Dominika Skoczylas

Obowiązki organów administracji publicznej w zakresie przetwarzania danych w systemach zinformatyzowanych przed i po wejściu w życie RODO i nowelizacji ustawy o ochronie danych osobowych

Celem artykułu jest wskazanie konsekwencji prawnych w zakresie dotyczącym zapewnienia bezpieczeństwa przetwarzania danych osobowych w systemach zinformatyzowanych. Ustawodawca wyznaczył administratorom danych osobowych, konkretne obowiązki w kwestii ustalenia odpowiednich środków organizacyjnych, osobowych, rzeczowych i technicznych, które mają uniemożliwić posługiwanie się danymi osobowymi przez nieuprawnione podmioty w nielegalnym celu. Od maja 2018 r. obowiązuje Rozporządzenie Parlamentu Europejskiego i Rady 2016/679 o ochronie danych osobowych. Wprowadza nowe regulacje prawne np. ustanawia inspektora ochrony danych. Pierwsza część artykułu wskazuje zadania administratorów danych polegające na użyciu środków zabezpieczających dane osobowe w systemach zinformatyzowanych, przed wejściem w życie RODO i ustawy z 10.5.2018 r. o ochronie danych osobowych. W drugiej zawarto najważniejsze zmiany odnoszące się do administratorów danych osobowych, określone w RODO i ustawie o ochronie danych osobowych. Metody badawcze obejmują komparatystyczną analizę podstawowych tekstów aktów prawnych z wykorzystaniem literatury przedmiotu (zastosowano metodę porównawczo-prawną).

1. Zagadnienia wstępne

Postęp technologiczny i zjawisko globalizacji w wyraźny sposób wpływają zarówno na kwestie gospodarcze jak i społeczne, a przede wszystkim na zmiany w zakresie ustawodawstwa. Obecnie, coraz częściej korzysta się z technologii informacyjnej jako elementu wykonywania zadań publicznych przez organy władzy publicznej. Wskazuje się na tzw. informatyzację administracji publicznej, czyli świadczenia usług w ramach e-administracji. Zdarzeniu temu sprzyja rozbudowa infrastruktury telekomunikacyjnej, a także kompatybilność sieci i urządzeń. Aby jednak zapewnić pełną skuteczność realizacji celów publicznych, należy wprowadzić a później wykorzystać odpowiednie środki

organizacyjne, rzeczowe i techniczne, nie zapominając o zasobach personalnych. Jednocześnie trzeba ustalić jednolite standardy bezpieczeństwa sieciowego, za pomocą których będzie możliwa elektroniczna weryfikacja danych, ich udostępnianie, zmiana oraz archiwizowanie w systemach zinformatyzowanych[1].

Określenie zasad dotyczących przetwarzania informacji w sieci, związane jest z zapotrzebowaniami społeczeństwa informacyjnego. Podmioty te zorientowane są głównie na przekazywanie, pobieranie i wykorzystywanie informacji. Zaletą zatem będzie powszechna dostępność, tzn. brak ograniczeń ze względu na czas, miejsce czy osobę oraz minimalizacja kosztów i szybkość świadczenia usług za pomocą urządzeń telekomunikacji elektronicznej[2]. Bez cienia wątpliwości, wartością dodaną jest również ekonomiczny aspekt informatyzacji, zapewniający z jednej strony opłacalność, z drugiej produktywność czy efektywność systemu. Organy posługujące się systemami elektronicznymi muszą zwrócić uwagę na bezpieczeństwo przetwarzania danych oraz na wymagania interoperacyjności, czyli zdolność systemów i serwerów do wymiany i wzajemnego wykorzystywania informacji. Ponadto używanie urządzeń komunikacji elektronicznej zapewnia błyskawiczny kontakt pomiędzy organem a podmiotem korzystającym z usług administracji.

