KRZYSZTOF CYGAŃCZUK

Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego Państwowy Instytut Badawczy

*kcyganczuk@cnbop.pl*

JÓZEF JANCZAK

Instytut Zarządzania, Wydział Zarządzania i Dowodzenia, Akademia Sztuki Wojennej

*j.janczak@akademia.mil.pl*

# Zmiany w prawie unijnym w zakresie ochrony danych osobowych

## *Changes in EU law in the area of personal data protection*

STRESZCZENIE

Celem referatu jest omówienie istotnych zagadnień dotyczących sposobów wdrażania przepisów rozporządzenia o ochronie danych osobowych (RODO), w tym wykorzystania dotychczasowych doświadczeń w stosowaniu przepisów o ochronie danych osobowych. Przeprowadzono analizę najważniejszych zmian wprowadzonych w unijnym rozporządzeniu o ochronie osób fizycznych w 2016 roku. Dokonano również oceny poziomu ochrony danych osobowych w sektorze publicznym oraz analiz stopnia spełnienia wymogów dotyczących tworzenia prawidłowej dokumentacji ochrony danych osobowych w Polsce.

ABSTRACT

The purpose of the paper is to discuss important issues related to the implementations of the RODO rules, including the use of previous experience in applying the rules. The most important changes introduced by the EU Personal Protection Regulation in 2016 have been analyzed. Moreover, we have assessed the level of personal data protection in the public sector and analyzed the degree of compliance with the requirements concerning the creation of correct personal data protection records in Poland.

**Słowa kluczowe:** bezpieczeństwo informacji, dane osobowe, administracja publiczna, dokumentacja ochrony danych osobowych, polityka bezpieczeństwa informacji.

**Keywords:** security of information, personal data, public administration, documentation of personal data protection, Information Security Policy.

## Wprowadzenie

Rozwojowi nowoczesnych technologii towarzyszą nowe wyzwania w środowisku przetwarzania danych osobowych. Wynikają one z upowszechnienia pracy w systemach informatycznych zarówno w organizacjach, jak i życiu prywatnym, rośnie liczba urządzeń podłączonych do Internetu, a także poprawia się ich wydajność i możliwości usługowe. Obserwuje się wzrost popularności portali społecznościowych, zakupów przez Internet i bankowości elektronicznej mobilnej. Korzystając z Internetu stacjonarnego lub mobilnego, telefonii komórkowej oraz innych technologii dostępowych osoby trzecie mogą pozyskiwać coraz więcej danych nie tylko w celach komercyjnych na temat miejsca i charakteru pracy lub pobytu, lecz także relacji międzyludzkich, a nawet zamożności użytkowników globalnych sieci informacyjnych.

Wobec tego pojawiają się w przestrzeni komunikacyjnej nowe kategorie danych osobowych, takich jak dane geolokalizacyjne[1], profil użytkownika – konsumenta[2] itp., niewystępujące dotąd. W 2016 roku minęło 21 lat od przyjęcia dyrektywy 95/46/WE Parlamentu Europejskiego i Rady WE[3], ustalającej zasady zbierania, gromadzenia, przechowywania i udostępniania danych osobowych. W erze informacyjnej, w której dominują nowoczesne cyfrowe technologie, jest to relatywnie długi okres. Przez ten czas zmieniły się diametralnie metody, techniki i warunki przetwarzania danych osobowych w porównaniu z okresem, w którym uchwalano „starą" dyrektywę. Zawarte w niej uregulowania okazały się nie tylko nieaktualne, lecz także zbyt skomplikowane i rozdrobnione, gdyż dyrektywa ta nie była implementowana do porządków krajowych w ten sam sposób. Wobec powyższego konieczne było zastąpienie krajowych regulacji jednym aktem prawnym w tym samym brzmieniu obowiązującym na terenie całej Unii Europejskiej. Uznano, że odpowiedzią na zidentyfikowane potrzeby ujednolicenia zasad i procedur w zakresie zapewnienia skutecznej ochrony danych osobowych w UE, w zmieniającym się otoczeniu (gospodarczym, technologicznym i organizacyjnym), są regulacje przyjęte w 2016 roku w tym obszarze problemowym. Miały one prowadzić przede wszystkim do dostosowania unijnych ram prawnych do nowych warunków technologicznych, zastąpienia nadmiernej biurokracji jednym aktem, ułatwienia przedsiębiorcom prowadzenia działalności oraz wzmocnienia praw obywateli.

