ARTYKUŁ PRZEGLĄDOWY

Rozprawy Społeczne 2018, Tom 12, Nr 4
ISSN 2081-6081

BEZPIECZEŃSTWO DANYCH OSOBOWYCH W UNII EUROPEJSKIEJ OD 2018 ROKU

THE SECURITY OF PERSONAL DATA IN EUROPEAN UNION SINCE 2018

Dariusz Brążkiewicz[1(A,B,C,D,E,F,G)]

[1]Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej

Brążkiewicz, D. (2018). Bezpieczeństwo danych osobowych w Unii Europejskiej od 2018 roku. *Rozprawy Społeczne, 12*(4), 39-45. https://doi.org/10.29316/rs.2018.35

Wkład autorów:
A. Zaplanowanie badań
B. Zebranie danych
C. Dane – analiza i statystyki
D. Interpretacja danych
E. Przygotowanie artykułu
F. Wyszukiwanie i analiza literatury
G. Zebranie funduszy

Streszczenie
Intensywny rozwój technologii informatycznych w początkach XXI wieku powoduje, że dane osobowe obywateli są bezustannie przetwarzane przy użyciu coraz bardziej zaawansowanych technologii cyfrowych. Tym samym rozwój technologiczny obejmuje coraz więcej obszarów życia współczesnego człowieka, w tym administracyjny, ekonomiczny i finansowy. W celu utrzymania i poprawy bezpieczeństwa w zakresie ochrony danych osobowych potrzebne jest tworzenie nowych rozwiązań prawnych. Wprowadzenie jednolitych rozwiązań ponadpaństwowych w Unii Europejskiej pozwoli na wyeliminowanie lub zdecydowane ograniczenie zagrożeń związanych z gromadzeniem, przetwarzaniem i wykorzystaniem danych osobowych. Odpowiedzialność za to bezpieczeństwo spoczywać będzie, tak jak dotychczas na instytucjach i firmach oraz na profesjonalnie przygotowanych pracownikach nadzorujących lub przetwarzających te dane. Wraz z wejściem w życie Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO) Unii Europejskiej w dniu 25 maja 2018 r. znalazła zastosowanie zwiększona ochrona danych osobowych poprzez: zwiększenie analizy ryzyka przetwarzania danych osobowych, rozliczalność przetwarzania danych osobowych, domyślność ochrony danych osobowych oraz odpowiedzialność za naruszenie przepisów o ochronie danych osobowych, w tym bardzo wysokie kary finansowe.

Słowa kluczowe: RODO (Rozporządzenie Ogólne o Ochronie Danych Osobowych Unii Europejskiej), ochrona danych osobowych, bezpieczeństwo jednostki

Summary
Intensive development of information technology in the early 21st century means that citizens' personal data is constantly processed using increasingly advanced digital technologies. At the same time, technological development includes more and more areas of a modern man, including administrative, economic and financial areas. In order to maintain and improve security in the field of personal data protection, it is necessary to create new legal solutions. The introduction of unitary supranational solutions in European Union will eliminate or significantly reduce the risks associated with the collection, processing and use of personal data. Responsibility for this security will rest, as it has been until now, on institutions and companies, and professionally prepared employees who supervise or process this data. When the General Data Protection Regulation (GDPR) of the European Union came into force on 25 May 2018, increased protection of personal data will be applied by: increasing the analysis of the risk of personal data processing, accountability of personal data processing, privacy of personal data protection and liability for violation of the provisions on the protection of personal data, including very high financial penalties.

Keywords: GDPR (European Union General Data Protection Regulation), personal data protection, security of the individual

Tabele: 0
Ryciny: 0
Literatura: 11
Otrzymano: listopad 2017
Zaakceptowano: maj 2018

Wstęp

Współczesne społeczeństwo informacyjne potrzebuje zwiększonej ochrony danych osobowych. Globalizacja jak i postęp technologiczny w wymianie informacji wymusza dostosowanie zasad przetwarzania danych do współczesnych wymogów. W obecnej dobie postęp technologii informatycznych jak i wzrost ich znaczenia w życiu codziennym powoduje, że tzw. starzenie się systemów i rozwiązań zabezpieczających jest procesem bardzo szybkim (kilkuletnim a nie kilkudziesięcioletnim). Tym samym istnieje potrzeba zmian legislacyjnych gwarantujących bezpieczeństwo danych osobowych.