Niezaprzeczalnym jest to, że odpowiedzialność za bezpieczeństwo przetwarzania informacji takich jak dane osobowe spoczywa na organach administracji publicznej, innych niż one podmiotach publicznych a także na podmiotach realizujących zadania publiczne. Przepisy prawa przyznają im szczególną rolę ze względu na opisywany w literaturze przedmiotu charakter władczy administracji publicznej (imperium). Oznacza ono podejmowanie działań w sposób jednostronny a jednocześnie prawnie wiążący wobec określonej strony stosunku administracyjno-prawnego, na mocy ustawowo przyznanych kompetencji. Władztwo to wyznacza dominującą pozycję organu, zarazem dokonując hierarchicznego podporządkowania podmiotu wobec działania administracji[3]. Oczywiście władztwo, wynika z legitymacji demokratycznej do wydawania określonych poleceń czy aktów, wobec podmiotów podporządkowanych. Istotne znaczenie, ma zatem w tym przypadku, zasada legalności oraz praworządności, w myśl których czynności podejmowane przez administrację muszą opierać na prawie i mieścić w jego granicach. Zdaniem doktryny, legalność dotyczy realizacji konkretnych zadań, zgodnie z powszechnie

1 A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Warszawa 2008, s. 44 i n.
2 K. Celarek, *Prawo informacyjne. Problem badawczy teorii prawa administracyjnego,* Warszawa 2013, s. 42 i n.
3 J. Bukowska, Z. Cieślak, W. Federczyk, M. Klimaszewski, B. Majchrzak, [w:] *Nauka administracji*, red. Z. Cieślak, wyd. 1, Warszawa 2012, s. 103.

obowiązującym prawem, natomiast praworządność działania odnosi się do realizacji idei demokratycznego państwa prawnego.[4]. Należałoby takie stanowisko uznać za prawidłowe, docelowo jednak każda władza ma swojego suwerena, a więc przede wszystkim, w ramach przyznanych jej kompetencji, powinna uwzględniać postulat użyteczności publicznej (celu, interesu społecznego).

Ponadto działania administracji czy jednostek administrujących polegają na wykonaniu zadań publicznych (celu publicznego). Ów cel czy interes publiczny jest umiejscowiony w kategorii dobra wspólnego. Rola organów administracji polega na wydawaniu określonych aktów prawnych, a także świadczenia usług na rzecz społeczeństwa, w znaczeniu szerokim, tj. ogólnym. De facto interes ogólny, mający wysoce zobiektywizowany charakter ma zastosowanie co do poszczególnych, indywidualnych przypadków[5].

Zadania podmiotów odpowiedzialnych gwarantują zapewnienie bezpieczeństwa sieciowego, związanego z informatyzacją zadań publicznych (cyberbezpieczeństwo), a zarazem chronią przed cyberterroryzmem. Definicją tego zjawiska jest atak lub groźba ewentualnego ataku na komputery, systemy i sieci informacyjne, którego celem ma być ograniczenie dostępu do internetowych baz danych lub całkowity jego brak. Podłożem działania, może być wymuszenie spełnienia określonych żądań ekonomicznych, politycznych czy innego rodzaju[6]. Dlatego tak ważna staje się rola organów administracji publicznej jako gwarantów bezpieczeństwa sieciowego, w tak istotnej materii, którą są dane osobowe.

Analizując zagadnienie obowiązków organów administracji publicznej w zakresie cyberbezpieczeństwa przetwarzania danych osobowych w systemach zinformatyzowanych należy wskazać, że jest to materia wielopłaszczyznowa. Warto zwrócić uwagę zarówno na podstawowe zasady dokonywania jakichkolwiek operacji na danych osobowych, zadania administratorów oraz standardy jakościowe ich pracy, mając na uwadze przepisy prawa polskiego jak i międzynarodowego (w szczególności unijnego).

Artykuł obejmuje charakterystykę zmian w zakresie ochrony danych osobowych, polegającą na porównaniu regulacji prawnych obowiązujących dotychczas i tych, które

4 M. Krawczyk, *Podstawy władztwa administracyjnego*, Warszawa 2016, s. 136 i n., s. 140 i n.
5 Z. Duniewska, *Cel publiczny, interes publiczny i dobro wspólne* [w:] *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie*, red. M. Stahl, wyd. 5, Warszawa 2013, s. 76 i n.
6 K. Liedel, P. Piasecka, *Jak przetrwać w dobie zagrożeń terrorystycznych. Elementy edukacji antyterrorystycznej,* Warszawa 2008, s. 40.

wynikają z RODO oraz ustawy z 10.5.2018 r. o ochronie danych osobowych[7]. Zamiarem Autorki jest wskazanie czy reforma ochrony danych osobowych była niezbędna i jakie skutki prawne wywoła, zarówno z punktu widzenia osoby, której dane dotyczą, użytkowników danych jak i samych administratorów, którymi najczęściej są organy publiczne.