## Pakiet proponowanych zmian w UE dla wzmocnienia ochrony danych osobowych

Na początku 2012 roku Komisja Europejska przedstawiła pakiet proponowanych zmian w celu wzmocnienia ochrony osób, których dane podlegają przetwarzaniu. W pakiecie tym zawarte są dwa projekty aktów prawnych – rozporządzenia zastępującego wycofywaną dyrektywę 95/46/WE i tzw. dyrektywy policyjnej, będącej *novum* regulacyjnym, mającym zapewnić prawo do ochrony danych osobowych w procesach ścigania i zwalczania przestępstw. W toku podjętych prac legislacyjnych oraz w odpowiedzi na uwagi zgłoszone przez Parlament Europejski (2014.03.12) i Radę (2015.06.11) udało się wypracować wspólne stanowisko. Kompromis osiągnięto między 3 instytucjami europejskimi: Radą, Komisją i Parlamentem. Wynegocjowany dokument odbiegał nieco od projektu przedstawionego na samym początku, jednak zasadniczo zakres regulacji pozostał bez zmian (Piech, 2016, s. 27–28).

W dniu 4 maja 2016 r. w Dzienniku Urzędowym UE L 119 zostały opublikowane oficjalne teksty następujących aktów prawnych składających się na reformę ochrony danych:

- 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) (dalej RODO);
- dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (dalej dyrektywa policyjna).

Dyrektywa weszła w życie dzień po publikacji, a rozporządzenie – które we wszystkich krajach członkowskich ma być stosowane bezpośrednio – po 20 dniach. Państwa dostały dwa lata na wdrożenie dyrektywy policyjnej do swoich przepisów krajowych. Rozporządzenie jako akt obowiązujący bezpo-

średnio nie wymaga wydania żadnego aktu wdrażającego w krajach członkowskich. Sądzi się jednak, że w Polsce konieczne będzie przyjęcie nowej ustawy, gdyż nie ma w naszym kraju aktu, który by regulował tę problematykę. W efekcie ma nastąpić pełna zgodność krajowego prawa o ochronie i przepływie danych z prawem obowiązującym w UE.

Dwuletnie *vacatio legis* (do 24 maja 2018 roku) to czas dla państw członkowskich UE, w tym Polski na przygotowanie się do stosowania nowych regulacji. Ustawodawcy powinni dokonać niezbędnych zmian przepisów o ochronie i przepływie danych w oparciu o analizę wpływu rozporządzenia na poszczególne instytucje i branże, a także dokonać przeglądu i ewentualnej nowelizacji przepisów znajdujących się w innych aktach prawnych dotyczących rozmaitych dziedzin (Krzysztofek, 2016, s. 5). Należy mieć na uwadze, że w okresie przejściowym zastosowanie nadal będą mały nasze krajowe przepisy o ochronie danych osobowych (Kowalik, Wociór, 2016, s. 4).

Z analizy dokumentów unijnych wynika, że dyrektywa policyjna gwarantuje ochronę osób w związku z przetwarzaniem danych osobowych na potrzeby zapobiegania, dochodzenia, wykrywania oraz ścigania przestępstw lub wykonywania sankcji karnych. Działania w tym obszarze problemowym należą do obowiązków służb odpowiedzialnych za zapewnienie bezpieczeństwa publicznego (głównie służb i różnych straży), które kierują się swoimi procedurami. Celem przyjęcia rozporządzenia w sprawie ochrony osób fizycznych było zapewnienie wysokiego i jednolitego poziomu bezpieczeństwa danych osobowych na terenie UE. Regulacja ta w założeniu miała być neutralna technologicznie. Należy sądzić, że podczas jej stosowania pojawi się wiele mechanizmów oraz instrumentów prawnych odnoszących się do cyfrowej gospodarki XXI wieku. Wśród nich pojawi się:

- nowe lub inaczej zdefiniowane prawa, w tym prawo do bycia zapomnianym;
- koncepcje, które dotąd miały charakter jedynie teoretycznych postulatów, np. obowiązek zgłaszania naruszeń, czy też ochrona danych w fazie projektowania,
- modyfikacje i powstanie niektórych terminów spowodowane uwzględnieniem środowiska cyfrowego, w tym nowa definicja danych osobowych (Wilk, 2016, s. 12).

