych osobowych powinny odnosić się do wszystkich osób przebywających na terytorium RP, nie tylko polskich obywateli, gdyż nie ma podstaw do różnicowania tej kwestii przy użyciu kryterium przynależności państwowej. Swoją regułę potwierdza, zwracając uwagę na sformułowania zawarte w art. 51 i innych Konstytucji. Przykładowo, autorka zwraca uwagę na użycie w ust. 2 sformułowania „informacje o obywatelach”, jednak na podstawie swoich rozważań postuluje o skorygowanie przepisu w sposób, aby całokształt norm odnoszących się do ochrony danych osobowych nie budził wątpliwości (Kulesza, 2015, s. 106). Zdaniem M. Wyrzykowskiego adresatów treści zawartych w art. 51 Konstytucji RP jest co najmniej kilku. Jako pierwszego wskazuje każdą jednostkę, niezależnie od obywatelstwa, którą ust. 1 omawianego artykułu obdarza prawem do nieujawniania informacji o sobie, za wyjątkiem sytuacji opisanych w odpowiednich ustawach. Drugi adresat, zgodnie ze stanowiskiem autora, wskazany został w ust. 2 i jest nim obywa-

tel polski, o którym władze publiczne mają prawo gromadzić i wykorzystywać dane jedynie niezbędne do zachowania demokratycznego porządku w państwie. W konsekwencji tego rozróżnienia pojawia się trudność w określeniu zakresu informacji, jakie mogą być przetwarzane przez władze publiczne i czy mają one prawo dysponować danymi osób z obywatelstwem innym niż polskie, biorąc pod uwagę obowiązki władz, które z definicji polegają właśnie na gromadzeniu danych o obywatelach innych państw (np. kontrwywiad). Idąc dalej, nie można zatem interpretować tego przepisu jako zakazu wykorzystywania danych o cudzoziemcach. Zestawiając to z zasadą legalności, nie można również odczytywać tej normy jako dopuszczenia takiej działalności (Wyrzykowski, 1999, s. 25).

Oba te stanowiska nie w pełni odnoszą się do problemu. Pierwsze zdaje się pomijać zasadę racjonalności prawodawcy, drugie prowadzi do zbyt daleko idących wniosków. Usytuowany jako ostatni ust. 5 art. 51 Konstytucji odwołujący do ustawy określającej zasady gromadzenia i wykorzystywania danych wskazuje, iż jego postanowienie powinno odnosić się do wszystkich wyżej wymienionych. Można zatem stwierdzić, że ustawodawca dostrzegł potrzebę zaakcentowania, iż treść art. 51 ust. 2 powinna odnosić się przede wszystkim do obywateli, co nie oznacza, że prawo to nie przysługuje również cudzoziemcom. Analiza przeprowadzona przez M. Sakowską-Baryłę doprowadziła autorkę do wniosku, iż normy zawarte w omawianym artykule winny odnosić się do wszystkich osób przebywających na terenie RP i nie są uzależnione od jakichkolwiek innych warunków (Sakowska-Baryła, 2015, s. 108).

W judykaturze przykładowo nie wzbudza wątpliwości, że prawo do ochrony danych osobowych dotyczy jedynie osób fizycznych[10] posiadających zdolność prawną, a więc od chwili urodzenia aż do śmierci[11]. Warto przy tym wskazać praktykę postępowania z danymi osób zmarłych lub poczętych, nienarodzonych. W momencie śmierci gaśnie co prawda prawo, jednak nie ustaje przetwarzanie danych, które często mogą dotyczyć jednocześnie osób żyjących (np. informacje o przebytych chorobach, szczególnie dziedzicznych). W takiej sytuacji uznać można, że informacje te podlegają regulacjom ustawy o ochronie danych osobowych. Wydaje się, że ustawa wymaga wprowadzenia zmian w tym zakresie, ponieważ nie określa, co dzieje się z danymi po śmierci osoby, a przecież taka sytuacja nie może być przyzwoleniem na przetwarzanie ich w sposób dowolny (Sakowska-Baryła, 2015, s. 116–119). Odnośnie do osób poczętych przyjęło się traktować informacje o dziecku nienarodzonym do momentu jego narodzin jako dane jego matki, ojca lub innych osób. Wszelkie informacje zebrane w trakcie życia płodowego w chwili narodzin powinny zostać uznane za dane osobowe dziecka. Po narodzinach do momentu osiągnięcia pełnoletności o przetwarzaniu tych danych decyduje przedstawiciel ustawowy samodzielnie lub wspólnie z osobą małoletnią, w zależności od jej wieku (Barta i Litwiński, 2016, s. 141–143).

## 4. Ochrona danych osobowych przedsiębiorcy

Status przedsiębiorcy jako osoby fizycznej może przysługiwać osobie fizycznej na podstawie przepisów Kodeksu cywilnego[12] (kc) oraz ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej[13] (usdg). Zgodnie z wcześniejszym ustaleniami spod działania ustawy o ochronie danych osobowych wyłączone zostały osoby prawne, stąd analiza przepisów w tym zakresie ograniczy się jedynie do osób fizycznych. W myśl art. $43^1$ kc przedsiębiorcą jest więc osoba fizyczna prowadząca działalność gospodarczą lub zawodową we własnym imieniu. Artykuł 4 usdg stanowi, że w rozumieniu ustawy przedsiębiorca to osoba fizyczna, osoba prawna oraz jednostka organizacyjna niebędąca osobą prawną, wykonująca we własnym imieniu działalność gospodarczą. Za działalność gospodarczą natomiast usdg w art. 2 uznaje zarobkową działalność wytwórczą, budowlaną, handlową, usługową oraz poszukiwanie, rozpoznawanie i wydobywanie kopalin ze złóż wykonywaną w sposób zorganizowany i ciągły. Ponadto, art. $43^2$ § 2 w związku z $43^4$ kc stanowi, iż przedsiębiorca ma działać pod firmą zawierającą przynajmniej jego imię i nazwisko, która, o ile odrębna ustawa nie stanowi inaczej, powinna być ujawniona w odpowiednim rejestrze. W odniesieniu do przedsiębiorców będących osobami fizycznymi zastosowanie znajdują przepisy usdg, na podstawie której wprowadzono Centralną Ewidencję i Informację o Działalności