Pierwsza część pracy koncentruje się na materii zadań administratorów danych podejmowanych w celu zapewnienia bezpieczeństwa systemów zinformatyzowanych, przed reformą ochrony danych osobowych w Polsce. Druga dotyczy zakresu zmian obowiązków administratorów i inspektora ochrony danych na gruncie Rozporządzenia o Ochronie Danych Osobowych, które obowiązuje w krajowym porządku prawnym od 25.5.2018 r, a także tych wynikających z nowej ustawy o ochronie danych osobowych.

2. Obowiązki ogólne administratora danych osobowych a bezpieczeństwo ich przetwarzania w systemach zinformatyzowanych na gruncie ustawy z 29.8.1997 r. o ochronie danych osobowych

Źródłem prawa do ochrony danych osobowych są przepisy Konstytucji Rzeczypospolitej Polskiej[8]. W art. 51 Konstytucji określono nieskrępowany dostęp do dotyczących jednostki dokumentów i zbiorów danych, żądanie sprostowania i usunięcia informacji, które są niezgodne z prawdą, niepełne lub zebrane w nielegalny sposób. Co więcej, wskazano także obowiązek spoczywający na organach władzy publicznej polegający na przetwarzaniu danych jedynie w niezbędnym zakresie (zgodnie z zasadą demokratycznego państwa prawnego). Rozważania na temat ochrony danych osobowych przez administratorów, uległy istotnej zmianie w momencie pojawienia się w 2018 r. nowej ustawy o ochronie danych osobowych i ogólnego rozporządzenia o ochronie danych osobowych. Warto jednak odwołać się do regulacji prawnych zawartych w poprzednio obowiązującym akcie prawnym. W art. 7 pkt 2 uchylonej ustawy o ochronie danych osobowych,[9] przetwarzaniem określono dokonywanie różnego typu operacji wykonywanych na danych osobowych, głównie w systemach informatycznych, poczynając od ich zbierania, przechowywania poprzez opracowywanie czy udostępnianie aż po całkowite usuwanie.

7 Ustawa z 10.5.2018 r. o ochronie danych osobowych, Dz. U. poz. 1000. W ramach harmonizacji prawa unijnego z prawem krajowym, polski ustawodawca ustanowił ramy prawne ochrony danych osobowych, tworząc nową ustawę o ochronie danych osobowych.
8 Konstytucja Rzeczpospolitej Polskiej z 2.4.1997 r., Dz. U. Nr 78, poz. 483, ze zm., dalej: Konstytucja.
9 Ustawa z 29.8.1997 r. o ochronie danych osobowych, Dz. U. z 2018 r. poz. 138, akt uchylony.

Dane osobowe już wówczas podlegały wyjątkowej ochronie, gdy należały do katalogu danych szczególnych (sensytywnych, wrażliwych), np. dane dotyczące zdrowia. Co do zasady, ich przetwarzanie było niemożliwe bez wyraźnej, pisemnej zgody podmiotu, ponadto istniały również inne przypadki, gdy ich udostępnienie miało miejsce ze względu na zaistniałe okoliczności (np. w celach medycznych, dochodzenia praw przed sądem czy prowadzenia badań naukowych)[10]. Uchylona ustawa z 1997 r., znała już pojęcie przetwarzania danych w systemach informatycznych. Niektóre pojęcia (które mają zastosowanie również co do nowych regulacji prawnych), doprecyzowane zostały przez inne ustawy. Systemem informatycznym nazywa się niezmiennie współpracę pomiędzy urządzeniami czy nośnikami a właściwymi oprogramowaniami, która umożliwia bezpośrednią transmisję danych[11]. Prawidłowe działanie sieci przesyłowych również aktualnie, związane z wykorzystywaniem środków komunikacji elektronicznej, poprzez udostępnianie danych w wyniku porozumiewania się stron na odległość[12].

Kompetencje administratorów danych, wynikające z poprzednio obowiązującej ustawy o ochronie danych osobowych, to co do zasady, zadania stricte decyzyjne, odwołujące się do wiedzy tych podmiotów, z zakresu zastosowania odpowiednich środków zabezpieczających dane osobowe w sieci. Za podmiot odpowiedzialny uważano, zarówno organ państwowy lub samorządowy, ale także inne podmioty publiczne lub niepubliczne realizujące zadania publiczne. Ponadto status administratora przysługiwał osobom fizycznym, prawnym i jednostkom organizacyjnym, które dokonywały operacji na danych osobowych, związanych z prowadzoną przez nie działalnością zarobkową, zawodową czy statutową. Podstawowy warunek dotyczył korzystania ze środków zapobiegających niewłaściwym działaniom wykonywanych na danych osobowych, legalnych na terytorium Rzeczypospolitej Polskiej[13].