Prace Rady Unii Europejskiej nad zmianą dotychczasowych zasad ochrony danych osobowych obowiązujących od 1995 r. trwały od 2012 r. do 15 czerwca 2015 r. Rada dostosowując przepisy do ery cyfrowej przyjęła ogólne podejście do rozporządzenia o ochronie danych. Główne punkty wypracowa-

Adres korespondencyjny: Dariusz Brążkiewicz, Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej, ul. Sidorska 95/97, 21-500 Biała Podlaska, e-mail: d.brazkiewicz@dydaktyka.pswbp.pl, tel. 83 344 99 00, https://orcid.org/0000-0002-5372-1210

nego porozumienia obejmowały: większą ochronę danych, szersze możliwości biznesowe na jednolitym rynku cyfrowym, liczniejsze i lepsze narzędzia egzekwowania przepisów, gwarancje w razie przekazywania danych osobowych poza UE (Komunikat prasowy 450/15).

Ostatecznie po kilku latach intensywnych prac nad europejską reformą ochrony danych osobowych, 27 kwietnia 2016 roku przyjęto dwa istotne akty prawne:

- rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/697 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (w skrócie: RODO – Rozporządzenie Ogólne o Ochronie Danych Osobowych, w UE: GDPR – General Data Protection Regulation).
- dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 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 uchylającą decyzję ramową Rady 2008/977/WSSiSW.

Należy wskazać, że przepisy RODO weszły w życie po uchwaleniu, ale praktyczne stosowanie przepisów jest realizowane od 25 maja 2018 roku.

W związku z tym, że rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/697 jest wiodącym dokumentem w zakresie bezpieczeństwa danych osobowych, to jego zapisy są elementem największej uwagi i stanowią podstawę do regulacji na terenie całej Unii Europejskiej oraz ma wpływ na powstanie aktów prawnych w poszczególnych krajach. I ten dokument jest podstawą analizy zmian wchodzących do praktycznej realizacji w 2018 r.

Potrzeby zmian – rozwój technologiczny

Twórcy dyrektywy 95/46/WE tworząc w połowie lat 90-tych XX wieku prawo o ochronie danych osobowych nie byli w stanie przewidzieć ogromnych przemian i gigantycznego rozwoju technologii informatycznych jakie nastąpiły w początkach XXI wieku. Przede wszystkim nie przypuszczali, iż tak szybko powstanie i rozwinie się na globalną skalę przetwarzanie danych osobowych setek milionów Europejczyków w systemie elektronicznym. W systemach państwowych, korporacyjnych czy społecznościowych. W obliczu tego procesu gwałtownego rozwoju stało się jasne dla wszystkich, że problem wyrażania zgody czy egzekwowania praw przysługuje osobom, których dane podlegają przetwarzaniu wymaga zmian lub doprecyzowania. Tym samym dyrektywa 95/46/WE odeszła do historii a na jej miejsce z dniem 25 maja 2018 r. w życie wprowadzone zostały ww. akty prawne. Obydwa te akty prawne są w równym stopniu ważne i dopiero razem tworzą spójny system ochrony danych osobowych. Dla większości administratorów zaś ze względu na zakres zastosowania i charakter prawny elementarne znaczenie będzie miało rozporządzenie o ochronie danych osobowych (GDPR).

Do tej pory we wszystkich 28 krajach Unii Europejskiej obowiązywały oddzielne, różniące się między sobą ustawy o ochronie danych osobowych. RODO od maja 2018 roku jest jedynym aktem prawnym obowiązującym w całej Unii Europejskiej z dopuszczeniem prawnych regulacji krajowych, takich jak:

- spraw, co do których RODO wymaga przyjęcia przepisów krajowych jak np.: organ nadzorczy i środki finansowe do jego działalności;
- uregulowania spraw, w których ustawodawca krajowy ma możliwość odmienne, chociaż w określonych ramach kwestii wprost przewidzianych w RODO, np. wskazanie wieku dziecka w granicach 16-13 lat, od którego może ono samodzielnie wyrazić zgodę na przetwarzanie swoich danych osobowych;
- doprecyzowanie przez ustawodawcę krajowego kwestii organizacyjno-technicznych;
- wprowadzenie przez ustawodawcę krajowego ograniczeń praw zagwarantowanych przez RODO po spełnieniu warunków w nim określonych.

