Kultura Bezpieczeństwa
Nauka Praktyka Refleksje
Nr 31, 2018 (169–186)
ISSN 2299-4033 DOI: 10.5604/01.3001.0012.8602

ZAKRES I CHARAKTER ZMIAN W SYSTEMACH OCHRONY DANYCH OSOBOWYCH INSTYTUCJI PUBLICZNYCH W ŚWIETLE PRZEPISÓW RODO[1]

SCOPE AND NATURE OF CHANGES IN PERSONAL DATA PROTECTION SYSTEMS OF PUBLIC INSTITUTIONS IN THE LIGHT OF THE PROVISIONS OF THE GDPR (GENERAL DATA PROTECTION REGULATION)

Marek MAZUR
Akademia Pomorska w Słupsku

ABSTRACT:
The EU GDPR Regulation introduced rules and regulations on the protection of individuals with regard to the processing of their personal data regardless of their citizenship or place of residence. The article focuses on issues related directly to the regulation on the protection of personal data and related to documents that regulate the protection of personal data and their processing in public institutions in Poland. The author presents basic estimates about the entry of the GDPR Regulation, indicates the importance of individual Dobies/organisations and entities playing a key role in the protection of personal data on the territory of Poland.

[1] 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, w skrócie RODO).

It describes the documents that establish minimum standards for personal data protection systems to be developed in public institutions to guarantee security. In this article, the author attempted to indicate the scope and nature of changes in personal data systems in the light of the provisions of the GDPR Regulation.

KEYWORDS:
regulation of personal data protection, personal data protection, personal data processing, national interoperability framework, president of the office of personal data protection, personal data controller, data protection policy, information security policy, risk management methodology

ABSTRAKT:
Unijne rozporządzenie RODO wprowadziło zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych niezależnie od obywatelstwa czy miejsca zamieszkania. Artykuł skupia się na zagadnieniach związanych bezpośrednio z rozporządzeniem o ochronie danych osobowych oraz związanych z dokumentami normującymi ochronę danych osobowych i ich przetwarzanie w instytucjach publicznych w Polsce. Autor przedstawia podstawowe zmiany po wejściu rozporządzenia RODO, wskazuje znaczenie poszczególnych organów i podmiotów odgrywających kluczową rolę w ochronie danych na terytorium Polski. Opisuje dokumenty ustanawiające minimalne standardy dla systemów ochrony danych osobowych, które należy opracować w instytucjach publicznych w celu zagwarantowania bezpieczeństwa. W artykule autor podjął się próby wskazania zakresu i charakteru zmian w systemach danych osobowych w świetle wprowadzonych przepisów RODO.

SŁOWA KLUCZE:
rozporządzenie RODO, ochrona danych osobowych, przetwarzanie danych osobowych, Krajowe Ramy Interoperacyjności, prezes Urzędu Ochrony Danych Osobowych, administrator danych osobowych, inspektor danych osobowych, polityka ochrony danych, polityka bezpieczeństwa informacji, metodyka zarządzania ryzykiem

WSTĘP

Integracja społeczna i gospodarcza wynikająca z funkcjonowania rynku wewnętrznego w Unii Europejskiej doprowadziła do znacznego zwiększenia

przepływów danych, w tym w szczególności wymiany danych osobowych pomiędzy podmiotami publicznymi i osobami prywatnymi, zrzeszeniami i przedsiębiorstwami w Unii, jak również wewnątrz poszczególnych państw członkowskich. Prawo Unii często wymaga od organów krajowych państw członkowskich, aby w celu wykonania swoich obowiązków lub w celu realizacji zadań w imieniu organu innego państwa członkowskiego współpracowały ze sobą i wymieniały się danymi osobowymi. Dane osobowe zgodnie z definicją RODO to „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (»osobie, której dane dotyczą«) – możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”[2]. Ponadto do danych osobowych, które umożliwiają zidentyfikowanie konkretnej osoby, zalicza się dane genetyczne, biometryczne oraz dane dotyczące zdrowia.

Z kolei szybki postęp techniczny i globalizacja przynoszą nowe wyzwania w zakresie ochrony naszych danych osobowych. Poziom zbierania i wymiany danych osobowych wzrósł znacząco. Dzięki technologiom zarówno podmioty prywatne, jak i organy publiczne wykorzystują dane osobowe w swojej działalności na wysoką skalę. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Nowoczesne technologie zmieniły gospodarkę, życie społeczne i powinny ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinny zapewniać wysoki stopień ochrony danych osobowych.