Przed zmianami w 2018 r., główne obowiązki administratorów danych osobowych można było podzielić na trzy grupy, mianowicie na zadania: informacyjne, rejestracyjne i zabezpieczające. W przypadku tych pierwszych, chodziło o przekazanie informacji o celu i sposobie zbierania danych, znanych lub potencjalnych odbiorcach, prawie dostępu do ich treści, z możliwością weryfikacji, tj. sprostowania, uzupełnienia, żądania usunięcia oraz dobrowolności lub obowiązku podania danych administratorowi[14]. Odnośnie do kwestii

10 A. Krasuski, *Dane osobowe w obrocie tradycyjnym i elektronicznym. Praktyczne problemy*, wyd.1, Warszawa 2012, s. 83.
11 Artykuł 3 pkt 3 ustawy z 17.2.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. z 2017 r. poz. 570.
12 Artykuł 2 pkt 5 ustawy z 18.7.2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. z 2017 r. poz. 1219.
13 Artykuł 7 pkt 4 w zw. z art. 3a ust. 1 ustawy z 29.8.1997 r. o ochronie danych osobowych, akt uchylony.
14 K. Celarek, *Prawo* …, s. 266.

rejestracyjnych, administratora określano gwarantem prowadzenia zbiorów danych osobowych w kompleksowy sposób, w których treści obejmowała informacje o podmiocie, który je przetwarza, celu, opisie kategorii osób, których dane dotyczą i odbiorców tych informacji oraz środki zabezpieczające[15]. Co do zasady, zadania te nie uległy większej zmianie w nowo wprowadzonych przepisach.

Zagrożenia w materii bezpieczeństwa przetwarzania danych stanowiły impuls do wzmocnienia pozycji administratora jako strażnika ustanawiającego kwestie przestrzegania standardów związanych z wykorzystywaniem informacji w wyniku użycia środków komunikacji elektronicznej. Koncepcja elektronicznej administracji, uwarunkowana zmianami w środowisku technologicznym, społecznym i gospodarczym, była podstawowym elementem, który miał wpływ na wdrożenie odpowiednich środków zabezpieczających dane osobowe w sieci. E-administracja miała (i ma) zastosowanie do rozwoju świadczenia usług drogą elektroniczną (e-usługi), wzmacnianiu roli społeczeństwa obywatelskiego (technologia IT jako podstawa e-demokracji) oraz do e-zarządzania, czyli stymulowania procesów administracyjnych przez organy, za pomocą urządzeń telekomunikacji elektronicznej[16].

Podstawy tej ochrony, zostały uwzględnione na gruncie ustawy o ochronie danych osobowych z 1997 r. Aktualnie, również i dzisiaj, potwierdzenie doktrynalne i praktyczne, znajduje fakt, że oprócz tego, że operacje takie jak opracowywanie czy udostępnianie danych mają pozostawać w zgodzie z zasadą legalizmu, adekwatności i celowości. W odniesieniu do podstawowych zasad, wymieniony wyżej akt wskazywał, że dane powinny być przechowywane w czasie, w którym korzystanie z nich uznaje się za niezbędne. Poprzednio obowiązująca ustawa podkreślała, że administrator danych musi liczyć się z tym, że w momencie, w którym wystąpią wątpliwości uzasadniające powstanie nieprawidłowości, w zakresie chociażby zmiany czy archiwizowania informacji, musi zastosować odpowiednio dobrane do zaistniałej sytuacji środki organizacyjne czy techniczne. Zabiegi te miały ustrzec przed udostępnieniem bądź zabraniem danych przez podmioty nieupoważnione oraz zmianą, utratą, uszkodzeniem a nawet zniszczeniem.[17]

Regulacje prawne z 1997 r. wyznaczyły również inne istotne aspekty pracy administratora, takie jak:

15 Artykuł 41 ust. 1 ustawy z 29.8.1997 r. o ochronie danych osobowych., akt uchylony.
16 K. Jastrzębska, *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych*, wyd. I, Warszawa 2018, s. 47.
17 M. Ganczar, *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009, s. 176 i n.

a) prowadzenie dokumentacji, w której znajduje się opis warunków ochrony przetwarzania danych osobowych, w tym specyfikacja użytych środków zabezpieczających (technicznych i organizacyjnych);
b) upoważnienia właściwych osób do pomocy przy przetwarzaniu danych, umożliwiające im dostęp i stałą weryfikację danych;
c) kontrola nad tym, kiedy i przez kogo informacje zostały wprowadzone do systemu i komu je przekazano.