Regulacje krajowe są ważne, ale zdecydowaną nowością jest fakt, że zwiększy się rola niewiążących wytycznych i wskazówek wydawanych na poziomie europejskim przez nowo powołaną Europejską Radę Ochrony Danych oraz na poziomie krajowym. Do tej pory w Polsce był to Generalny Inspektor Ochrony Danych Osobowych (GIODO), a obecnie jest Prezes Urzędu Ochrony Danych Osobowych. Te wytyczne i wskazówki będą miały spore znaczenie praktyczne i mają zapewnić większą elastyczność w sposobie realizacji przez administratorów danych i podmioty przetwarzające. Zmieniające się środowisko działalności człowieka w zakresie technologii, organizacji i gospodarki wymusza poprawę skuteczności ochrony danych osobowych. Twórcy RODO doskonale zdawali sobie sprawę, jak radykalnie od 1995 roku zmieniły się metody przetwarzania danych. Ich inspiracją było m.in. – dogonić współczesne oczekiwania pojedynczego człowieka w zglobalizowanym świecie. Jeszcze kilkanaście lat temu nie istniało generowanie danych w postaci cyfrowej, nie było też zagrożeń wynikających ze zwiększonej możliwości wykorzystania tych danych. Tym samym rozwój technologiczny wymusił potrzebę zmiany modelu regulacji ochrony danych osobowych. Nowością w RODO jest odejście od obowiązków notyfikacyjno-rejestracyjnych a w zamian nastąpiło przeniesienie głównych zasad na poziomie procedur i rozwiązań praktycznych i zapewnienie ich realnego przestrzegania (GIODO 2016).

Zasady dotyczące przetwarzania danych osobowych wg art. 5 ust. 1 RODO:

„1. Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu");
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
d) 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");
e) 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, 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 przechowywania");
f) 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")."

Chociaż RODO w swojej podstawowej strukturze musi pozostać neutralne technologicznie, to jednak jego postanowienia wprowadzają zarówno mechanizmy jak i instrumenty prawne dotyczące gospodarki cyfrowej. Zostały więc wprowadzone nowe lub zdefiniowane na nowo prawa, np.:

– prawo do bycia zapomnianym (prawo do usunięcia danych) – art. 17,
– prawo do ograniczenia przetwarzania danych – art. 19,
– prawo do przenoszenia danych – art. 20;

a część praw, która do tej pory miały charakter teoretyczny obecnie weszły w życie i będą miały zastosowanie praktyczne, np.:

– zapewnienie ochrony danych na etapie projektowania,
– domyślna ochrona danych,
– zgłaszanie naruszeń ochrony danych osobowych.

RODO zmienia lub likwiduje:

– sformalizowaną dokumentację,
– zgłaszanie zbiorów,
– rejestr zbiorów,
– sztywne wymogi w zakresie zabezpieczenia danych - koniec ze zmianą haseł co 30 dni (Lubasz & Wspólnicy 2017).

Podstawowe zmiany – ryzyko, rozliczalność, projektowanie, domyślna ochrona

Jednym z ważniejszych elementów pojawiających się w przepisach RODO to pojęcie ryzyka. Zarówno podmiot przetwarzający dane, a w szczególności administratorzy danych powinni zawsze brać pod uwagę już istniejące lub mogące pojawić się ryzyka dla ochrony danych osobowych. Nadrzędnym celem staje się praktyczne zastosowanie odpowiednich do stopnia ryzyka środków bezpieczeństwa. W sytuacjach najwyższego ryzyka, gdy najistotniejsze jest zachowanie odpowiedniego poziomu ochrony, ustawodawca unijny zwalnia w wielu przypadkach administratorów z pozostałych obowiązków i nakłada nań obowiązek wykorzystania narzędzi zmniejszających ryzyko. Art. 4 RODO definiuje pojęcie „administratora", (fr.): „oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych …".

Kolejnym, ważnym elementem ochrony danych osobowych jest pojęcie rozliczalności, mające zastosowanie w wielu dziedzinach takich jak socjologia, zarządzanie czy prawo. Tym samym stanowi element poprzednich i obecnych regulacji ochrony danych osobowych. Zasada rozliczalności nabiera coraz większego znaczenia wraz ze zwiększaniem ilości przetwarzanych danych a także w obliczu konieczności zapewnienia właściwych gwarancji ochrony danych osobowych w kontekście transgranicznym. Bardzo ściśle zasadę rozliczalności i odpowiedzialności administratora definiuje art. 5 ust. 2 RODO. Bardzo ważne staje się przeniesienie zasad ogólnych ochrony danych, w tym obowiązków ratyfikacyjnych i rejestracyjnych na poziom praktycznych rozwiązań i procedur stosowanych w jednostkach przetwarzających dane osobowe. Tak więc – reasumując – w świetle nowych przepisów RODO to administrator ponosi odpowiedzialność za przestrzeganie przepisów prawa o ochronie danych osobowych i jego obowiązkiem jest wykazanie, że właściwie spełnia wymogi określone tymi przepisami.