W związku z powyższym ochrona danych osobowych stanowi najważniejszy element podczas ich przetwarzania przez konkretne podmioty. Podmioty (oznaczają osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora) muszą zapewniać ochronę danych poprzez odporność sieci lub systemu informacyjnego na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentycz-

[2] Art. 4. ust. 1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., op. cit.

ność, integralność i poufność przechowywanych lub przesyłanych danych osobowych – oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy. Należy skutecznie chronić dane osobowe i być świadomym tego, jak dynamicznym środowiskiem jest w szczególności cyberprzestrzeń i zwiększające się z tym środowiskiem zagrożenia dotyczące „naszych" danych. Aby ochrona danych osobowych była skuteczna, należy wzmocnić i doprecyzować prawa osób, których dane dotyczą, oraz obowiązki podmiotów przetwarzających dane osobowe i decydujących o przetwarzaniu, a także zapewnić uprawnienia w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych. Stąd też przedmiotem rozważań w niniejszym artykule stały się analiza oraz ocena zakresu i charakteru zmian w systemach ochrony danych osobowych w instytucjach publicznych w świetle wprowadzonych przepisów RODO.

ZAKRES I CHARAKTER REGULACJI PRAWNYCH ZAWARTYCH W PRZEPISACH EUROPEJSKICH I POLSKICH

Rozporządzenie RODO to unijne rozporządzenie zawierające przepisy o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych oraz zapewniające swobodny przepływ danych osobowych.

Celem rozporządzenia jest doprowadzenie do pełnej harmonizacji prawa w ramach Unii Europejskiej i swobodnego przepływu danych osobowych. W założeniu rozporządzenie pozwala mieszkańcom Unii Europejskiej na lepszą ochronę ich danych osobowych, a w szczególności zapewnia prawo do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej. Rozporządzenie ujednolica przepisy umożliwiające urzędom państwowym, firmom ograniczanie biurokracji oraz ma na celu zwiększenie zaufania obywateli związanego z przetwarzaniem danych osobowych.

Wprowadzenie RODO umożliwia uszczelnienie dostępu do danych osobowych przez osoby upoważnione do ich przetwarzania oraz wprowadza właściwe procedury, procesy i wskazuje szkolenia dla osób mających dostęp do przetwarzania informacji, w tym danych osobowych, przez osoby odpowiednio wytypowane i przeszkolone. Do chwili obecnej

system ochrony danych osobowych był nieszczelny, co zostało pokazane w Polsce na przykładzie dostępu komorników do bazy danych PESEL[3]. Jak można przeczytać na stronie money.pl: „Użytkownik mógł mieć więcej niż jedną kartę z certyfikatem umożliwiającym dostęp do rejestru PESEL. Ponadto w aplikacji nie dało się zaznaczyć, w jakim celu użytkownik chce zbadać dane. Nie zainstalowano również oprogramowania do analizy zdarzeń dotyczących systemu (logów systemowych). Bez tego nie dało się wyśledzić, kto się loguje i co robi w systemie PESEL. Wymienione luki zauważyli komornicy i korzystali z nich ponad miarę"[4]. Nieprawidłowości w przedstawionym przypadku polegały na tym, że osoby nieupoważnione posiadały dostęp do pozyskiwania danych, mogły je pobierać zdecydowanie więcej i częściej, niż było im to niezbędne do prowadzonych postępowań. Komornicy nie musieli podawać żadnego uzasadnienia, w jakim celu to robią, oraz niezależnie od tego, czy były im potrzebne informacje, czy nie. Kolejnym przykładem, który potwierdza zasadność wprowadzenia RODO, jest stale rosnąca liczba prób cyberataków m.in. na Polskę. Jak można przeczytać w artykule na stronie interia.pl: „Liczba cyberataków skierowanych w stronę Polski w pierwszej połowie 2018 r. była dwukrotnie wyższa niż w tym samym okresie poprzedniego roku. (…) W ciągu ostatniego roku podjęto ponad sześć milionów prób cyberataków na Polskę. (…) Główne źródła zagrożeń w ostatnim roku to Stany Zjednoczone, Francja, Rosja oraz Chiny. (…) systemy wykryły niemal 1,5 miliona prób cyberataków z USA w ciągu ostatniego roku. Sześćdziesiąt proc. incydentów stanowił ruch HTTPS oraz HTTP – oznacza to, że skanowano serwery w poszukiwaniu aplikacji internetowych, których luki można wykorzystać do wykradania danych lub przejęcia kontroli nad konkretnym urządzeniem"[5]. Obecnie trudno wyobrazić sobie funkcjonowanie ludzi bez sieci teleinformatycznych o zasięgu lokalnym bądź globalnym, nowoczesnych technologii oraz programów umożliwiających tworzenie baz danych. Incydenty mogą mieć charakter zamierzony (w przypadku wspomnianych cyberataków) lub stanowić przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych

[3] *PESEL* – Powszechny Elektroniczny System Ewidencji Ludności.