Nie bez znaczenia również, według poprzednio obowiązującego stanu prawnego, było to, że środki techniczne i organizacyjne miały czynić zadość postulatom integralności i poufności danych. Walorem regulacji prawnych w przedmiotowym aspekcie, stała się rozliczalność pracy administratorów, gdyż wykonując zadania ochronne, uwierzytelniali dokonane przez siebie zmiany, jednoznacznie wskazujące na osobę, która zastosowała dane rozwiązanie[18]. Postulat rozliczalności zadań ciążących na administratorze danych stanowi jedną z podstawowych zasad wynikających z RODO i mających swoje odzwierciedlenie w nowej ustawie o ochronie danych osobowych. Nie ulega zatem wątpliwości, że na administratorach od dawna ciąży niemały obowiązek czuwania nad bezpieczeństwem przetwarzania danych osobowych i jest to zadanie wielowątkowe. Jednakże swoboda przepływu osób, towarów i usług, w tym otwarcie na rynki zagraniczne, wymusiła harmonizację przepisów prawa, w celu skutecznej i jednolitej ochrony danych osobowych, wszystkich członków Unii Europejskiej.

3. Zasady ochrony danych osobowych wynikające z Rozporządzenia o Ochronie Danych Osobowych i ustawy z 10.5.2018 r. o ochronie danych osobowych a szczególna pozycja administratora danych

Rzeczpospolita Polska, będąc członkiem Unii Europejskiej, odpowiedzialna jest za implementację aktów prawa unijnego na swoim terytorium. Propozycja zwiększenia i poprawy skuteczności ochrony danych osobowych w krajach członkowskich była przyczyną powstania Rozporządzenia o Ochronie Danych Osobowych[19], które w Polsce obowiązuje od 25.5.2018 r. Podstawowe zadania w zakresie ich ochrony zostały mocą przepisów,

18 J. Janowski, *Administracja elektroniczna. Kształtowanie się informatycznego prawa administracyjnego i elektronicznego postępowania administracyjnego w Polsce*, Warszawa 2009, s. 146 i n.
19 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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, Dz.Urz.UE.L Nr 119/1, dalej: RODO.

nałożone na administratora danych osobowych (administratora). Zgodnie z obowiązującymi przepisami, administratorem może być zarówno osoba fizyczna, prawna jak i organ publiczny czy inna jednostka lub podmiot, która może samodzielnie lub we współpracy z innymi określić cel i sposób przetwarzania danych. Akcentowana, w omawianym przypadku jest pozycja tzw. współadministratorów danych, kiedy to co najmniej dwa podmioty mają prawo przetwarzać dane osobowe. W takiej sytuacji są oni zobligowani do uzgodnienia zakresu swoich obowiązków i ustalenia podziału zadań, za których wykonanie będzie odpowiedzialny każdy z nich - indywidualnie[20].

Standardy posługiwania się danymi osobowymi obejmują przede wszystkim ich przetwarzanie zgodnie z prawem, przy czym jakiekolwiek operacje na nich mają być wykonywane w sposób rzetelny i jasny dla osoby, do której one należą. Kolejno, muszą być zbierane i archiwizowane w konkretnych, wyraźnych celach, adekwatnie (stosownie) do osiągnięcia uzasadnionych w określonej sytuacji efektów (ograniczenie celu i minimalizacja danych). Ponadto administrator jest gwarantem prawidłowości, uaktualniania i prostowania danych, a także gromadzenia ich w formie zapewniającej identyfikację osoby, przez czas nie dłuższy niż jest to niezbędne. Bardzo szerokie uprawnienia przyznano administratorowi w kwestii zabezpieczenia danych w systemach zinformatyzowanych. Przede wszystkim pełnią oni funkcję ochronną przed niedozwolonym, niezgodnym z prawem m.in udostępnianiem danych osobowych, a także przed ich zniszczeniem, utratą czy uszkodzeniem, posługując się właściwymi środkami technicznymi i organizacyjnymi. Zadania te są ukierunkowane na integralność i poufność zachowania danych[21].