W świetle nowych przepisów (art. 35 ust. 1 RODO) dla administratora obowiązkowa będzie

ocena skutków dla ochrony danych, która polega na zautomatyzowanym przetwarzaniu, a także profilowaniu. Jest ona konieczna, gdy przetwarzane są szczególne kategorie danych osobowych lub np. dane dotyczące wyroków sądowych i innych naruszeń prawa. Dalszą konsekwencją oceny skutków w zakresie ochrony danych są konsultacje administratora z organem nadzorczym. Reguluje to art. 36 RODO. Konsultacje – zgodnie z wprowadzonymi przepisami – powinny odbywać się w sytuacji, gdy ocena skutków wykaże, „… że przetwarzanie, powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka …". Organ nadzorczy udziela pisemne zalecenie dla administratora oraz podmiotowi przetwarzającemu w terminie ośmiu tygodni od wpłynięcia wniosku. W art. 58 RODO wyraźnie zaznacza się, że organ nadzorczy może skorzystać z kompetencji naprawczych. Tak więc, jeśli charakter konsultacji jest złożony, okres może być przedłużony o kolejne sześć tygodni. Jednocześnie jeśli organ nadzorczy nie posiada wszystkich informacji, które są mu niezbędne do celów konsultacji, terminy te mają prawo ulec wydłużeniu.

Dla administratorów i podmiotów przetwarzających art. 25 RODO wprowadza dwa działania:

– uwzględnianie ochrony danych w fazie projektowania,
– domyślna ochrona danych.

Pierwsze działanie gwarantuje, że w etapie projektowania podmioty przetwarzające przystąpią do realizacji rozwiązań służących ochronie danych. Tym samym usługodawca ma możliwość dopracowania systemu informatycznego gwarantującego ochronę danych osobowych według wymogów RODO na wszystkich etapach, z wdrożeniem włącznie. A tu należy uwzględnić zgodnie z art. 25 ust. 1 RODO: „…stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, …". Drugie, bardzo istotne działanie to domyślna ochrona danych. Początkowo działanie to dotyczyło osób przystępujących do nowych, powstających portali społecznościowych, a więc miała na celu ochronę danych osób przystępujących do usług świadczonych drogą elektroniczną. Domyślna ochrona danych miała uchronić niektórych użytkowników portali społecznościowych przed nieświadomym udostępnianiem swoich danych szerokim kręgom odbiorców. Obecne przepisy RODO rozszerzyły tę ideę. Tak więc obecnie domyślnie będą przetwarzane tylko takie dane, które są niezbędne dla osiągnięcia właściwego celu przetwarzania. To na administratorze spoczywa obowiązek wdrożenia odpowiednich środków organizacyjno-technicznych domyślnego przetwarzania danych. Administrator ponosi odpowiedzialność za odpowiednią ilość zbieranych danych, zakres ich przetwarzania, okres przechowywania danych, a także dostępność danych. Najistotniejsze jest natomiast aby domyślne dane nie były przekazywane bez interwencji zainteresowanej osoby nieokreślonej liczbie osób fizycznych.

Aby ułatwić podmiotom właściwe stosowanie przepisów RODO wprowadza możliwość tworzenia specjalnych kodeksów postępowania. Dla państw członkowskich, organów nadzorczych, dla Europejskiej Rady Ochrony Danych Osobowych kodeksy postępowania będą pomocne w doprecyzowaniu wymogów i specyfiki różnych sektorów, w których przetwarza się dane osobowe. Szczegóły dotyczące doprecyzowania przepisów RODO omawia art. 40 ust. 2. Zrzeszenia i podmioty tworząc kodeks postępowania muszą przedstawiać opracowany kodeks do zatwierdzenia organowi nadzorującemu. Zatwierdzony kodeks jest rejestrowany przez organ nadzorujący i przez niego jest też wydawany. Do nowości w RODO należy zaliczyć certyfikaty i znaki jakości oraz oznaczeń w zakresie ochrony danych, które będą wydawane na potwierdzenie zgodności przetwarzania operacji z przepisami RODO prowadzonych przez administratorów i podmioty przetwarzające. Certyfikacja ma być dobrowolna co gwarantują zapisy art. 42 ust. 3 RODO. Administrator i podmiot przetwarzający będą otrzymywały certyfikaty na okres 3 lat, z możliwością przedłużenia (GIODO 2016).