[4] *Sąd: Komornicy wiedzieli o nas więcej niż powinni. I wykorzystywali luki*, online:http://www.money.pl/gospodarka/wiadomosci/artykul/sad-komornicy-wiedzieli-o-nas-wiecej-niz,91,0,2413147.html (dostęp: 16.08.2018).

[5] *700 cyberataków każdej godziny na Polskę*, online: https://interia.pl/news-700-cyberatakow-kazdej-godziny-na-polske,nId,2607174 (dostęp: 16.08.2018).

w celu ochrony informacji. W związku z powyższym szczególnie teraz niezbędne i celowe są regulacje prawne mające na celu ochronę danych osobowych oraz ograniczanie dostępu do nich przez nieuprawnione podmioty i osoby.

Rozporządzenie RODO zostało przyjęte 27 kwietnia 2016 r. i w momencie wejścia w życie w dniu 25 maja 2018 r., po dwuletnim okresie przejściowym, zaczęło obowiązywać w krajach członkowskich Unii Europejskiej bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego. Rozporządzenie dopuszcza jednak doprecyzowanie lub zawężenie jego przepisów przez odrębne prawo państw członkowskich, aby krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie – poprzez włączenie wybranych elementów rozporządzenia do swojego prawa krajowego.

W związku z powyższym 10 maja 2018 r. Sejm RP uchwalił nową ustawę o ochronie danych osobowych[6], która zapewnia stosowanie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 o ochronie danych osobowych. Ustawa weszła w życie 25 maja 2018 r.

ROLA I ZADANIA PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH (W SKRÓCIE PREZES UODO)

Prezes UODO jest organem właściwym do spraw ochrony danych osobowych na terytorium Polski[7], został powołany ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych. Jest przede wszystkim organem nadzorczym w rozumieniu ogólnego rozporządzenia o ochronie danych (RODO)[8]. Prezes UODO jest prawnym kontynuatorem Generalnego Inspektora Ochrony Danych Osobowych[9], zachował jego majątek, wierzytelności oraz przejął wszczęte przez niego postępowania.

Prezes podlega jedynie ustawie i jest powoływany przez sejm na wniosek premiera. Prezes urzędu jako niezależny organ zyskał szereg nowych uprawnień[10]. Może występować z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie bądź zmianę aktów prawnych w sprawach

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

[7] Ibidem, art. 34. ust. 1.

[8] Ibidem, art. 34. ust. 2.

[9] *Generalny Inspektor Ochrony Danych Osobowych* – organ do spraw ochrony danych osobowych w latach 1997–2018, działający na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (w skr. GIODO).

[10] online: https://uodo.gov.pl (dostęp: 15.08.2018).

dotyczących ochrony danych osobowych. Uzyskał także uprawnienie do nakładania kar finansowych bezpośrednio po stwierdzeniu naruszenia przepisów. Zastępcy prezesa są wybierani przez premiera RP po zaopiniowaniu przez ministrów: sprawiedliwości, obrony narodowej i finansów oraz prokuratora generalnego. Posiadanie przez prezesa UODO zastępców jest wynikiem zwiększenia jego kompetencji i nałożonych na niego obowiązków (względem GIODO). Zwiększona została niezależność nowego organu, co można dostrzec po oddelegowaniu nowej kompetencji, jaką jest nadawanie statutu Urzędu Ochrony Danych Osobowych. Dotychczas w formie rozporządzenia statut biura GIODO nadawał prezydent RP wyłącznie w oparciu o zasięgniętą opinię GIODO. Ta zmiana pozwala prezesowi UODO samodzielnie decydować o organizacji urzędu, obszarze działań jego zastępców czy zakresie działań i trybie prac komórek organizacyjnych Urzędu Ochrony Danych Osobowych[11]. W skład Urzędu Ochrony Danych Osobowych, poza prezesem i jego zastępcami, wchodzi także rada do spraw ochrony danych osobowych. Zgodnie z nową ustawą rada stanowi organ opiniodawczo-doradczy. Skład rady mogą tworzyć nie tylko przedstawiciele administracji, ale również osoby reprezentujące różne interesy[12].Główną rolą rady jest wsparcie prezesa UODO w części jego nowych obowiązków. To przede wszystkim opiniowanie projektów dokumentów organów i instytucji Unii Europejskiej dotyczących spraw ochrony danych osobowych czy przekazanych przez prezesa UODO projektów aktów prawnych i innych dokumentów dotyczących spraw ochrony danych osobowych. To także inicjowanie działań związanych z ochroną danych osobowych oraz przedstawianie prezesowi propozycji zmian prawa w tym obszarze. Dodatkowo została wprowadzona certyfikacja realizowana poprzez ustanawianie mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Zgodnie z przepisami zarówno prezes urzędu, jak i przedsiębiorcy są uprawnieni do wydawania certyfikatów. Certyfikacji dokonuje się na podstawie kryteriów określonych przez prezesa urzędu bądź podmiot certyfikujący (w Polsce jest to Polskie Centrum Akredytacji).