Szczególną pozycję administratora daje się zauważyć na przykładzie podjęcia działań związanych z tzw. prawem do bycia zapomnianym, czyli żądania usunięcia danych. Na wniosek osoby, której dane bezpośrednio dotyczą, administrator ma obowiązek usunąć je z systemu bez zbędnej zwłoki np. w przypadku, w którym dane nie są już niezbędne do celów, dla których je zebrano, osoba cofnęła zgodę na ich udostępnianie, czy wniosła sprzeciw co do sposobu ich przetwarzania[22].

Z treści rozporządzenia wynika szereg obowiązków nałożonych na administratorów, w szczególności informacyjnych i rejestracyjnych. Jednakże, w związku z dokonywaniem operacji na danych osobowych w systemach zinformatyzowanych, najczęściej komentowanym

20 A. Krasuski, *Ochrona danych osobowych na podstawie RODO,* wyd. 2, Warszawa 2018, s. 134 i n.
21 Artykuł 5 RODO.
22 http://samorzad.infor.pl/sektor/organizacja/rodo-2018/760958, Prawo-do-bycia-zapomnianym-juz-od-25-maja-2018-r.html (dostęp: 13.4.2018 r.).

zagadnieniem jest materia zapewnienia bezpieczeństwa informacji w sieci. Być może jest to związane ze zmianą, a raczej rozszerzeniem definicji danych osobowych. Oprócz informacji o zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, którą można bezpośrednio lub pośrednio zidentyfikować np. na podstawie imienia, nazwiska czy numeru identyfikacyjnego, danymi osobowymi są również identyfikatory internetowe (np. takie jak adresy IP, identyfikatory plików cookie itp.)[23]. Zostawianie śladów w sieci może bowiem skutkować tym, że serwery porównując dane wyszukiwane przez jednostkę, umożliwią ich bezpośrednią lub pośrednią identyfikację.

Ustalono, że administrator będzie podmiotem odpowiedzialnym za wdrożenie środków technicznych i organizacyjnych, zabezpieczając dane głównie przy pomocy ich pseudonimizacji i szyfrowania. Pojęcie pseudonimizacji oznacza takie przetworzenie danych, na podstawie którego nie można ich przypisać do konkretnej osoby fizycznej, korzystając jedynie z prostego wyszukiwania informacji. Należy odwołać się do danych dodatkowych przechowywanych osobno i odpowiednio zabezpieczonych przed podmiotami trzecimi, właściwymi środkami technicznymi i organizacyjnymi[24].

Ponadto, administrator podejmie działania gwarantujące zachowanie poufności, integralności, dostępności oraz odporności systemów i usług przetwarzania czy szybkie i właściwe reagowanie w sytuacji, gdy dostęp do nich zostanie ograniczony wskutek fizycznego postępowania czy nieprawidłowości natury technicznej. Wskazano, że czynności kontrolne i zabezpieczające powinny polegać również na regularnym testowaniu, sprawdzaniu, wykonywaniu pomiarów i ocenianiu efektywności środków przeznaczonych do zapewnienia bezpieczeństwa zarówno integralności danych, jak i ich prawidłowemu przetwarzaniu w systemach teleinformatycznych[25]. Co należy podkreślić, rozporządzenie nie wyznacza konkretnych środków zabezpieczających, a jedynie podaje cele, jakie ma osiągnąć administrator, wykonując obowiązki zabezpieczające. Zastosowanie takich czy innych metod zależy bowiem od ilości i jakości możliwości, które posiada, rodzaju danych podlegających ochronie oraz od stopnia zagrożenia prawidłowości ich przetwarzania. Zagadnienie bezpieczeństwa obejmuje nie tylko przygotowanie sieci i systemów teleinformatycznych do obrony przed utratą, uszkodzeniem czy nieuprawnionym wykorzystywaniem, ale również

23 D. Lubasz, *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi,* Warszawa 2018, s. 20 i n.
24 Artykuł 4, pkt 5 RODO.
25 P. Litiwński, *Przewodnik po RODO dla adwokatów*, Kraków 2018, s. 19.

samych urządzeń (nośników danych), pomieszczeń i osób, które będą na co dzień zarządzać danymi osobowymi.