Gospodarczej (dalej: CEIDG), której zadaniem jest między innymi ewidencjonowanie przedsiębiorców i udostępnianie informacji o nich w określonym ustawą zakresie.

W myśl art. 38 ust. 1 usdg wszelkie informacje zawarte w CEIDG są jawne. Wpisanie ich przez osobę fizyczną chcącą podjąć działalność gospodarczą do ewidencji jest zatem świadome i stawia podane informacje w charakterze powszechnie dostępnych. Wobec tego można wysnuć wniosek, iż wszelkie dane identyfikujące przedsiębiorcę w zakresie wykonywanej przez niego działalności nie podlegają przepisom ustawy o ochronie danych osobowych (Dziurla, 2014). Potwierdziło to orzeczenie Naczelnego Sądu Administracyjnego, który stwierdził, że ani nazwa, ani numer telefonu kancelarii nie stanowią danych osobowych w rozumieniu ustawy, bowiem nie służą do identyfikacji osoby fizycznej, a jednostki organizacyjnej, podobnie jak do kategorii tej nie należy zaliczać nazwy spółki cywilnej. Sąd potwierdził również, że objęcie przez przedsiębiorcę swoich danych osobowych w zakresie danych indywidualnych dotyczących jego działalności gospodarczej nie upoważnia go jako osoby fizycznej do domagania się ochrony tych danych, gdyż wykorzystywane są one nie jako dane osobowe, a dane przedsiębiorcy. Toteż „decydując się na utożsamianie tych danych godzi się tym samym na szersze ich ujawnianie i słabszą ochronę”[14]. Wszystkie ujawnione w CEIDG informacje pokrywające się z danymi dotyczącymi samego przedsiębiorcy nie powinny zatem podlegać ochronie ustawy.

Inne stanowisko prezentuje A. Mednis, którego zdaniem informacje identyfikują konkretną osobę, dopóki należą do danych osobowych i są objęte ochroną uodo (Mednis, 1999, s. 25). Jak podkreśla W. Szlawski, firma osoby fizycznej zawiera informacje dotyczące zidentyfikowanej bądź możliwej do zidentyfikowania osoby, toteż bez wątpienia można uznać ich charakter jako danych osobowych i objąć zakresem regulacji uodo. Jak wskazuje autor, do końca 2011 roku obowiązywał jasny przepis wyłączający stosowanie przepisów uodo w zakresie informacji zawartych w Ewidencji Działalności Gospodarczej (poprzednik CEIDG)[15]. W związku z jego uchyleniem ustawodawca doprowadził do sytuacji, w której dane zawarte w rejestrze nie są wyłączone z zastosowania ustawy, czyli mają podlegać zasadom ogólnym uodo (Szlawski, 2014).

Ostatecznie, w związku z rezygnacją ze wspomnianego wyżej przepisu, wszelkie dane osób fizycznych, również tych związanych z prowadzeniem działalności gospodarczej, podlegają regulacjom uodo. Wydaje się to jednak kłopotliwe, w praktyce utrudniając między innymi swobodny przepływ informacji o przedsiębiorcy. Należy bowiem podkreślić, że w przypadku informacji dotyczących przedsiębiorców dysponowanie ich danymi związanymi z wykonywaną działalnością ułatwia prowadzenie interesów z nimi i może pozytywnie wpływać na ich wiarygodność w obrocie gospodarczym. Zasadny wydaje się więc powrót do rozwiązania, w którym wyłączone z zastosowania uodo są informacje zawarte w CEIDG. W obecnym stanie prawnym uodo podlegają zarówno informacje o charakterze wewnętrznym związane z funkcjonowaniem przedsiębiorcy, jak i informacje powszechnie dostępne, co w przypadku danych osobowych przedsiębiorców może być problematyczne, a czasem wręcz paradoksalne. Trudno bowiem bronić słuszności w odniesieniu do omawianego przypadku, np. obowiązku informacyjnego czy zgłoszenia zbiorów do rejestru. Ustawodawca dostrzegł ten problem, czego przejawem jest uchwalona 25 września 2015 roku ustawa o zmianie ustawy o swobodzie działalności gospodarczej oraz niektórych innych ustaw[16]. Zmiany te weszły w życie 19 maja 2016 roku i są istotne w odniesieniu do ochrony danych osobowych przedsiębiorcy. Nowelizacja wprowadziła bowiem do usdg zbliżony do wspomnianego wcześniej przepisu uchylonego z końcem 2011 roku art. 39b o następującym brzmieniu: „Do jawnych danych i informacji udostępnianych przez CEIDG nie stosuje się przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, z wyjątkiem przepisów art. 14–19a i art. 21–22a oraz rozdziału 5 tej ustawy”. Wcześniejsze całkowite wyłączenie stosowania uodo w odniesieniu do informacji zawartych w rejestrze zostało ograniczone dwiema podstawowymi zasadami przetwarzania – zwolnienie dotyczy wyłącznie danych dostępnych jawnie w CEIDG, ponadto podmiot przetwarzający dane pobrane z rejestru wciąż podlega w pewnym zakresie kontroli GIODO. Niestety i to rozwiązanie budzi wątpliwości, ponieważ grozi sytuacją, w której

informacje o konkretnym przedsiębiorcy będą podlegały dwóm rodzajom regulacji jednocześnie. Ponadto istnieje ryzyko, że administratorzy przeoczą ograniczenia, traktując nowe przepisy jako przyzwolenie do dowolonego przetwarzania wszystkich danych o przedsiębiorcach. Jak twierdzi M. Kwiatkowska-Cylke, może to doprowadzić do wielu naruszeń zasad ochrony danych osobowych (Kwiatkowska-Cylke, 2016).