[11] Art. 45. ust. 3. ustawy z dnia 10 maja 2018 r.…, op. cit.

[12] Ibidem, art. 48.

ROLA I ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH (W SKRÓCIE ADO)

Funkcja administratora danych została wprowadzona w związku z postanowieniami Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Zgodnie z definicją, administratorem danych była osoba fizyczna lub prawna, władza publiczna, agenda lub inny organ, która samodzielnie lub wspólnie z innymi podmiotami określała cele i sposoby przetwarzania danych[13].

Po wejściu w życie rozporządzenia RODO w maju 2018 r. zmieniona została definicja administratora, a także nałożono na osoby sprawujące tę funkcję nowe obowiązki. Aby przetwarzanie danych osobowych odbywało się zgodnie z rozporządzeniem, do wdrażania odpowiednich środków technicznych i organizacyjnych wyznacza się administratora danych osobowych[14]. W imieniu administratora do przetwarzania danych osobowych wykorzystuje się osoby fizyczne lub prawne, organy publiczne, jednostki lub inne podmioty. Administrator samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Dla podmiotów publicznych cele przetwarzania danych ustala ustawodawca, który aktami prawnymi określa zadania (cele) związane z przetwarzaniem danych osobowych. Administrator określa sposoby osiągnięcia celów poprzez wskazanie m.in. jakie dane są przetwarzane, przez kogo, jak długo, powinien również stosować odpowiednie matematyczne lub statystyczne procedury profilowania. Powinien wdrożyć odpowiednie środki techniczne i organizacyjne mające na celu korektę nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów. Do jego obowiązków należy także zabezpieczenie danych osobowych w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą. Do kompetencji ADO należy określenie celów i strategii ochrony danych osobowych, podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, współpraca z kierownikami podległych komórek organizacyjnych, a w szczególności wyznaczenie inspektora ochrony danych.

---

[13] Art. 2. Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.… op. cit.

[14] Art. 4. pkt 7. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.… op. cit.

ROLA I ZADANIA INSPEKTORA OCHRONY DANYCH (W SKRÓCIE IOD)

Przed wprowadzeniem funkcji inspektora ochrony danych przez administratora danych był powoływany administrator bezpieczeństwa informacji (w skrócie ABI), wprowadzony ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. ABI miał zapewniać przestrzeganie przepisów o ochronie danych osobowych według funkcjonujących przepisów prawa. Osoby, które przed 25 maja 2018 r. pełniły funkcję ABI, automatycznie stały się IOD na okres od 25 maja 2018 r. do 31 sierpnia 2018 r. Po 1 września 2018 r. osoby te nadal mogą pełnić funkcję IOD, o ile administrator danych – zgodnie z art. 10 ust. 1 ustawy o ochronie danych osobowych – zawiadomi o tym prezesa UODO[15].

Ogólne rozporządzenie o ochronie danych w art. 37 ust. 1 RODO przewiduje obowiązek wyznaczenia inspektora dla administratorów i podmiotów przetwarzających wówczas, gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości. Organy i podmioty publiczne, przez które rozumie się jednostki sektora finansów publicznych (np. jednostki samorządu terytorialnego, uczelnie publiczne), instytuty badawcze oraz Narodowy Bank Polski, obowiązane są do wyznaczenia IOD[16].