Odpowiedzialność za ochronę – sankcje administracyjne i finansowe, zgłaszanie naruszeń, notyfikacja naruszeń

Certyfikaty i znaki jakości przyznawane będą w przypadku odpowiedniego stosowania kodeksów postępowań, zaś w sytuacji naruszenia przepisów o ochronie danych osobowych RODO przewiduje złożone sankcje administracyjne do kar pieniężnych włącznie. Reguluje to art. 58 RODO. Zostały określone ściśle zasady odpowiedzialności cywilnoprawnej. Ujednolicono zasady nakładania kar pieniężnych przez organy nadzorcze i wyeliminowanie procederu przenoszenia działalności do państwa, w których sankcje za naruszenie tych samych wymogów są niższe. Konsekwencją tego ujednolicenia jest wzmocnienie i zharmonizowanie sankcji administracyjnych w całej Unii Europejskiej. To, że administracyjne kary pieniężne nakłada się razem z nakazami lub zamiast nich, reguluje art. 83 ust. 2 RODO. Do obowiązków rad nadzorczych należy także dopilnowanie aby kary były proporcjonalne, skuteczne i odpowiednio odstraszające. W art. 83 ust. 1 RODO ujednolica kryteria, które należy wziąć pod uwagę podejmując decyzję, czy nałożyć administracyjną karę pieniężną oraz jej wysokość. Biorąc pod uwagę rodzaj naruszenia RODO określa górne limity administracyjnych kar pieniężnych, przy czym najwyższy limit do 20 mln euro, zaś w przypadku przedsiębiorstw do 4% jego całkowitego światowego obrotu we wskazanej w art. 83, ust. 5 grupie naruszeń przepisów RODO oraz niższy limit kara do 10 mln euro i dla przedsiębiorstwa 2% obrotu we

wskazanej w art. 83, ust. 4 grupie naruszeń przepisów RODO. Rozporządzenie ogólne pozostawia państwom członkowskim decyzję, czy i w jakim zakresie można nakładać administracyjne kary pieniężne na organy i podmioty publiczne. Za naruszenie przepisów art. 82 RODO wprowadza zasady odpowiedzialności odszkodowawczej. Każda osoba fizyczna ma prawo dochodzenia od administratora lub podmiotu przetwarzającego odszkodowania za szkodę majątkową lub niemajątkową. To właśnie administrator biorący udział w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym przepisy RODO. Inaczej jest w przypadku podmiotu przetwarzającego. Odpowiada on tylko wtedy, gdy nie dopełnił obowiązków, gdy działał poza zgodnymi z prawem instrukcjami lub działał wbrew tym instrukcjom (art. 82 ust. 2 RODO). W sytuacji gdy administrator lub podmiot przetwarzający udowodnią, że wina za powstanie szkody nie leży po ich stronie, zostają zwolnieni od odpowiedzialności odszkodowawczej. Jednocześnie art. 82 ust. 2 RODO mówi o tym, że osoby, których dane dotyczą nie muszą udowadniać winy, gdyż główny ciężar dowodu przeniesiony został na podmioty przetwarzające. Istnieje też pojęcie odpowiedzialności solidarnej, które obowiązuje wówczas, gdy dochodzi do udowodnienia szkód spowodowanych przetwarzaniem danych przez kilka podmiotów. Tak więc jeśli w tych samych operacjach przetwarzania bierze udział zarówno administrator jaki i podmiot przetwarzający lub więcej niż jeden administrator i kilka podmiotów przetwarzających wówczas ponoszą oni odpowiedzialność solidarną za całą szkodę, a osoba, której dane przetwarzano musi uzyskać rzeczywiste odszkodowanie. Dopuszcza się też roszczenia regresywne pomiędzy podmiotami. W tym wypadku dopuszcza się sytuację, że jeśli odpowiada się solidarnie za szkodę, to podmioty przetwarzające mogą skutecznie dochodzić zwrotu poniesionych kosztów od rzeczywistego winowajcy (podmiotu przetwarzającego).