Nie można także pominąć bardzo ważnej kwestii, jaką jest rejestrowanie czynności przetwarzania danych osobowych. Poprawnie prowadzona dokumentacja odnosi się do zasady rozliczalności administratora z realizacji powierzonych obowiązków. Czynności, w stosunku do których zastosowano środków techniczne i organizacyjne, muszą być odpowiednio rejestrowane, po to aby organ nadzorczy mógł ocenić sposób przetwarzania danych. Rejestr ten zawiera wiele informacji istotnych z punktu widzenia zarówno osoby, której dane dotyczą, jak i organów nadzorujących zadania administratorów. Znajdują się w nim: informacje o administratorze, współadministratorach i inspektorze ochrony danych, wskazany jest cel przetwarzania, kategorie danych i osób, których one dotyczą, a także odbiorców danych, informacje o przekazaniu danych do państwa trzeciego czy organizacji międzynarodowej, termin usunięcia danych i ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. Adresatem obowiązku jest każdy administrator (bądź podmiot przetwarzający dane w imieniu administratora)[26].

Każdorazowo naruszenie ochrony danych podlega zgłoszeniu. I tak, administrator jest zobowiązany poinformować, bez zbędnej zwłoki, nie później niż do 72 godzin po stwierdzeniu naruszenia (z drobnymi wyjątkami) np. o zgubieniu nośnika zawierającego dane osobowe. RODO, doprecyzowuje również minimalną treść takiego zgłoszenia, które musi zawierać: opis naruszenia ochrony danych osobowych (kategorię danych, liczbę osób, których dane dotyczą), dane kontaktowe inspektora ochrony danych, wskazanie konsekwencji naruszenia ochrony danych, a także środki które mogą być użyte (lub zostały) w celu zminimalizowania negatywnych skutków zaistniałej sytuacji[27].

Warto nadmienić, że rozporządzenie o ochronie danych osobowych, wprowadziło nowego uczestnika o znaczącej pozycji faktycznej i prawnej, a mianowicie inspektora ochrony danych, do którego można przypisać funkcje odnoszące się do monitoringu, współpracy i udzielania stosownych zaleceń. Inspektor uczestniczy w realizacji zadań dopiero po wyznaczeniu go przez administratora i podmiot przetwarzający, gdy jakichkolwiek operacje na danych osobowych są dokonywane przez: organy lub podmioty publiczne z wyłączeniem spraw, którymi zajmuje się wymiar sprawiedliwości, osoby, instytucje czy organy,

26 D. Lubasz, *Rejestrowanie czynności przetwarzania,* [w:] *RODO, ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 661 i n.
27 W. Chomiczewski, *Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu,* [w:] *RODO, ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 714 i n.

których głównym przedmiotem postępowania jest działalność polegająca na systematycznym i regularnym monitorowaniu podmiotów na dużą skalę, lub gdy przetwarzają tzw. dane szczególnie chronione oraz informacje dotyczące wyroków skazujących i naruszeń prawa (rozległy zakres)[28]. Zadania te są zatem zorientowane na współpracę pomiędzy inspektorem, administratorem oraz przetwarzającym dane w celu poprawy skuteczności i efektywności ochrony i zabezpieczenia informacji, w szczególności w kwestii nadzoru i informacji. Uwaga inspektora powinna być skupiona na charakterze, zakresie, kontekście i celu operacji wykonywanych na danych osobowych, z uwzględnieniem ryzyka wystąpienia jakichkolwiek zagrożeń zarówno o podłożu wewnętrznym jak i zewnętrznym. Inspektor ochrony danych jawi się zatem jako następca administratora bezpieczeństwa informacji, występującego na gruncie przepisów uchylonej ustawy o ochronie danych osobowych.

Z kolei w ustawie z 10.5.2018 r. o ochronie danych osobowych scharakteryzowano procedurę ustanowienia Inspektora Ochrony Danych. Podmiot, który wyznaczył inspektora, musi powiadomić Prezesa Urzędu Ochrony Danych Osobowych o jego wskazaniu w terminie 14 dni od wskazania (podając imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora oraz inne niezbędne dane identyfikujące podmiot). Każdorazowo zmiana danych dotyczących inspektora czy informacja o jego odwołaniu powinna zostać przekazana w terminie 14 dni od dnia zaistnienia określonej sytuacji faktycznej[29].