## 5. Dane osobowe w relacji z pracownikami oraz osobami starającymi się o pracę

Zgodnie z §6 Rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika pracodawca ma do czynienia z danymi osobowymi w toku rekrutacji, okresie zatrudnienia, a także po jego ustaniu[17]. W procesie rekrutacji mogą być zbierane w zasadzie dowolne dane, na co osoba aplikująca wyraża zgodę, umieszczając odpowiednią klauzulę w aplikacji, co zazwyczaj robi chętnie, gdyż w jej interesie jest zainteresować swoją osobą potencjalnego pracodawcę. Aplikacja bez takiej zgody w polskim systemie prawa powinna być natychmiast o nią uzupełniona bądź usunięta przez przedsiębiorcę. Zgody nie wymagają jedynie określone w kodeksie pracy[18] dane, tj. imię i nazwisko, data urodzenia, miejsce zamieszkania (adres do korespondencji), wykształcenie oraz przebieg dotychczasowego zatrudnienia[19]. Jeśli polski ustawodawca postanowi skorzystać z zaleceń niezależnego zespołu roboczego ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (powszechnie zwanego Grupą Roboczą Art. 29 ds. Ochrony Danych Osobowych, powołanego na mocy europejskiej dyrektywy 95/46/WE) samo wysłanie życiorysu do pracodawcy stanowić będzie zgodę na przetwarzanie przez niego podanych informacji w celu rekrutacji[20].

Kontrowersje wzbudzają testy rekrutacyjne w celu określenia przydatności zawodowej pracownika. Jak stwierdził GIODO w jednym ze sprawozdań ze swojej działalności, pracodawcy nadużywają tej metody do pozyskiwania dodatkowych informacji dotyczących cech kandydata, co nie jest zgodne z prawem. Jednakże WSA w swoim orzeczeniu zwrócił uwagę na pominięcie przez GIODO istotnej kwestii, jaką jest zgoda kandydata na uczestniczenie w teście. Można więc wysnuć wniosek, że dopóki udział w teście jest dobrowolny i nie wpływa na inne niż pozostałych traktowanie kandydata jest on zgodny z prawem[21].

W okresie zatrudnienia pracodawca ma obowiązek wydawania upoważnień do przetwarzania jakichkolwiek danych przez pracownika w związku z wykonywaniem pracy, ale także chronić i nie nadużywać wykorzystywania danych dotyczących osoby przez niego zatrudnionej. Biorąc pod uwagę nieuniknioną potrzebę wymiany informacji (nie zawsze o charakterze zawodowym) między pracownikiem a pracodawcą, oraz względnie wąski zakres regulacji przepisów prawa pracy, zalecaną praktyką jest wdrożenie jasnej i przejrzystej polityki prywatności w przedsiębiorstwie. Powinna ona być dostępna dla pracowników w każdej chwili, określając:

- rodzaje danych osobowych pracowników, jakie są gromadzone i przetwarzane przez pracodawcę oraz cele tego przetwarzania,
- listę osób upoważnionych do wglądu w te informacje,
- rozróżnienie między obligatoryjnie a dobrowolnie przekazywanymi danymi oraz konsekwencje w przypadku odmowy ich podania,
- okres przechowywania danych oraz metody ich usuwania po upływie tego okresu,
- prawa pracowników w sferze bezpieczeństwa dotyczących ich danych osobowych,
- możliwe operacje przekazywania danych do krajów trzecich,
- dane kontaktowe urzędnika ds. ochrony danych (jeżeli istnieje) (Lifelong Learning Programme Leonardo Da Vinci, 2012, s. 16).
- Po zakończeniu stosunku pracy pracodawca często dalej przechowuje dokumentację byłego pracownika, jednak podstawy prawne przetwarzania tych danych osobowych ulegają znacznemu ograniczeniu. Przetwarzanie danych zawartych w aktach byłego pracownika dozwolone jest wyłącznie na podstawie przepisów prawa, takich jak np. przepisy emerytalne, dotyczące ochrony zdrowia,

podatków czy archiwizacji (Lifelong Learning Programme Leonardo Da Vinci, 2012, s. 28).

Ponadto w celu udokumentowania roszczeń pracodawcy dane mogą być przechowywane w okresie równym okresowi przedawnienia tych roszczeń. Istotny z punktu widzenia pracodawcy jest okres przechowywania dokumentacji dla celów ubezpieczeń społecznych, gdyż może on wynosić nawet do 50 lat (Lifelong Learning Programme Leonardo Da Vinci, 2009, s. 42–43).