W tym miejscu warto podkreślić także, że treść rozporządzenia o ochronie danych powstała w oparciu o cały dotychczasowy dorobek legislacyjny oraz orzeczniczy, jaki rozwijał się w Europie przez ostatnie dziesięciolecia. Rozporządzenie to jest postrzegane jako akt przyszłości, który zmieni model ochrony dany osobowych. Dawne ograniczanie się przede wszystkim do wypełniania obowiązków notyfikacyjno-rejestracyjnych zostało zastąpione przez przenoszenie najważniejszych zasad na poziom praktycznych rozwiązań i procedur oraz zapewnienie ich realnego przestrzegania (Wilk, 2016, s. 11). Poniżej zidentyfikowano i przeanalizowano najważniejsze zmiany.

## Nowa rola administratorów bezpieczeństwa informacji

Po 2018 roku administratorzy bezpieczeństwa informacji (ABI) będą dalej pełnić swoje zadania, jednak już jako inspektorzy ochrony danych (IOD). Unijni ustawodawcy nie tylko zmienili nazwę, lecz także zmodyfikowali i wzmocnili ich status. Nałożył na IOD wiele nowych obowiązków. W przypadku podmiotów organizacji publicznych, w tym administracji, wprowadzono istotną zmianę, nakazując im powoływanie inspektorów ochrony danych w każdej sytuacji. Pozostałym podmiotom zapewniono możliwość swobodnego wyboru funkcjonowania z IOD lub radzenia sobie bez niego. Innym ważnym, a zarazem innowacyjnym rozwiązaniem, jest stworzona możliwości wyznaczania wspólnego IOD dla grup przedsiębiorców oraz podmiotów publicznych. Zwiększono przy tym wymagania wobec kwalifikacji kandydatów na stanowisko IOD. W art. 39 RODO określono też liczne zadania inspektorów ochrony danych, do których zaliczono przede wszystkim:

- edukowanie administratora danych, rozumiane jako informowanie go o jego zadaniach wynikających z obowiązujących przepisów;
- monitorowanie przestrzeganie rozporządzenia, innych przepisów europejskich i krajowych oraz polityk administratora danych;
- audyty oraz szkolenia personelu;
- łączenie współpracy z organem ochrony danych, w naszym kraju funkcję tę pełni GIODO (będzie UODO) z funkcją punktu kontaktowego.

Przedstawione powyżej zadania (nowe lub zmodyfikowane) są uważane jako minimum, które nie zamyka drogi do podejmowania innych czynności oraz działań na rzecz poprawy bezpieczeństwa danych osobowych (Bielak-Jomaa, Lubacz, 2016, s. 154–155).

## Dodatkowe obowiązki administratora danych osobowych

Dodatkowe obowiązki administratorów danych osobowych najogólniej podzielono na dwie grupy. Pierwsza grupa dotyczy obowiązków informacyjnych administratorów. Obowiązki te wynikają z poszerzonych uprawnień osób, których dane podlegają przetwarzaniu. Do obowiązków tych należy informowanie każdej osoby o przypadkach sprostowania, usuwania, ograniczenia przetwarzania jej danych osobowych lub gromadzenia danych na jej temat. Pozostały też znane z dotychczasowej ustawy o ochronie danych osobowych zagwarantowane prawa dostępu i do poprawiania danych, a także dbałość o ich poprawność. Druga grupa obejmuje natomiast czynności, które są związane z wdrożeniem środków organizacyjnych oraz technicznych dotyczących danych osobowych.

Twórcy unijnego rozporządzenia dokonali także modyfikacji wymogów administracyjnych. Wobec czego zrezygnowali z obowiązkowego rejestrowania zbiorów danych u krajowych organów nadzoru dokonywanych przez administratorów danych. Takiego obowiązku nie będą mieli też inspektorzy ochrony danych. Nie zwalniano jednak administratorów z obowiązku posiadania wiedzy o przetwarzanych przez nich zbiorów danych lub znajdujących się w ich posiadaniu, o czym świadczą art. 37–39 RODO. Oznacza to, że prowadzenie przez nich rejestru zbioru danych osobowych będzie nadal praktykowane. Natomiast nowym administracyjnym obowiązkiem inspektorów ochrony danych (IOD) ma być prowadzenie wewnętrznych rejestrów wszystkich dokonywanych czynności przetwarzania. W rejestrach tych powinny znaleźć się:

- dane osobowe oraz kontaktowe administratorów, współadministratorów, inspektorów danych osobowych i ich przedstawicieli;
- cele przetwarzania danych, które przyczynią się do łatwiejszego identyfikowania celowości przetwarzania oraz usprawnią przebieg ewentualnych kontroli;
- kategorie przetwarzanych danych oraz kategorie osób, których one dotyczą;
- wykazy osób lub kategorii, którym dane są ujawniane, a zwłaszcza tych, którzy funkcjonują poza obszarem UE;
- informacje dotyczące przekazywania danych do państw trzecich (jeśli do nich dochodzi);

- planowane terminy usuwania i niszczenia danych, zgodnie z zasadą czasowości przetwarzania;
- opis podjętych działań i środków bezpieczeństwa.