Zgodnie z art. 37 ust. 5 RODO inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. Poziom wiedzy inspektora powinien być ustalany w kontekście konkretnych potrzeb administratora danych osobowych. Wymagany poziom fachowej wiedzy nie jest nigdzie jednoznacznie określony, ale musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki. Wobec czego inspektor ochrony danych powinien posiadać[17]:

- fachową wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych,

---

[15] *Terminy na wyznaczenie inspektora ochrony danych*, online: https://uodo.gov.pl/pl/138/271 (dostęp: 20.09.2018).

[16] Art. 9. ustawy z dnia 10 maja 2018 r.… op. cit.

[17] *Wyznaczenie Inspektora Ochrony Danych (IOD)*, online: https://uodo.gov.pl/pl/121/192 (dostęp: 17.08.2018).

- fachową wiedzę z zakresu praktyk w dziedzinie ochrony danych osobowych,
- dogłębną znajomość przepisów RODO,
- wiedzę biznesową i sektorową dotycząca działalności administratora,
- odpowiednią wiedzę na temat procesów przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych,
- w przypadku organów i podmiotów publicznych IOD powinien również wykazywać się znajomością procedur administracyjnych i funkcjonowania jednostki.

Inspektor ma odgrywać kluczową rolę w zakresie ochrony danych osobowych oraz pomagać w implementacji niezbędnych elementów rozporządzenia RODO, tj.:

- zasady przetwarzania danych osobowych,
- prawa osób, których dane dotyczą,
- ochrony danych w fazie projektowania oraz domyślnej ochrony danych,
- prowadzenia rejestru czynności przetwarzania,
- wymogów bezpieczeństwa przetwarzania,
- zgłaszania naruszeń.

Zgodnie z art. 37 ust. 6 RODO inspektorem może zostać zarówno pracownik administratora lub podmiotu przetwarzającego, jak i osoba spoza grona pracowników ww. podmiotów (tzw. *outsourcing*).

Każdy użytkownik przed przystąpieniem do przetwarzania danych osobowych musi zostać przeszkolony przez IOD z zakresu:

- przepisów o ochronie danych osobowych oraz przepisów regulujących zasady przetwarzania informacji w tym danych osobowych,
- zasad przetwarzania danych osobowych w konkretnej instytucji,
- procedur realizowanych w systemach informatycznych służących do przetwarzania danych osobowych,
- zasad użytkowania urządzeń i systemów informatycznych do przetwarzania danych osobowych.

OBOWIĄZKI KADR KIEROWNICZYCH I PRACOWNIKÓW INSTYTUCJI PUBLICZNYCH WYNIKAJĄCE Z WPROWADZENIA NOWYCH PRZEPISÓW

W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych (informacji), a w szczególności danych osobowych,

niezbędne jest zaangażowanie ze strony kadr kierowniczych, pracowników i upoważnionych osób zewnętrznych. Przed wprowadzeniem rozporządzenia RODO, ABI zapewniał tylko, że osoby przetwarzające dane osobowe zapoznają się z przepisami o ochronie danych osobowych. Po wprowadzeniu nowych przepisów IOD informuje administratora oraz użytkowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy ogólnego rozporządzenia oraz innych przepisów o ochronie danych i doradza im w tej sprawie. Ponadto IOD monitoruje przestrzeganie ogólnego rozporządzenia, innych przepisów o ochronie danych oraz polityk administratora, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów i na żądanie udziela użytkownikom zaleceń co do oceny skutków ochrony danych oraz nadzoruje ich wykonanie.

Do podstawowych obowiązków kadry kierowniczej i pracowników instytucji publicznych w zakresie ochrony danych osobowych i ich przetwarzania należy:

- wskazanie podstaw prawnych, celu oraz zakresów przetwarzania informacji w tym danych osobowych w komórkach organizacyjnych,
- wnioskowanie do administratora danych osobowych o nadanie upoważnień dla pracowników podległej komórki organizacyjnej,
- zapewnienie przetwarzania informacji, w tym danych osobowych, zgodnie z RODO i KRI (Krajowe Ramy Interoperacyjności[18]), a także z zapisami w dokumentach regulujących zasady przetwarzania informacji, w tym danych osobowych, w instytucji publicznej,
- zachowanie w tajemnicy wiedzy o przetwarzanych informacjach, o sposobach ich zabezpieczenia, aktywach wykorzystywanych do ich przetwarzania przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
- znajomość zasad bezpieczeństwa i bezwzględne przestrzeganie przepisów prawa RODO, KRI oraz pozostałych dokumentów regulujących zasady przetwarzania informacji, w tym danych osobowych.