## 6. Przetwarzanie danych osobowych pozyskanych w związku z działalnością prowadzoną w Internecie

Dane osobowe są istotnym elementem funkcjonowania większości przedsiębiorców. Ich ochrona jest częścią wymaganych prawem zabezpieczeń, ale również budowy wizerunku przedsiębiorcy w sieci i poza nią. Ciężko wyobrazić sobie serwis lub sklep internetowy niemający styczności z danymi osobowymi podczas prowadzenia własnej działalności. Wykorzystywane są one bowiem przy operacjach takich jak wysyłka towaru, rozpatrywanie reklamacji, świadczenie usług drogą elektroniczną.

W myśl definicji ustawowej „dane osobowe" to wszelkie informacje identyfikujące bądź pozwalające zidentyfikować osobę fizyczną. W kontekście danych przetwarzanych w systemach teleinformatycznych bardzo istotna jest pośrednia możliwość identyfikacji osoby, szczególnie w odniesieniu do danych służących rozpoznawaniu użytkowników i uwierzytelnianiu dostępu do treści (np. adres e-mail, login, nick czy numery identyfikujące urządzenia końcowe, tj. numer telefonu czy IP komputera). Przedstawiona przez ustawodawcę definicja nie określa, jakie dane należy traktować jako osobowe, a jedynie wskazuje kryteria ich klasyfikacji, którymi należy się kierować, stąd wniosek, że każdy przypadek należy rozpatrywać indywidualnie. W praktyce pomocne w tym zakresie mogą być publikacje Generalnego Inspektora Danych Osobowych, które choć nie mają charakteru wiążącego, zawierają istotne wskazówki praktyczne porządkujące klasyfikację danych osobowych w sieci (Generalny Inspektor Ochrony Sanych Osobowych, 2009, s. 11). Przykładowo, w większości przypadków podmioty korzystające z usług dostępu do sieci telekomunikacyjnych i teleinformatycznych są związane umowami z usługodawcami, określającymi ich dokładną tożsamość. Oznacza to, że dostawcy dysponują szczegółowymi informacjami na temat swoich abonentów w ramach świadczonej usługi, w tym danymi lokalizacyjnymi oraz danymi o ruchu telekomunikacyjnym. Dane lokalizacyjne to dane o położeniu geograficznym użytkownika w określonym czasie podawane jako długość i szerokość geograficzna oraz wysokość nad poziomem morza. Z ich pomocą można łatwo określić szybkość oraz kierunek przemieszczania się danej osoby. Dane o ruchu telekomunikacyjnym to dane dotyczące połączenia sieciowego, m.in. trasowanie (*routing*), czas rozpoczęcia i zakończenia, ilość przekazanych informacji, wykorzystany protokół, sieć źródłowa i końcowa (Generalny Inspektor Ochrony Sanych Osobowych, 2009, s. 13). Danymi osobowymi mogą być też informacje, tj. pliki *cookies*[22], numer MAC karty sieciowej, numer IMEI telefonu komórkowego, rejestr odwiedzanych stron. Mogą być one bowiem wykorzystywane do identyfikacji osób lub analizy ich potrzeb, zainteresowań czy preferencji. Istotne znaczenie przy odpowiedniej klasyfikacji tych danych ma kryterium nadmierności nakładów, co bada się indywidualnie w każdym przypadku (Piątek, 2015).

Często używaną informacją w sieciach informatycznych jest login. Pod pojęciem tym rozumie się ciąg znaków pozwalających określić użytkownika i powiązać go z przydzielonymi mu uprawnieniami. Jest on więc niezbędny do rozpoczęcia przez użytkownika pracy w zamkniętym systemie, pozwala go rozpoznać i zidentyfikować jego uprawnienia oraz dokonane dotychczas operacje. Login w danym systemie powinien więc być unikatowy dla każdego użytkownika, co nie wyklucza istnienia tego samego identyfikatora należącego do innej osoby w innym systemie. Z punktu widzenia administratora systemu informatycznego identyfikator w postaci loginu w momencie rejestracji użytkownika powiązany zostaje najczęściej z danymi takimi jak imię, nazwisko, adres e-mail, numer telefonu, przyznane uprawnienia itp. Dane te odnoszą się do konkretnej osoby, mają zatem charakter danych osobowych. Nie zawsze jednak powiązania te są weryfikowane pod kątem ich prawdzi-

wości. Najczęściej jednak regulamin serwisu nakłada na użytkownika obowiązek podania informacji zgodnych ze stanem faktycznym, zrzucając tym samym z siebie odpowiedzialność za dane fałszywe. Zdarzają się też systemy ograniczające zakres danych podawanych przez użytkownika. Sytuacja taka ma miejsce między innymi na wszelkiego rodzaju forach dyskusyjnych, gdzie każdy użytkownik dysponuje takim samym zakresem uprawnień i posługuje się nazwą niedającą się z nim powiązać. W takim przypadku login zwany jest *nickiem* i w odróżnieniu od stałego loginu może być również tymczasowy. Samoistnie nie ma on charakteru danych osobowych, jednak może stanowić informację ułatwiającą identyfikację użytkownika (Generalny Inspektor Danych Osobowych, 2009, s. 20–22).