Należy sądzić, że rejestry zabierające takie dane mogą zastąpić od 2018 roku obowiązujące dokumenty, czyli politykę bezpieczeństwa informacji oraz instrukcję zarządzania systemem informacyjnym, które prowadzone są w obecnej formie przez administratorów. Zgodnie z art. 30 RODO rejestr ma stać się kompleksowym dokumentem dotyczącym ochrony danych osobowych. Będzie obowiązywał zarówno podmiotów z sektora publicznego, jak i prywatnego.

## Nowy status krajowych organów ochrony danych osobowych

Zgodnie z zapisami w nowym rozporządzeniu unijnym obecne krajowe organy powoływane do spraw ochrony danych osobowych zostały nazwane organami nadzorczymi. W Polsce organem tym jest Generalny Inspektor Ochrony Danych Osobowych (GIODO). Unia Europejska nie określiła szczegółowych wytycznych odnośnie do ustanawiania państwom członkowskim. Nie określono też trybu ich powoływania, wymaganych kwalifikacji, długości kadencji, możliwości ponownego wyboru ani też dodatkowych obowiązków zatrudnianego w urzędzie personelu. Decyzja w tej kwestii pozostaje do samodzielnego uregulowania na poziomie krajowym. Widnieje natomiast zapis w RODO (rozdział 6), że krajowy organ nadzoru powinien być niezależny oraz wybierany przez rząd, parlament głowę państwa. Powinien znać przepisy o ochronie danych osobowych, doświadczenie oraz odpowiednie kwalifikacje. Organ ten powinien posiadać niezbędne zasoby techniczne, finansowe oraz kadrowe do wypełnienia swoich obowiązków. Wydaje się, że zadania i uprawnienia przyznane organom nadzorczym w rozporządzeniu unijnym (art. 55–62 RODO) są zbliżone do polskich regulacji ustawowych odnoszących się do GIODO. Pewną nowością jest przyznanie temu organowi dodatkowych uprawnień nadzorczych i naprawczych, np.: nakazywanie administratorom sprostowania, usunięcia danych itp.; nakładanie zakazów przetwarzania; prowadzenie audytów i certyfikowania. Obecnie, w zgodzie z polskim prawem, GIODO posiada jedynie kompetencje do przeprowadzania kontroli i wydawania decyzji administracyjnych. Zwrócono także uwagę na współpracę między organami nadzorczymi (Nowakowski i inni, 2016, s. 249). W tej sytuacji przyjęcie ROchrOsFiz prawdopodobnie będzie

wiązało się z koniecznością nowelizacji ustawy o ochronie danych osobowych w Polsce oraz dostosowania przepisów o GIODO do nowych regulacji unijnych. Jak podkreślono powyżej, status, uprawnienia oraz procedura wyboru GIODO w dużej mierze odpowiadają określonym wymogom w rozporządzeniu unijnym. Poszerzony został jednak zakres kompetencji w zakresie nadzoru, a także współpracy międzynarodowej. Wobec tego zaszła potrzeba dokonania zmian w przepisach krajowych. Wydawało się, że nazwa organu (Generalny Inspektor Ochrony Danych Osobowych) na tyle trwale zapisała się w świadomości naszego społeczeństwa, że w nowej ustawie o ochronie danych osobowych może zostać zachowana w niezmienionym brzmieniu. Ostateczne rozstrzygnięcie zależeć będzie jednak od woli ustawodawcy. W projekcie nowej ustawy o ochronie danych osobowych procedowanym w Polsce umieszczono zapis Prezes Urzędu Ochrony Danych Osobowych (Kuflewski, 2017, s. 1).