Każdy użytkownik przed przystąpieniem do przetwarzania danych powinien zostać przeszkolony przez IOD z zakresu:

[18] Ustawa z dnia 5 grudnia 2017 r. – Obwieszczenie Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. 2017 r., poz. 2247.

- przepisów o ochronie danych osobowych, a także Polityki wprowadzonej przez ADO,
- zasad przetwarzania danych osobowych,
- procedur dotyczących bezpiecznego przetwarzania danych osobowych w systemach informatycznych,
- zasad użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych,
- zagrożeń, na jakie może być narażone przetwarzanie informacji, w tym danych osobowych, w szczególności informacji przetwarzanych w systemach informatycznych,
- zasad dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
- procedur postępowania w przypadku naruszenia ochrony informacji, w tym danych osobowych.

DOKUMENTACJA DOTYCZĄCA OCHRONY DANYCH OSOBOWYCH W INSTYTUCJACH PUBLICZNYCH W ŚWIETLE NOWYCH UREGULOWAŃ PRAWNYCH

Administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, wdraża odpowiednie środki techniczne i organizacyjne w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą. Środki te są w razie potrzeby poddawane przeglądom i uaktualnieniom. W związku z powyższym niezbędne jest opracowanie dokumentacji zapewniającej ochronę informacji i danych osobowych oraz wykluczenie naruszenia ochrony danych osobowych. Przed wejściem rozporządzenia RODO w skład wymaganej dokumentacji ABI wchodziła *Polityka bezpieczeństwa*, *Instrukcja zarządzania systemem informatycznym* oraz niezbędny zestaw dokumentów dodatkowych np. pełnomocnictwa, wszelkiego rodzaju oświadczenia itp. Z kolei na dokumentację wynikającą z RODO w instytucjach publicznych składają się następujące dokumenty:

1. Polityka ochrony danych[19] oraz polityka bezpieczeństwa informacji[20]. Dokumenty mają zawierać zestawy efektywnych, udokumento-

[19] Art. 24. ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.… op. cit.

[20] Rozdział I par. 2.15., ustawa z dnia 5 grudnia 2017 r.…, op. cit.

wanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania. Dokumenty ustanawiają minimalne standardy ochrony informacji, w tym danych osobowych, oraz procedury postępowania i działania, które należy stosować, aby właściwie wykonywać obowiązki administratora danych osobowych w zakresie zabezpieczenia danych osobowych. W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko (jak zostało napisane w *Poradniku RODO*: „(…) szacowanie ryzyka ma na celu określenie, co może się zdarzyć – kiedy, gdzie, jak i dlaczego i jak dotkliwe straty mogą powstać”[21]) właściwe dla przetwarzania oraz wdrożyć środki minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej, koszty ich wdrożenia w stosunku do ryzyka i charakteru podlegających ochronie danych osobowych. Stosowane zasady powinny być znane i wykorzystywane przez wszystkie osoby, które biorą udział w procesie przetwarzania danych.

2. Metodyka zarządzania ryzykiem[22] – wspiera zapewnienie adekwatnych oraz skutecznych środków organizacyjnych i technicznych mających na celu minimalizowanie ryzyka naruszenia praw i wolności osób fizycznych, zapewnia ochronę przed nieuprawnionym dostępem do informacji, w tym danych osobowych, i aktywów służących ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i aktywów. W przytoczonym już wcześniej *Poradniku RODO* można znaleźć następującą informację: „Na gruncie RODO nie została wskazana jedna określona metodyka przeprowadzania procesu zarządzania ryzykiem. Obecnie znanych jest wiele metod, z których można czerpać inspirację i dobre przykłady dla tworzenia własnych rozwiązań. Wybór metody powinien odpowiadać specyfice danego podmiotu, uwzględniać zakres i cele przetwarzania oraz rodzaj danych, a także wielkość, strukturę oraz możliwości organizacyjne,

[21] A. Kaczmarek i in., *Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 2*, s. 17, online: https://www.uodo.gov.pl/pl/123/208 (dostęp: 16.08.2018).