Duże znaczenie praktyczne ma odpowiednie zakwalifikowanie adresu IP (*Internet Protocol Address*). Adres ten, będący numerem identyfikującym urządzenie komputerowe (komputery, drukarki, kamery, itp.), umożliwia połączenie urządzenia z siecią telekomunikacyjną, przy czym często urządzenia przypisane są do konkretnej osoby. W Internecie adres IP urządzenia nadawany jest przez dostawcę połączenia z siecią w ramach przysługującej puli adresowej przydzielanej przez organizację RIPE Network Coordination Center, zajmującej się zarządzaniem zasobami internetowymi, między innymi w Europie. W systemach informatycznych przetwarzane są dwa rodzaje danych – dane o abonentach łączące publiczny numer IP z danymi osobowymi użytkownika oraz dane o wykonywanych połączeniach teleinformatycznych. Pierwsze są danymi osobowymi bezpośrednio identyfikującymi klientów, drugie mają charakter danych osobowych w momencie, gdy dotyczą ruchu generowanego przez urządzenie należące do osoby fizycznej dającej się zidentyfikować pośrednio (Generalny Inspektor Danych Osobowych, 2009, s. 20). Adres IP został ostatecznie uznany za informację umożliwiającą zidentyfikowanie osoby, co poparła w swojej opinii niezależna Grupa Robocza Art. 29 ds. ochrony danych osobowych[23]. Numeru IP nie uznaje się jednak za dane osobowe, gdy urządzenie, do którego jest przypisany ten numer, pozostaje w dyspozycji podmiotu niebędącego osobą fizyczną, przez co niemożliwe jest jednoznaczne wskazanie osoby sprawującej nad nim wyłączną kontrolę. Danymi osobowymi nie są więc np. adres IP serwerów wyszukiwarki internetowej czy poczty elektronicznej (jest to sytuacja podobna do urządzenia telefonicznego zainstalowanego w miejscu publicznym, np. budce telefonicznej)[24].

Można zatem przyjąć, ze względu na kryterium nadmiernych kosztów, czasu lub działań, że stałe adresy IP komputera należące do osób fizycznych lub dostawców Internetu stanowią co do zasady dane osobowe (Barta i Litwiński, 2016, s. 92).

## 7. Zmiany przewidziane w Rozporządzeniu Ogólnym o Ochronie Danych Osobowych (RODO)

W maju 2016 roku Parlament Europejski razem z Radą Unii Europejskiej przyjęły nowelizację przepisów o ochronie danych osobowych. Z dniem 25 maja 2018 roku zaczną one obowiązywać we wszystkich państwach członkowskich i bezpośrednio wpłyną na funkcjonowanie przedsiębiorców przetwarzających dane osobowe, niezależnie od ich rozmiaru.

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 (dalej: RODO)[25] ma na celu dostosowanie regulacji do dynamicznie rozwijającego się świata technologii, w którym Internet stał się standardem, usługi chmurowe codziennością, a informacje wymieniane są w skali globalnej w sposób ciągły i nieprzerwalny. Rozporządzenie jest odpowiedzią na aktualne problemy ochrony danych osobowych, a nieprzestrzeganie go wiąże się z wysokimi karami pieniężnymi – nawet do 20 mln euro lub 4% całkowitego, światowego obrotu z poprzedniego roku[26]. RODO ma stanowić kompleksową regulację dotyczącą ochrony danych osobowych, zmieniając dotychczas praktykowane podejście do tej problematyki. RODO ma regulować w szczególności: zasady ochrony danych osobowych; prawa osoby, której dane dotyczą; obowiązki i prawa adminsitratora oraz podmiotu przetwarzającego; przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych; funkcjonowanie niezależnych organów nadzorczych;

współpracę i spójność działań unijnych i krajowych organów nadzorczych; środki ochrony prawnej, odpowiedzialność i sankcje za naruszenie przepisów rodo.

Zasady przyjęte w RODO, co dotychczas nie miało miejsca, różnicują małe oraz większe jednostki, przewidując dla tych pierwszych uproszczone reguły dotyczące przetwarzania danych osobowych (Osiński, 2017). Co istotne, przepisy RODO dotyczyć mają także jednostek, których siedziba znajduje się poza UE, jeśli oferują one dobra lub usługi obywatelom UE lub monitorują ich zachowania, a nie jak dotychczas jedynie jednostek unijnych (Deloitte, 2017, s. 7–9). Oznacza to, że do nowego porządku prawnego będą się musiały dostosować także korporacje amerykańskie, takie jak np. Facebook czy Google.

Nowe przepisy wzmacniają pozycję osób fizycznych, wskazując podmiot przetwarzający dane jako domyślnie odpowiedzialny za ich ochronę. Oznacza to, że osoba, której dane dotyczą, nie musi podejmować żadnych działań mających na celu ich ochronę, bowiem przetwarzający dane ma obowiązek zadbać o ich bezpieczeństwo już na etapie tworzenia produktów czy usług oraz systemów i procesów przetwarzania danych (*privacy by default*) (Rachelski i Współnicy, 2017). Dodatkowo, aby uzyskać większą kontrolę, osoba, której dane przetwarzane są w zautomatyzowanym systemie, na podstawie umowy lub zgody, zostanie wyposażona w prawo do przeniesienia tych danych. Osoba wykonująca to prawo będzie mogła żądać od administratora danych dostarczenia danych jej dotyczących w ustrukturyzowanym, powszechnie używanym formacie możliwym do odczytu maszynowego i przenieść je do innego administratora[27]. RODO poszerza również, istotne z punktu widzenia przedsiębiorców bazujących na analityce danych, uprawnienia osób fizycznych o prawo do sprzeciwu i zakazu stosowania wobec nich marketingu bezpośredniego (PWC, 2017).