## Wprowadzenie ochrony w fazie projektowania i domyślnej ochrony danych

Wprowadzenie ochrony w fazie projektowania i domyślnej ochrony danych wynika bezpośrednio z zapisów art. 25 RODO. Regulacja ta nie występowała wcześniej w prawie UE ani też w regulacjach krajowych, chociaż wynikała bezpośrednio z zasady adekwatności. Wprowadzona w rozporządzeniu regulacja w zakresie ochrony w fazie projektowania polega na zapewnieniu gwarancji poszanowania prywatności już w fazie konstruowania założeń i instrumentów (aplikacji, urządzeń i całych systemów ochrony danych). Do jej wdrożenia postuluje się podejście proaktywne zamiast reaktywnego oraz zaradcze zamiast naprawczego (Krzysztofek, 2016, s. 208). Ochrona danych w toku projektowania polega więc na tym, że w czasie tworzenia nowego systemu, a nawet urządzenia, rozważa się ich wpływ na sferę prywatności. Przewiduje się możliwe problemy, a nie reaguje dopiero, gdy one wystąpią. Rozwinięciem ochrony danych w toku projektowania jest ochrona domyślna (ang. *privacy by default*), obejmująca przedsięwzięcia w trakcie konstruowania aplikacji i systemów. Rozwiązania te mają zapewnić możliwość konfigurowania ustawień prywatności przez samego użytkownika. Użytkownik ma też mieć zapewnioną możliwość podejmowania decyzji o udostępnieniu danych osobowych na swój temat osobom trzecim. Reprezentatywnym przykładem tego rozwiązania jest udostępnianie danych osobowych przez portale społecznościowe. Obecnie zarządcy tych por-

tali bardzo swobodnie zarządzają ustawieniami domyślnymi. Po wejściu w życie rozporządzenia zarządcy portali społecznościowych będą zobowiązani do konfiguracji ustawień domyślnych, aby nie było automatycznej zgody na publiczne udostępnianie danych, zdjęć i postów itp.

## Poszerzenie zakresu uprawnień dla podmiotów danych

W rozporządzeniu o ochronie danych osób fizycznych zdefiniowano nowe i rozbudowano dotychczasowe uprawnienia przysługujące osobom, których dane są przetwarzane zarówno przez podmioty sektora publicznego, jak i prywatnego. Większość z tych uprawnień jest zbliżona treścią do uregulowań krajowych zawartych w ustawie o ochronie danych osobowych. Znajdują się też zupełnie nowe uregulowania, do których należą między innymi:

- prawo dostępu,
- prawo usunięcia danych (do bycia zapomnianym),
- prawo do przenoszenia danych,
- prawo sprzeciwu (istniejące w naszych przepisach krajowych, art. 32 ust. 1 pkt ustawy o ochronie danych osobowych).

Zgodnie z pkt 63 preambuły RODO „każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Obejmuje to prawo dostępu osób, których dane dotyczą, do danych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi. Dlatego też każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania".

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych (art. 17 RODO), a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zacho-

dzi jedna z następujących okoliczności: dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane; osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania; osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania; dane osobowe były przetwarzane niezgodnie z prawem; dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator; dane te zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

Prawo do przenoszenia danych (art. 20 RODO) dotyczy osoby, której dane dotyczą. Ma ona prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli: przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz przetwarzanie odbywa się w sposób zautomatyzowany.

Kiedy RODO zacznie obowiązywać, prawo odmowy obejmie również sprzeciw wobec profilowania (art. 22 RODO). Każdemu zapewnia się możliwość sprzeciwienia się dalszemu przetwarzaniu jego danych osobowych. Sprzeciw jest skuteczny, jeżeli administrator nie wykaże istnienia uzasadnionych podstaw przetwarzania (np. prawnych). W przypadku przetwarzania danych osobowych do celów marketingowych sprzeciw będzie można wnieść w dowolnym momencie i od tej chwili dane tej osoby nie będą mogły podlegać dalszemu przetwarzaniu.

## Określenie zasad profilowania

Profilowanie[4] jest metodą przetwarzania danych oraz kategoryzowania ludzi. Polega na dopasowywaniu i korelowaniu określonych zachowań (np. preferencji i decyzji konsumenckich) z cechami, takimi jak płeć, wiek, wykształcenie, zainteresowania. Jest szeroko wykorzystywane zarówno przez przedsiębiorców,

którzy dopasują swoje usługi do profili i potrzeb odbiorców, jak i w sektorze publicznym (np. przez policję i służby bezpieczeństwa oraz organy administracji publicznej odpowiedzialne za politykę społeczną lub aktywizację zawodową. Reforma prawa unijnego stała się okazją do ucywilizowania tego procesu. W art. 4 ust. 4 RODO znajduje się europejska definicja, natomiast w art. 22 RODO wprowadzono ograniczenia i przyznano podmiotom danych prawo sprzeciwu wobec profilowania. Tym samym profilowanie zostało dopuszczone jedynie w kilku określonych sytuacjach, jeżeli: jest niezbędne do zawarcia czy wykonania umowy oraz jeżeli pozwala na to przepis krajowy, który jednocześnie przewiduje zastosowanie odpowiednich środków ochrony; podmiot danych sam wyrazi na to zgodę. Ograniczenia uprawnień dotyczących profilowania wynikają zawsze z przepisów i mają służyć zapewnieniu bezpieczeństwa publicznego, zapobieganiu przestępstwom, ochronie życia itp. (Niklas, 2015).