Jeśli dojdzie do naruszenia bezpieczeństwa zgodnie z przyjętą definicją (art. 4 pkt. 12 RODO) „…prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" to w zakresie nowych obowiązków administratorów danych osobowych leży notyfikacja naruszeń. Do tej pory w istniejących przepisach obowiązek notyfikacji dotyczył tylko wybranych sektorów. Obecnie RODO upowszechnił zasięg notyfikacji i objął nią wszystkich administratorów. Jest to nowością w większości krajów Unii Europejskiej, zaś stosowane było już wcześniej w Irlandii oraz Niemczech. W RODO najważniejszy jest charakter naruszenia bezpieczeństwa oraz jego ewentualne konsekwencje. W momencie naruszenia ochrony danych osobowych administratorzy danych powinni zgłosić je organowi nadzorczemu w terminie 72 godzin po stwierdzeniu naruszenia (art. 33, ust.1 RODO). Kolejnym obowiązkiem administratorów jest zgłoszenie naruszeń osobom, których dane dotyczą. W przypadku, gdy to podmiot przetwarzający stwierdzi naruszenie danych to powinien natychmiast zgłosić, to administratorowi danych. Istnieją jednak pewne ograniczenia co do obowiązku notyfikacji wprowadzone przez RODO. Ograniczenia te dotyczą sytuacji, gdy jest mało prawdopodobne by naruszenia wiązały się z ryzykiem naruszenia praw lub wolności osób fizycznych. Wówczas nie ma obowiązku zgłaszania naruszenia organowi nadzorczemu. Jeśli chodzi o zawiadomienie osoby, której dane dotyczą, to dokonuje się go wtedy, gdy zdarzenie mogłoby doprowadzić do wysokiego ryzyka naruszenia praw i wolności osoby fizyczne. W momencie, gdy administrator danych zastosuje właściwe środki ochrony zarówno organizacyjne jak i techniczne dotyczące incydentu, wówczas nie ma już obowiązku zawiadamiania osób, których dane dotyczyły. Przykładem zastosowania właściwych środków ochrony danych uniemożliwiających osobom nieupoważnionym dostęp jest szyfrowanie. Ograniczenia w obowiązku powiadamiania dotyczą też sytuacji, gdy zawiadomienie wszystkich osób, których dane dotyczą nakładałaby na administratora zbyt duży wysiłek. W tej sytuacji można zastosować publiczny komunikat, który dotrze do zainteresowanych (GIODO 2016).

Nadzór unijny i krajowy

Najważniejszym i głównym elementem europejskiego systemu ochrony danych osobowych są organy nadzorcze. Ich zadania, rola i status zostały dokładnie określone w art. 28 dyrektywy 95/46/WE, w art. 16 Traktatu o funkcjonowaniu UE, a także w orzecznictwie Trybunału sprawiedliwości UE. Organy nadzorcze poszczególnych krajów UE posiadają gwarancję niezależności w ochronie danych osobowych. Aktualnie przepisy RODO wykorzystują dotychczasowe standardy i rozwijają niektóre kompetencje organów nadzorczych. Aby wzmocnić pozycje organów nadzorczych przerzucono na państwa członkowskie obowiązek zapewnienia niezbędnych środków technicznych, organizacyjnych i finansowych. W RODO dąży się też do wyraźnego ujednolicenia i wyeliminowania różnic w kompetencjach krajowych organów danych osobowych. Czerpiąc z istniejących rozwiązań obowiązujących w prawie unijnym RODO wprowadza jednolity katalog zadań i kompetencji organów nadzorczych. Do nowych kompetencji nieznanych dotąd w Polsce w przepisach o ochronie danych osobowych należy kompetencja do nakładania administracyjnych kar finansowych. Organy nadzorcze sprawują też funkcję edukacyjną i doradczą, tak jak dotychczas. Ponadto ustawodawca europejski zwraca uwagę na większą rolę organów nadzorczych w mechanizmach funkcjonowania systemów certyfikacji i samoregulacji. Wśród zadań organów nadzor-

czych jednym z ważniejszych jest upowszechnienie wiedzy oraz podejmowanie działań edukacyjnych wśród najmłodszych a także rozpowszechnianie wśród administratorów wiedzy o spoczywających na nich obowiązkach. W art. 57 RODO są też wytyczne dotyczące takich zadań organów nadzorczych jak rozpatrywanie skarg osób, których dane dotyczą, egzekwowanie przestrzegania przepisów o ochronie danych a także monitorowanie postepowań przy ewentualnych naruszeniach praw. Obecnie RODO kładzie duży nacisk by organy nadzorcze doradzały rządom, parlamentom narodowym i innym instytucjom w dziedzinie aktów prawnych i środków administracyjnych oraz udzielały osobom, których dane dotyczą informacji o prawach im przysługujących. W ostatnim czasie coraz większą uwagę przywiązuje się do współpracy pomiędzy organami nadzorczymi wzajemnej wymiany informacji (GIODO 2016).

Na szczeblu Unii Europejskiej powołano w RODO Europejską Radę Ochrony Danych. Organ przeznaczony jest do działań koordynacyjnych jak i odwoławczych. Ponadto będzie rozstrzygał spory między członkami Unii Europejskiej oraz będzie reprezentować Unię w sporach międzynarodowych. Poza tym będzie nadzorować certyfikacje podmiotów (Zegarek 2016).