Przedsiębiorca w nowym porządku prawnym ma być zwolniony z obowiązku zgłaszania rejestru danych, zobowiązany jednak będzie do wdrożenia rejestru czynności związanych z przetwarzaniem danych osobowych oraz zgłaszania wszelkich naruszeń Generalnemu Inspektorowi Ochrony Danych Osobowych w ciągu 72 godzin od momentu ich stwierdzenia (w niektórych przypadkach może wystąpić również konieczność powiadomienia osoby o wystąpieniu ryzyka naruszenia jej praw). RODO rozbudowuje ponadto obowiązki informacyjne przetwarzającego dane poprzez wskazanie licznych informacji niezbędnych przy poprawnie formułowanej komunikacji sposobu przetwarzania danych oraz uzyskiwaniu ważnych i weryfikowalnych zgód na przetwarzanie danych od osób, których dotyczą.

RODO odnosi się również do kwestii profilowania należącego do tej pory w znacznej części do „szarej strefy". RODO bezpośrednio definiuje, czym jest profilowanie konsumenta oraz w pewnym zakresie ustanawia odrębne zasady, które należy do niego stosować (Krawecki, 2017, s. 132). Co więcej, wprowadzona została definicja „identyfikatorów internetowych", do których należą m.in. adresy IP i identyfikatory plików *cookie,* które w połączeniu z innymi informacjami pozyskiwanymi w sposób zautomatyzowany mogą być wykorzystywane do tworzenia profili i identyfikowania konkretnych osób[28].

RODO porusza kwestię przetwarzania danych biometrycznych, która nabiera na znaczeniu w niektórych branżach. Do tej pory przepisy ustawy nie odnosiły się wprost do danych biometrycznych, a więc obowiązki związane z ich przetwarzaniem należało oceniać na zasadach ogólnych, czyli traktować je jako dane zwykłe. RODO wprost określa zasady przetwarzania danych biometrycznych, zaliczając je do tzw. szczególnych kategorii danych osobowych, co w praktyce oznacza traktowanie ich na równi z danymi wrażliwymi[29].

Obecnie obowiązująca dyrektywa regulująca kwestię ochrony danych osobowych na terenie UE wymagała implementacji do prawa krajowego nie później niż w 3 lata od daty przyjęcia dyrektywy[30]. Rozporządzenie RODO ma charakter bezpośredni, czyli wchodzi w życie na terenie całej Unii bez potrzeby implementacji do krajowych porządków prawnych z chwilą ogłoszenia i upływem *vacation legis*. Ma to ułatwić prowadzenie transgranicznej działalności gospodarczej, ograniczając rozbieżności pomiędzy prawem krajowym a unijnym.

## Podsumowanie

Osoba decydująca się na podjęcie działalności gospodarczej w obecnym porządku prawnym musi pogodzić się z pewnym

poziomem rozpoznawalności. Dane przedsiębiorców, a czasem również ich pracowników, są bowiem jawne i łatwo dostępne, zwłaszcza gdy działalność prowadzona jest przy użyciu Internetu. Co więcej, prowadzenie działalności wiąże się z ciągłym przetwarzaniem danych osób trzecich, tj. w szczególności: pracowników, klientów, dostawców, kontrahentów. Przedsiębiorcy często nie zdają sobie sprawy, że mają do czynienia z gromadzeniem danych osobowych podlegających przepisom prawa (np. budując relacje poprzez newslettery czy mailingi). Z jednej strony, niewywiązanie się z obowiązków narzuconych przez ustawodawcę jest czynem zabronionym, za który przewidziane są odpowiednio kary. Z drugiej strony, brak bezpieczeństwa danych osobowych wiąże się z wieloma zagrożeniami, których skutki mogą przyjąć skalę globalną i być długotrwałe.

Naruszenia w sferze ochrony danych osobowych są w dzisiejszych czasach na porządku dziennym. Klienci powierzają swoje dane usługodawcom, uznając ich za cyfrowe „twierdze" wyposażone w zaawansowane systemy bezpieczeństwa. Tymczasem informacje o masowych wyciekach danych (w tym wielu wrażliwych, takich jak stan zdrowia, dane finansowe, dane logowania) obiegają świat częściej, niż by się wydawało. Na przestrzeli paru lat ofiarą przestępców komputerowych padły korporacyjne giganty, tj. Instagram[31], LinkedIn[32], Myspace[33], Wonga[34], Deloitte[35], a nawet Facebook[36]. Do grupy tej dołączyły ostatnio również cztery polskie banki (ING Bank Śląski, mBank, Idea Bank, Credit Agricole), w związku z ofertą dotyczącą sprzedaży danych klientów, takich jak numery rachunków, salda, numerów PESEL, adresów i telefonów komórkowych, opublikowaną w sieci[37].

Wejście w życie omawianego Rozporządzenia unijnego o Ochronie Danych Osobowych w maju 2018 roku istotnie zmieni sytuację przedsiębiorców oraz ich klientów i ma na celu ograniczenie występowania tego typu sytuacji. Przede wszystkim, jak już wskazano powyżej, każdy incydent będzie musiał zostać zgłoszony w ciągu 72 godzin odpowiednim organom[38] – dotychczas zdarzało się, że o wielkich wyciekach danych dowiadywaliśmy się nawet po kilku latach od ich wykrycia. Ponadto, zwiększone zostaną kary za dopuszczenie się naruszeń (mają się one wahać od 10 do 20 mln euro lub między 2–4% rocznego obrotu)[39].