## Zawiadomienie o naruszeniach ochrony danych osobowych

W RODO wprowadzono nowy obowiązek dla administratorów danych poinformowania osoby o tym, że doszło do naruszenia bezpieczeństwa jej danych osobowych. Określane jest też jako prawo do bycia informowanym. Dotyczy ono sytuacji, gdy incydent poważnie zagraża prawom oraz wolnościom podmiotów danych. Zawiadomienie musi być sformułowane zrozumiale i określać możliwe konsekwencje tego naruszenia. Powinno określać również środki zastosowane w celu zminimalizowania negatywnych skutków oraz informować, gdzie lub u kogo udzielane są dodatkowe informacje. Unijny ustawodawca zamieścił jednak w rozporządzeniu kilka zwolnień z tego obowiązku. Dotyczą one sytuacji, gdy administrator zdążył zareagować i zastosował środki ochrony danych w celu zmniejszenia prawdopodobieństwa wystąpienia zagrożenia dla praw i wolności. W sytuacji gdy zawiadamianie wymaga nieproporcjonalnie dużego wysiłku, dopuszcza się możliwość wystosowania publicznego komunikatu.

Wprowadzenie obowiązkowego zawiadamiania wydaje się trafnym rozwiązaniem, ponieważ nie tylko poszerzyło uprawnienia osób, których dane są przetwarzane, lecz także może przyczynić się do poprawy bezpieczeństwa. Skuteczne zawiadomienie obywateli o wystąpieniu naruszenia prawdopodobnie zajmie na tyle dużo czasu oraz będzie tak kosztowne, że bardziej opłacalne okaże się stworzenie procedur zapobiegających incydentom oraz wdrożenie technicznych i organizacyjnych zabezpieczeń.

## Większa ochrona dzieci

W RODO uwagę zwrócono również na szczególną ochronę danych osobowych dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń oraz praw przysługujących im w związku z przetwarzaniem danych osobowych wykorzystywanych do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika, a także gdy korzystają one z usług skierowanych bezpośrednio do nich. Wyrazem troski o najmłodszych było poszerzenie lub przyznanie im szczególnej ochrony. Dzieci zwykle mają bowiem mniejszą świadomość konsekwencji swoich czynów, czyhających na nie zagrożeń czy przysługujących im praw. W odniesieniu do usług internetowych (głównie korzystania z portali społecznościowych) twórcy rozporządzenia w art. 8 RODO przewidzieli, że do momentu ukończenia przez dziecko 16. roku życia zgodę na przetwarzanie jego danych osobowych wydają rodzice lub prawni opiekunowie. Państwom członkowskim pozostawiono pewną swobodę w uregulowaniu tej kwestii i zezwolono im na ewentualne obniżenie progu wiekowego (maksymalnie do 13 lat).

## Sankcje administracyjne za naruszenie przepisów ochrony danych osobowych

Twórcy RODO nie przewidzieli potrzeby uchwalenia przejściowych przepisów. Wobec tego wszystkie toczące się procesy przetwarzania danych osobowych mają być dostosowane do wymogów niniejszego rozporządzenia w ciągu dwóch lat od dnia jego wejścia w życie. Wymóg tego dostosowania zabezpieczono systemem bardzo wysokich pieniężnych sankcji zarówno na przedsiębiorstwa[5], jak i osoby niebędące przedsiębiorstwem. Dla wspierania spójnego stosowania administracyjnych kar pieniężnych przewidziano także używanie mechanizmu spójności. Wobec tego państwa członkowskie zostały zobowiązane do określenia, czy oraz w jakim zakresie administracyjnym karom pieniężnym powinny podlegać organy publiczne. Postanowiono też, że nałożenie administracyjnej kary pieniężnej lub wydanie ostrzeżenia nie wpływa na stosowanie innych uprawnień organów nadzorczych ani sankcji na mocy niniejszego rozporządzenia. Artykuł 83 RODO, dotyczący ogólnych warunków nakładania administracyjnych kar pieniężnych, ma ułatwić egzekwowanie przestrzegania przepisów. Za niewywiązywanie się lub nienależyte wypełnianie nowych obowiązków grozi kara pieniężna od 10 do 20 milionów euro lub od 2% do 4% wysokości rocznych obrotów w przypadku przedsiębiorstw.