W ochronie danych osobowych ważne staje się również stałe monitorowanie rozwoju technologii informacyjno-komunikacyjnych oraz śledzenie zmian mających wpływ na ochronę danych osobowych w innych dziedzinach. Bardzo istotnym wśród zadań organów nadzorczych jest zadanie dotyczące kodeksów postępowania i udzielania certyfikacji oraz prowadzenia wykazów operacji dla oceny skutków ochrony danych. Kolejnym zadaniem organów nadzorczych jest wydawanie dokumentów prawnych umożliwiających przekazywanie danych osobowych do państw trzecich, które nie podlegają RODO. Poza tym jednym z obowiązków organów nadzorczych jest prowadzenie wewnętrznego rejestru naruszeń i działań naprawczych podjętych zgodnie z przepisami. Każdy organ jest także zobowiązany do udostępniania odpowiedniego formularza w formie elektronicznej w celu ułatwienia wnoszenia skargi przez osoby, których dane dotyczą (art. 57, ust. 2 RODO). W wypadku jeśli żądania są nieuzasadnione lub zbyt często powtarzające się, a zatem uznane za nadmierne, ustawodawca europejski dopuszcza odmowę podjęcia żądanych działań oraz pobranie opłaty wynikającej z kosztów administracyjnych w rozsądnej wysokości (art. 57, ust. 4 RODO).

Państwowe organy nadzorcze posiadają uprawnienia doradcze czyli mają prawo do wydawania opinii parlamentom narodowym, rządowi państwa członkowskiego i osobom fizycznym w sprawach dotyczących ochrony danych osobowych oraz do udzielania wskazówek administracyjnych w zakresie wcześniejszych konsultacji. Organy nadzorcze w ramach kompetencji do wydawania zezwoleń mogą wydawać tzw. zezwolenia uprzednie na pewne operacje przetwarzania danych, mogą akredytować podmioty certyfikujące, udzielać certyfikatów i zatwierdzać kryteria certyfikacji. W dobie tzw. transgranicznego przetwarzania danych niezwykle istotnym staje się ujednolicenie w całej Unii Europejskiej zarówno zadań i kompetencji jak i obowiązków organów nadzorczych. Przetwarzanie transgraniczne to takie, które odbywa się w unii w więcej niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego. Organ nadzorczy posiada w sprawach transgranicznych określoną przez RODO jurysdykcję i stosuje właściwe procedury współpracy pomiędzy organami, których sprawa może dotyczyć. Ostatecznie w wypadku konfliktu w przetwarzaniu transgranicznym wiążące decyzje powinna wydawać Europejska Rada Ochrony Danych (RODO 2016).

Krajowa ochrona danych osobowych

W Polsce przygotowanie projektu nowej ustawy o ochronie danych osobowych oraz zmian w przepisach sektorowych leżał w kompetencjach Ministerstwa Cyfryzacji. Projekt z 12 września 2017 r. poddano procedurze uzgodnień i konsultacji. Przyjęta 10 maja Ustawa o ochronie danych osobowych (Dz.U. 2018 poz. 1000) zawiera wyłącznie unormowania, które przepisy unijne wprost przekazują do uregulowania w prawie krajowym lub gdy przepisy unijne pozwalają na swobodę regulacyjną w poszczególnych krajach członkowskich Unii Europejskiej.

Wybrane unormowania ujęte w polskiej ustawie o ochronie danych osobowych:

- określono zakres podmiotowy, przedmiotowy i terytorialny projektowanej ustawy;
- wskazano wiek dziecka – do 13 lat, gdy na przetwarzanie jego danych osobowych w usługach społeczeństwa informacyjnego konieczne będzie uzyskanie zgody rodzica bądź opiekuna prawnego, tym samym projektodawca skorzystał z przewidzianej w art. 8 rozporządzenia 2016/679 możliwości obniżenia wieku dziecka z lat 16;
- uregulowano tryb notyfikacji inspektorów ochrony danych osobowych oraz podmioty obowiązane w polskim porządku prawnym do wyznaczenia inspektora ochrony danych osobowych;
- stworzono nowy krajowy systemu ochrony danych osobowych, na czele z organem nadzorczym, którym według projektodawcy unijnego powinien być Prezes Urzędu Ochrony Danych Osobowych;
- uregulowano język korespondencji: polski i angielski;
- uregulowano zasady certyfikacji oraz tryb postępowania w tych sprawach. W projekcie ustawy zaproponowano, by w polskim systemie prawnym certyfikacji udzielał organ nadzorczy (Prezes Urzędu Ochrony Danych Osobowych);