Wydaje się, że na razie nie wszyscy przedsiębiorcy zdają sobie sprawę ze skali zmian oraz konsekwencji braku dostosowania do wymogów nowego porządku prawnego. Według raportu Fundacji „Wiedza To Bezpieczeństwo", 26% przedsiębiorców nie podjęło jeszcze działań, a 23% nie ma żadnej świadomości dotyczącej nadchodzących zmian. Z drugiej strony, w ponad połowie przebadanych organizacji wprowadzono już zmiany w procedurach, jednak 46% osób odpowiedzialnych za funkcję inspektora ochrony danych (IOD) ma jedynie ogólną wiedzę dotyczącą nadchodzących zmian. Badania wykazały potrzebę szkoleń i pogłębienia wiedzy z zakresu ochrony danych osobowych (tylko co 10. osoba stwierdziła, że nie jest to potrzebne). Aktualnie, sprawdzanie zgodności nowego procesu w organizacji ma miejsce po jego wdrożeniu. Po wejściu w życie RODO uwzględnienie ochrony danych osobowych wymagane będzie już w fazie projektowania produktu lub usługi. Istnieje zagrożenie, że organizacje będą interpretowały nowe przepisy zbyt literalnie, nie dostrzegając zmiany całej koncepcji i nie zdążą dostosować się do nowych ram (Fundacja Wiedza…, 2017).

Podsumowując, najistotniejsza z punktu widzenia przedsiębiorstw przetwarzających dane osobowe jest edukacja i świadomość aktualnego porządku prawnego. W obliczu nadchodzących zmian pierwsze kontrole organu nadzorczego w praktyce pokażą, jak duże zmiany są potrzebne w każdej organizacji. Jeśli przedsiębiorca nie dostrzega istoty bezpieczeństwa danych osobowych, zwiększone kary powinny zmotywować go do dokładniejszego przyjrzenia się sprawie i potraktowania ochrony danych osobowych poważnie. Z drugiej strony, skuteczny system wymaga również sprawnie działających organów nadzorczych.

## Przypisy

1 T.j. Dz. U. z 2016 r. poz. 922, z 2018 r. poz. 138.
2 Art. 2 pkt a Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady WE.
3 Opinion 4/2007 of Article 29 Data Protection Working Party on the concept of personal data, June 2007, 01248/07/EN, WP 136, s. 6.
4 Decyzja GIODO z 26 listopada 2009 roku, DOLiS/DEC-1183/09 dot. DOLiS-440-459/09, s. 2–3.

[5] Wyrok WSA w Warszawie z dnia 3 marca 2009 roku, II SA/Wa 1495/08 na podstawie Dubicz, S. (red.) (2003). *Uniwersalny Słownik Języka Polskiego*. Warszawa, s. 96.
[6] Wyrok WSA w Warszawie z dnia 3 marca 2009 roku, II SA/Wa 1495/08.
[7] Ibidem.
[8] Art. 6 ust. 3 uodo.
[9] http://www.giodo.gov.pl/317/id_art/973/j/pl/, dostęp: 12.03.2016.
[10] Wyrok NSA z dnia 28 listopada 2002 roku, II SA 2289/01.
[11] Zob. Dział I, Rozdział I Kodeksu Cywilnego, Dz.U. 2017 poz. 459 oraz http://giodo.gov.pl/319/id_art/974/j/pl/, dostęp: 10.03.2016.
[12] Dz.U. 2017 poz. 459, dalej: kc.
[13] Dz.U. 2004 nr 173 poz. 1807, dalej: usdg.
[14] Wyrok NSA z dnia 28 listopada 2002 roku, II SA 3389/01.
[15] Art. 7a ust. 2 ustawy z dnia 19 listopada 1999 r. Prawo działalności gospodarczej, Dz.U. z 2004 r. Nr 173, poz. 1808.
[16] Dz.U. 2015, 1893.
[17] Zob. Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika, Dz.U. 1996 nr 62 poz. 286.
[18] Dz.U. 2018 poz. 108, dalej: kp.
[19] Por. art. $22^1$ kp.
[20] Opinion 15/2011 of Article 29 Data Protection Working Party on the definition of consent, July 2011, 01197/11/EN, WP 187, s. 11 w: Kępa (2011, s. 60).
[21] http://uodo.pl/2014/kandydacie-do-pracy-jakich-danych-moze-od-ciebie-zadac-przyszly-pracodawca/, dostęp: 14.03.2016, zob. też dostępne na stronie http://www.giodo.gov.pl/138/id_art/2685/j/pl/ Sprawozdanie z działalności GIODO w roku 2009, s. 16.
[22] Więcej na temat *cookies:* Piątek (2015).
[23] Opinion 4/2007 of Article 29 Data Protection Working Party on the concept of personal data, June 2007, 01248/07/EN, WP 136, s. 16.
[24] http://www.giodo.gov.pl/319/id_art/2258/j/pl/, dostęp: 8.05.2016 oraz Wiecióra (2016, s. 56).
[25] 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.
[26] Art. 83 pkt. 5 RODO.
[27] Motyw 68 preambuły RODO.
[28] Motyw 30 preambuły RODO.
[29] Zob. art. 9 RODO.
[30] Art. 32 Dyrektywy 95/46/WE.
[31] http://money.cnn.com/2017/09/01/technology/business/instagram-hack/index.html?iid=EL, dostęp: 3.12.2017.
[32] https://www.cultofmac.com/171752/massive-linkedin-security-breach-leads-to-6-5-million-stolen-passwords/, dostęp: 3.12.2017.
[33] http://money.cnn.com/2017/09/07/technology/business/biggest-breaches-ever/index.html, dostęp: 3.12.2017.
[34] http://www.zdnet.com/article/payday-lender-wonga-confirms-data-breach/, dostęp: 3.12.2017.
[35] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails, dostęp: 3.12.2017.
[36] https://www.theguardian.com/technology/2017/jun/16/facebook-moderators-identity-exposed-terrorist-groups, dostęp: 3.12.2017.
[37] http://tvn24bis.pl/z-kraju,74/wyciek-danych-z-czterech-bankow,775771.html, dostęp: 3.12.2017.
[38] Art. 33 RODO.
[39] https://tech.wp.pl/wielki-wyciek-danych-w-uberze-firma-zaplacila-okup-po-wejsciu-rodo-taki-numer-juz-nie-przejdzie-6190474457331841a, dostęp: 3.12.2017.