## Podsumowanie

Wprowadzenie przedstawionych powyżej zmian w poszczególnych państwach UE ma ograniczyć możliwości wystąpienia rozbieżności w unijnym prawie o ochronie danych osobowych. Jednolite stosowanie przepisów unijnych nie eliminuje jednak całkowicie regulacji krajowych. Analiza treści RODO pozwala bowiem na wyodrębnienie czterech grup spraw pozostawionych państwom członkowskim do uregulowania we własnym zakresie (Wilk, 2016, s. 9):

1. Kwestie wymagające przyjęcia odpowiednich przepisów krajowych, a jako przykład można podać wymóg ustanowienia niezależnego organu ochrony. Do krajowych ustawodawców pozostawiono decyzję m.in. o sposobie jego wyboru, kadencyjności itp.
2. Sprawy, które krajowy ustawodawca może uregulować odmiennie, nie wykraczając jednocześnie poza ramy RODO. Przykładem może być możliwość obniżenia progu wiekowego, od którego dzieci mogą same wyrażać zgodę na przetwarzanie swoich danych osobowych w Internecie, jeżeli mają co najmniej 13 lat (w RODO określono ukończony 16. rok życia – art. 8).
3. Ustawodawcy krajowi mają możliwość precyzowania spraw określonych w RODO.
4. Wprowadzenie instytucji wyłączeń i ograniczeń, które kraje mogą wprowadzać pod określonymi warunkami.

Wobec powyższego wdrożenie RODO niesie ze sobą konieczność dostosowania istniejącego krajowego ustawodawstwa do nowych przepisów unijnych. Należy nie tylko wykonać te przedsięwzięcia terminowo (do 25 maja 2018 roku), lecz także zachowując przy tym najwyższe standardy prawodawstwa oraz ochrony praw obywatelskich. Mimo że RODO ma status aktu bezpośrednio skutecznego, to jednak niektóre kwestie powinny być doprecyzowane lub uregulowane w zgodzie z prawem krajowym. Mając na uwadze konieczność zapewnienia bezpieczeństwa i porządku publicznego, dopuszcza się możliwość wprowadzania wyjątków i odstępstw przez państwa członkowskie mieszczących się w przyjętych normach i z poszanowaniem prawa unijnego.

W przypadku drugiego dokumentu, czyli dyrektywy policyjnej, zachowano jeszcze większą swobodę państwom członkowskim (Walkowiak, Niklas, 2016). Obecnie trudno jest nawet oszacować, ile ustaw będzie wymagało uchylenia lub nowelizacji.

Z informacji podanych do publicznej wiadomości przez nasze Ministerstwo Cyfryzacji, które odpowiada za implementację RODO i koordynację procesu dostosowywania sytuacji w naszym kraju do wymogów unijnych w zakresie przetwarzania danych osobowych wynika, że przynajmniej kilkaset aktów prawnych musi zostać poddanych aktualizacji pod kątem ich zgodności z nowymi przepisami unijnymi. Projekt ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych wraz z dokumentami towarzyszącymi znajduje się w Wykazie prac legislacyjnych Rady Ministrów pod numerem UC100[6]. Zgodnie z projektem z dniem wejścia w życie nowej ustawy o ochronie danych osobowych, Biuro Generalnego Inspektora Ochrony Danych Osobowych ma stać się Urzędem Ochrony Danych Osobowych (Kuflewski, 2017, s. 1).

Podsumowując, w Polsce trwają obecnie prace nad dostosowaniem prawa krajowego do wymogów przepisów unijnych. W nowej ustawie o ochronie danych osobowych powinny znaleźć się przede wszystkim uregulowania dotyczące nowego statusu oraz poszerzonych kompetencji organu ochrony, w tym do nakładania kary finansowej. Nasz ustawodawca powinien zająć się też zasadami nadzoru oraz współpracy w celu zapewnienia ochrony danych osobowych. Należy uwzględnić także instytucje i procedury, które nie występowały wcześniej w polskim porządku prawnym, np. podmioty certyfikujące czy też procedura certyfikacji.