[22] Art. 32. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.… op. cit. oraz rozdział IV par. 20.3., ustawa z dnia 5 grudnia 2017 r.…, op. cit.

techniczne i finansowe danej jednostki. (…) Ważne jest, aby wybrana metoda pozwalała na rzetelną i obiektywną ocenę. Administrator lub podmiot przetwarzający, niezależnie od wybranej metody (jednej spośród gotowych lub stworzonej samodzielnie na podstawie kilku dostępnych), powinien jednolicie w całej organizacji stosować zbiór pojęć. (…) Skuteczność przyjętych środków powinna być regularnie monitorowana, zwłaszcza w przypadku większych, bardziej skomplikowanych lub obciążonych większym ryzykiem operacji przetwarzania danych"[23]. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

3. Rejestr czynności przetwarzania danych osobowych[24].
4. Sprawozdanie z analizy ryzyka[25].
5. Wykaz osób upoważnionych do przetwarzania informacji i danych osobowych[26].
6. Rejestr naruszenia ochrony danych osobowych i incydentów naruszenia bezpieczeństwa informacji[27].
7. Ocena skutków dla przetwarzania danych osobowych[28] – dokument obowiązkowy, jeżeli dany rodzaj przetwarzania danych osobowych

[23] A. Kaczmarek i in., *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1*, s. 10–11, online: https://www.uodo.gov.pl/pl/123/208 (dostęp: 14.08.2018).

[24] Art. 30. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.… op. cit.

[25] Art. 32. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.… op. cit. oraz rozdział IV par. 20.3., ustawa z dnia 5 grudnia 2017 r.…, op. cit.

[26] Ibidem, art. 29.

[27] Ibidem, art. 33. ust. 5.

[28] Art. 35. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.… op. cit.

ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

8. Wprowadzone przez administratora i inspektora dokumenty będące uzupełnieniem powyższych dokumentów oraz stanowiące komplet dokumentacji z zakresu bezpieczeństwa informacji, w tym danych osobowych.

PODSUMOWANIE I WNIOSKI

Znaczenie, jakie mają współcześnie dane osobowe, oraz ich przetwarzanie zmuszają do podejmowania coraz to nowych rozwiązań w kwestii zapewnienia im bezpieczeństwa. Wprowadzenie rozporządzenia o ochronie danych osobowych oraz innych dokumentów normujących ochronę danych osobowych i ich przetwarzanie wniosły w życie nowe regulacje określające obowiązki i prawa administratorów i podmiotów przetwarzających dane, czyli zobowiązanych do aktywności w ramach rozporządzenia, w tym szczególne rozszerzenie uprawnień i zadań dla prezesa UODO, ADO oraz IOD. W pewnych przypadkach przyznano dodatkowe uprawnienie ustawodawcy krajowemu do doprecyzowania niektórych związanych z tym aspektów. Ma on bowiem możliwość wyłączenia pewnych przepisów albo modyfikacji niektórych obowiązków. Wśród firm i instytucji, które w jakikolwiek sposób mają do czynienia z danymi osobowymi, narasta świadomość nowych zadań i obowiązków, które nakładają na nie nowe unijne przepisy. Prawo unijne powołało organ do egzekwowania tych przepisów spełniający wymogi rozporządzenia, wprowadza szereg innych regulacji, dotyczących choćby akredytacji czy certyfikacji w celu ustanawiania jakości ochrony danych osobowych i ich przetwarzania. Organ nadzorczy ma prowadzić ewidencję zawiadomień dotyczących IOD. Odmiennie niż to było do momentu wprowadzenia rozporządzenia RODO, to administrator decyduje, bazując na analizie ryzyka, jakiego rodzaju zabezpieczenia, jakie środki techniczne, organizacyjne i prawne będzie musiał wdrożyć, żeby prawidłowo przetwarzać dane osobowe, aby robić to zgodnie z rozporządzeniem i bezpiecznie. Jest to jakościowo bardzo istotna zmiana w stosunku do wcześniejszych przepisów, w których te obowiązki określone były w sposób sztywny. Wprowadzenie rozporządzenia oraz nowych obowiązków i zadań dla podmiotów przetwarzających dane osobowe wymuszają poszukiwanie przez podmioty optymalnych rozwiązań i zmian dotyczących zarówno technicznych i technologicznych