## Bibliografia


Banyś, T. i Łuczak, J. (2014). *Ochrona danych osobowych w praktyce. Jak unikać błędów i ich konsekwencji prawnych*. Wrocław: Prescom Sp. z o.o.

Barta, P. i Litwiński, P. (2016). *Ustawa o ochronie danych osobowych. Komentarz*, wydanie 4. Warszawa: C.H. Beck.

Brieskorn, N. (1999). Ochrona danych osobowych a zagrożenia prywatności. W: M. Wyrzykowski, *Ochrona danych osobowych*. Warszawa: Instytut Spraw Publicznych.

Deloitte (2017). *Praktyczny przewodnik po Ogólnym Rozporządzeniu o Ochronie Danych Osobowych (RODO), Jak dostosować funkcjonujący w firmie model bezpieczeństwa i ochrony danych osobowych do wymogów nowych przepisów?*. Deloitte Polska.

Dziurla, P. (2014). *Dane osobowe przedsiębiorcy prowadzącego jednoosobową działalność gospodarczą, które podlegają ochronie ustawy o ochronie danych osobowych. Kompendium Prawne pracowników Kancelarii Prawnej Renata Urowska i Wspólnicy sp.k.* Poznań.

Fundacja Wiedza To Bezpieczeństwo (2017). *Co wiemy o ochronie danych*. Warszawa.

Generalny Inspektor Ochrony Danych Osobowych (2009). *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych*. Warszawa.

Kępa, L. (2011). *Dane osobowe w firmie. Praktyczny poradnik* przedsiębiorcy. Warszawa: Difin.

Krawecki, M. i Osieja, T. (red.) (2007). *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia.* Warszawa: C.H. Beck.

Kulesza, E. (2000). *Konstytucyjne prawo do ochrony danych osobowych i jego ustawowa realizacja*. *HZN*, *7*.

Kwiatkowsa-Cylke, M. (2016). *Czy przetwarzanie danych przedsiębiorców będzie łatwiejsze?* PortalODO.

Lifelong Learning Programme Leonardo da Vinci (2009). *Wybrane zagadnienia z zakresu ochrony danych osobowych. Przewodnik dla przedsiębiorców.* Projekt Partnerski 2009-1-PL1-LEO04-05167

Lifelong Learning Programme Leonardo Da Vinci (2012) *Ochrona prywatności w miejscu pracy. Przewodnik dla pracowników.* Projekt partnerski – 2012-1-PL1-LEO04-28097.

Mednis, A. (1999). *Ustawa o ochronie danych osobowych. Komentarz.* Warszawa: Wydawnictwo Naukowe PWN.

Opinion 15/2011 of Article 29 Data Protection Working Party on the definition of consent, July 2011, 01197/11/EN, WP 187.

Opinion 4/2007 of Article 29 Data Protection Working Party on the concept of personal data, June 2007, 01248/07/EN, WP 136.

Osiński, R. (2017). *Rewolucyjne zmiany w ochronie danych osobowych w 2018 r.*, Infor.pl

Piątek, S. (2015). Prawne warunki stosowania cookies. *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, *6*(4).

Pryciak, M. (2010). Prawo do prywatności. W: M. Sadowski i P. Szymaniec (red.), *Prawa człowieka: idea, instytucje, krytyka*. Wrocław: Wrocławskie Studia Erazmiańskie.

PWC (2017). *10 najważniejszych zmian, które wprowadza RODO*, pwc.pl

Rachelski i Wspólnicy Kancelaria Prawna (2017). *RODO a nowe obowiązku przedsiębiorców*, Infor.pl

Sakowska-Baryła, M. (2015). *Prawo do ochrony danych osobowych*. Wrocław: Prescom sp. z o.o.

Szlawski, W. (2014). *Firma osoby fizycznej prowadzącej działalność gospodarczą – dane osobowe czy nie?* PortalODO

Wiecióra D. (red.) (2016). *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*. Warszawa: C.H. Beck.

Wyrzykowski, M. (1999). *Ochrona danych osobowych*. Warszawa: Instytut praw Publicznych.

**Orzecznictwo:**

Wyrok NSA z dnia 28 listopada 2002 roku, II SA 2289/01

Wyrok NSA z dnia 28 listopada 2002 roku, II SA 3389/01

Wyrok WSA w Warszawie z dnia 3 marca 2009 roku, II SA/Wa 1495/08

**Akty prawne:**

Decyzja GIODO z 26 listopada 2009 roku, DOLiS/DEC-1183/09 dot. DOLiS-440-459/09

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

Kodeks cywilny (Dz.U. 2017 poz. 459)

Kodeks Pracy (Dz.U. 2018 poz. 108)

Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika, Dz.U. 1996 nr 62 poz. 286

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, Dziennik Urzędowy Unii Europejskiej L 119 z dnia 4 maja 2016 r.

Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz.U. 2004 nr 173 poz. 1807)

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922)

Ustawa z dnia 19 listopada 1999 r. Prawo działalności Gospodarczej (Dz. U. Z 2004 r. Nr 173, poz. 1808)

**Strony internetowe:**

www.encyklopedia.pwn.pl

www.giodo.gov.pl

www.sjp.pwn.pl

www.uodo.pl