## Bibliografia

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

Bielak-Jomaa J.E., Lubasz D. (red.). (2016). *Polska i europejska reforma ochrony danych osobowych*. Warszawa: Wolters Kluwer.

Kowalik P., Wociór D. (2016). *Rozdział I. Zastosowanie przepisów o ochronie danych osobowych w jednostkach sektora publicznego*, [w:] I. Rogowska (red.), *Ochrona danych osobowych w sektorze publicznym z uwzględnieniem ogólnego rozporządzenia unijnego*, wyd. 3. Warszawa: C.H.Beck.

Krzysztofek M. (2016). *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*. Warszawa: C.H. Beck.

Kuflewski P. (2017). *Projekt ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych*, pdf, MC.

Niklas J. (2015). *Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji*, http://ptpa.org.pl/site/assets/files/publikacje/opinie/Opinia_profilowanie_w_kontekscie_ ochrony_danych_osobowych_i_zakazu_dyskryminacji.pdf [dostęp: 24.04.2017].

Nowakowski B., Kowalik P., Wociór D. (2016). *Uprawnienia organu do spraw ochrony danych osobowych*, [w:] I. Rogowska, *Ochrona danych osobowych w sektorze publicznym z uwzględnieniem ogólnego rozporządzenia unijnego*. Warszawa: C.H. Beck.

Piech M. (2016). *„Deregulacyjna" nowelizacja i unijna reforma zasad ochrony danych osobowych z perspektywy administratora danych osobowych*, [w:] E. Bielak-Jomaa, D. Lubacz (red.), *Polska i europejska reforma ochrony danych osobowych*. Warszawa: Wolters Kluwer.

Rogowska I. (red.). (2016). *Ochrona danych osobowych w sektorze publicznym z uwzględnieniem ogólnego rozporządzenia unijnego*, wyd. 3. Warszawa: C.H. Beck.

Rozporządzenie (WE) nr 45/2001 z dnia 18 grudnia 2001 roku o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L 8 z 12.01.2001.

Rozporządzenie Parlamentu Europejskiego z dnia 14 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz.Urz. UE L 119 z 4.05.2016 r.

Szczygielska W. (red.) (2016). *Ochrona danych osobowych w praktyce – 180 kluczowych porad z uwzględnieniem rewolucyjnych zmian rozporządzenia UE*. Warszawa: Wiedza i Praktyka.

Walkowiak A., Niklas J. (2016), *Reforma ochrony danych osobowych w Polsce: czy grozi nam bałagan?*, https://panoptykon.org/wiadomosc/reforma-ochrony-danych-osobowych-w-polsce-czy-grozi-nam-balagan [dostęp: 28.03.2017].

Wilk M. (red.). (2016). *Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych*, pdf. Warszawa: Biuro GIODO.

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

## Endnotes

[1] Na dane geolokalizacyjne składają się w szczególności: dane przekazywane z lokalizatorów oraz zewnętrznych systemów lokalizacji w postaci współrzędnych geograficznych dotyczących położenia środka transportu, daty i godziny pozyskania tych współrzędnych, daty i godziny zatrzymania środka transportu oraz numeru lokalizatora albo urządzenia. Źródło: http://www.mf.gov.pl/krajowa-administracja-skarbowa/wiadomosci/komunikaty/-/asset_publisher/2UWl/content/projekt-nowelizacji-ustawy-o-sent/pop_up?_101_INSTANCE_2UWl_viewMode=print [dostęp: 22.09.2017].

[2] http://www.egospodarka.pl/tematy/profil-konsumenta [dostęp: 22.09.2017].

[3] http://www.giodo.gov.pl/pl/568/603 [dostęp: 22.09.2017].

[4] Profilowanie polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobi-

stych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa (pkt 73 preambuły RODO).

[5] Jeżeli administracyjna kara pieniężna jest nakładana na przedsiębiorstwo, to przedsiębiorstwo należy do tych celów rozumieć zgodnie z art. 101 i 102 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Jeżeli administracyjna kara pieniężna jest nakładana na osobę niebędącą przedsiębiorstwem, organ nadzorczy, ustalając właściwą wysokość kary pieniężnej, powinien wziąć pod uwagę ogólny poziom dochodów w danym państwie członkowskim oraz sytuację ekonomiczną tej osoby (pkt 150 preambuły RODO), http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679 [dostęp: 10.10.2017].

[6] http://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-przepisy-wprowadzajace-ustawe-o-ochronie-danych-osobowych.html [dostęp: 10.10.2017].