aspektów ochrony, jak i wdrażania nowych procedur i zmian organizacyjnych. Dlatego bieżąca kontrola przez ADO oraz IOD w instytucjach publicznych (i nie tylko) w zakresie funkcjonowania systemu ochrony oraz audyty wdrożonych dokumentów (w szczególności polityki ochrony danych oraz polityki bezpieczeństwa informacji, metodyki zarządzania ryzykiem), postępowanie zgodnie z ustalonymi procedurami, egzekwowanie znajomości nowych przepisów i procedur postępowania przez kadry kierownicze i pracowników są niezbędne, aby zapewnić bezpieczeństwo przetwarzanych danych osobowych. Cykliczny przegląd procedur bezpieczeństwa jest bardzo ważny ze względu na ilość i jakość danych w nich gromadzonych. Wskazane osoby (podmioty) muszą stale dokonywać oceny ryzyka, jakie wiąże się z prowadzeniem przetwarzania danych osobowych, i wdrażać adekwatne środki bezpieczeństwa. To nie może być jednorazowa ocena, ale ciągły proces mający na celu zminimalizowanie i wyeliminowanie przez podmioty przetwarzające naruszeń ochrony danych osobowych. Podsumowując, wprowadzenie rozporządzenia RODO ma na celu stworzenie systemu ochrony danych osobowych jako bardziej uporządkowanego, bardziej elastycznego niż ten, który funkcjonował wcześniej, podlegającego stałej ewaluacji i jednolitego w całej Unii Europejskiej. Wprowadzenie nowego zakresu i charakteru zmian dokonywanych w systemach ochrony danych osobowych w instytucjach publicznych w świetle wprowadzonych przepisów RODO należy zatem traktować jako zalety tego prawa mające na celu większą ochronę danych osobowych i ich przetwarzanie oraz, co ważne, trzeba pamiętać, że są dostosowane do aktualnej sytuacji w aspekcie postępującej globalizacji, wzrostu postępu technicznego i zagrożeń związanych z przetwarzaniem danych osobowych.

Należy zauważyć, iż powyższy artykuł nie wyczerpuje do końca tematu, którego merytoryczny zakres skupia się na zmianach w systemach ochrony danych osobowych po wprowadzeniu rozporządzenia RODO. Jest jedynie wstępem do szerszej debaty na ten temat, a przede wszystkim podjęcia dalszych, szczegółowych badań.

BIBLIOGRAFIA:

LITERATURA:

1. Kaczmarek A. i in., *Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1*, online: https://www.uodo.gov.pl/pl/123/208 (dostęp: 14.08.2018).

2. Kaczmarek A. i in., *Jak stosować podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 2*, online: https://www.uodo.gov.pl/pl/123/208 (dostęp: 16.08.2018).

AKTY PRAWNE:

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.
2. 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).
3. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2018 r., poz. 1000.
4. Ustawa z dnia 5 grudnia 2017 r. – Obwieszczenie Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. 2017 r., poz. 2247.

ŹRÓDŁA INTERNETOWE:

1. https://uodo.gov.pl (dostęp: 20.09.2018).
2. *Sąd: Komornicy wiedzieli o nas więcej niż powinni. I wykorzystywali luki*, online: http://www.money.pl/gospodarka/wiadomosci/artykul/sad-komornicy-wiedzieli-o-nas-wiecej-niz,91,0,2413147.html (dostęp: 16.08.2018).
3. *Terminy na wyznaczenie inspektora ochrony danych*, online: https://uodo.gov.pl/pl/138/271 (dostęp: 20.09.2018).
4. *Wyznaczenie Inspektora Ochrony Danych (IOD)*, online: https://uodo.gov.pl/pl/121/192 (dostęp: 17.08.2018).
5. *700 cyberataków każdej godziny na Polskę*, online: https://interia.pl/news-700-cyberatakow-kazdej-godziny-na-polske,nId,2607174 (dostęp: 16.08.2018).

MGR INŻ. MAREK MAZUR – ukończył studia pierwszego stopnia w Wyższej Oficerskiej Szkole Radiotechnicznej w Jeleniej Górze oraz na Politechnice

Wrocławskiej na kierunku elektronika i telekomunikacja. Jest absolwentem studiów drugiego stopnia na kierunku elektronika i telekomunikacja na Politechnice Szczecińskiej w Szczecinie oraz studiów podyplomowych na kierunku zarządzanie i dowodzenie na Akademii Marynarki Wojennej w Gdyni. Jego zainteresowania naukowe skupiają się wokół problematyki bezpieczeństwa wewnętrznego oraz zarządzania. Obecnie jest wykładowcą na Wydziale Nauk o Zarządzaniu i Bezpieczeństwie Akademii Pomorskiej w Słupsku.

CITE THIS ARTICLE AS:
M. Mazur, *Zakres i charakter zmian w systemach ochrony danych osobowych instytucji publicznych w świetle przepisów RODO*, „Kultura Bezpieczeństwa Nauka Praktyka Refleksje", 2018, nr 31, p. 169–186, DOI: 10.5604/01.3001.0012.8602.