- uregulowano tryb postępowania w sprawach naruszenia przepisów o ochronie danych osobowych, który znosi dwuinstancyjności postępowania w sprawach naruszenia przepisów o ochronie danych osobowych przyspieszając prowadzone postępowania (wynika to z dotychczasowych wniosków, gdzie postępowania trwały zbyt długo);
- wprowadzono funkcję „inspektora ochrony danych", jako osoby fizycznej wyznaczanej przez administratora bądź podmiot przetwarzający obowiązanej do szeroko rozumianego monitorowania przestrzegania ochrony danych osobowych;
- uregulowano również kwestie dotyczące administracyjnych kar pieniężnych ograniczając wysokość kar finansowych do 100 000 zł dla instytucji państwowych w rozumieniu ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (art. 9 pkt. 1-12 i 14) (Ocena skutków 2017).

Podsumowanie

Nowe przepisy RODO wprowadzają dużo zmian i nowych rozwiązań dla przedsiębiorców i obywateli w zakresie ochrony danych osobowych, w tym wiele innowacyjnych, dostosowanych do współczesnych wymogów. Osobom fizycznym przynoszą zdecydowanie lepszą kontrolę nad swoimi danymi osobowymi oraz dostęp do nich. Jednocześnie zmiany te nie burzą dotychczasowych systemów ochrony danych osobowych tylko je kierunkują na nowoczesne tory w sposób wyważony w czasie. Wprowadzone 27 kwietnia 2016 roku przepisy RODO zaczną obowiązywać 25 maja 2018 roku. Krajom członkowskim Unii Europejskiej pozostawiono więc dość długi czas na to, aby dostosowały własne przepisy krajowe do nowych postanowień unijnych. Tym samy również administratorom danych i podmiotom przetwarzającym dano odpowiedni czas na przygotowanie się do nowych obowiązków, by w konsekwencji zapewnić ochronę danych osobowych zgodnie z nowymi przepisami RODO. Ponadto nie czekając na krajowe uszczegółowienie wielu wątków wprowadzanej ochrony danych osobowych, administratorzy danych na podstawie przepisów i dyrektyw unijnych mogli rozpocząć prace przygotowawcze do realizacji ochrony zgodnie z przepisami RODO. Natomiast w przypadku wątpliwości pierwszeństwo przed ustawodawstwem krajowym mają przepisy RODO.

Literatura:

1. 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, dziennik Urzędowy Wspólnot Europejskich L 281/31 z 23.11.1995.
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 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 uchylającą decyzję ramową Rady 2008/977/WSSiSW, Dziennik Urzędowy Unii Europejskiej L 119 z 4.5.2016.
3. *General Data Protection Regulation (GDPR) requirements, deadlines and facts*, Michael Nadeau, 23/04/2018, Biuletyn CSO, Pobrane z: https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html.
4. *Ocena skutków regulacji do projektu Ustawy o ochronie danych osobowych z 12 września 2017 r.*, Ministerstwo Cyfryzacji. Pobrane z: http://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-ochronie-danych-osobowych.html.
5. *Ochrona danych: Rada zatwierdza podejście ogólne*, Komunikat prasowy 450/15, Rada Unii Europejskiej, Bruksela 15/06/2015. Pobrane z: http://www.consilium.europa.eu/press-releases-pdf/2015/6/40802199180_pl.pdf.
6. *RODO pod lupą. Przewodnik po przepisach rozporządzenia ogólnego o ochronie danych* (2017). Łódź: Wyd. Lubasz & Wspólnicy. Pobrane z: http://rodo.lubasziwspolnicy.pl/pl/.
7. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/697 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 4.5.2016.
8. Ustawa o ochronie danych osobowych, projekt z 12 września 2017 r., Ministerstwo Cyfryzacji. Pobrane z: http://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-ochronie-danych-osobowych.html.
9. Uzasadnienie do projektu Ustawy o ochronie danych osobowych z 12 września 2017 r., Ministerstwo Cyfryzacji. Pobrane z: http://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-ochronie-danych-osobowych.html.
10. *Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych* (2016). Warszawa: wyd. Biuro GIODO. Pobrane z: http://www.giodo.gov.pl/1520282.
11. Zegarek P. (2016). *W końcu finalny tekst Rozporządzenia Ochrony Danych Osobowych!* Pobrane z: http://blog-daneosobowe.pl/koncu-finalny-tekst-rozporzadzenia-ochrony-danych-osobowych/.