Nie ulega wątpliwości, że do wejścia w życie ustawy z 10.5.2018 r. o ochronie danych osobowych, to Generalny Inspektor Ochrony Danych Osobowych (GIODO) pełnił główną rolę w zakresie kontroli przetwarzania danych osobowych, wydawał decyzje administracyjne i rozpatrywał skargi, prowadząc przy tym rejestry zbiorów danych, a także był ciałem doradczym, opiniodawczym oraz inicjatorem projektów w zakresie przedsięwzięć związanych z ochroną danych (miał wpływ na kształt przepisów krajowych oraz współpracował z organizacjami i instytucjami międzynarodowym)[30].

Obecnie organem właściwym w sprawie ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych. Pełni rolę organu nadzorującego zadania obejmujące ochronę danych osobowych, a także podejmuje współpracę międzynarodową, dokonuje certyfikacji w zakresie ochrony danych, wspomaga działania edukacyjne i informacyjne, jest organem opiniującym akty prawne o tematyce ochrony danych, a także prowadzi postępowania

28 M. Mędrala-Natkaniec, *Jakie zmiany w zakresie ochrony danych osobowych pracowników wprowadza RODO*, Warszawa 2018, s. 12.
29 Artykuł 10 ustawy z 10.5.2018 r. o ochronie danych osobowych.
30 Artykuł 12 ustawy z 29.8.1997 r. o ochronie danych osobowych, akt uchylony.

w przypadku naruszania ich ochrony[31]. Na mocy ustawy, organem opiniodawczo-doradczym Prezesa Urzędy, jest Rada do Spraw Ochrony Danych Osobowych, która m.in. wydaje opinie do projektów dokumentów organów unijnych, odnośnie ochrony danych osobowych czy innych projektów aktów przekazanych przez samego Prezesa Urzędu[32]. Warto nadmienić, że Prezes Urzędu, podobnie jak wcześniej GIODO, może przez upoważnionych pracowników dokonywać kontroli przestrzegania ochrony danych osobowych, a także nakładać w drodze decyzji, administracyjne kary pieniężne.

Wprowadzenie RODO i nowej ustawy o ochronie danych osobowych jest niezwykle ciekawe, zwłaszcza ze względu na ustalenie zasad wzajemnej współpracy pomiędzy inspektorami ochrony danych osobowych a administratorami. Kompetencje tych podmiotów są rozłączne, jednak jednocześnie w wielu aspektach połączone (równoważne) mają przysłużyć się skuteczności realizacji zadań w zakresie bezpieczeństwa danych osobowych, uwzględniając bardzo kompleksową regulację przepisów prawa unijnego, implementowaną do prawodawstwa krajowego. Przedstawiciele doktryny wskazują, że kompleksowe i jednoznaczne ujęcie tematyki ochrony danych osobowych we wszystkich krajach Unii Europejskiej nie jest w pełni możliwe. Wynika to z problemu relacji w zakresie kompetencji unijnych i poszczególnych państw. W szczególności komplikacje mogą pojawić się w przypadku określenia zakresu naruszenia ochrony danych osobowych i sankcji nałożonych na podmioty, które przetwarzają dane na zewnątrz[33] (np. do państw trzecich).

4. Podsumowanie

Konkludując, obowiązki organów administracji publicznej, a także innych podmiotów realizujących zadania publiczne w zakresie przetwarzania danych osobowych w systemach zinformatyzowanych są niezwykle istotne, a to ze względu na zagrożenia związane z ich umiejscowieniem w sieci. Dokładne określenie zadań administratorów wynika ze zintegrowania usług o szczególnym znaczeniu dla społeczeństwa, w ramach e-administracji. Utworzenie odpowiednich standardów funkcjonowania e-administracji przy zastosowaniu właściwych środków organizacyjnych, rzeczowych oraz osobowych i ich późniejsze

31 https://www.poradyodo.pl/relacje-z-giodo/prezes-uodo-nowy-organ-ochrony-danych-osobowych-8266.html (dostęp: 26.7.2018 r.).
32 Artykuł 48 ustawy z 10.5.2018 r. o ochronie danych osobowych.
33 M. Niedźwiedź, M. Tarnawa-Zajączkowska, *RODO - może jednak nie dla wszystkich? Problem zakresu zastosowania unijnej regulacji w praktyce*, [w:] *CASUS*, red. K. Sieniawska, Kraków 2018, nr 89, s. 58.

zastosowanie, stanowi reakcję na zagrożenia występujące w przypadku chociażby nieprawidłowości udostępniania czy przechowywania danych.

Realizacja zadań publicznych w omawianej materii, polega przede wszystkim na zapewnieniu bezpieczeństwa danych w systemach zinformatyzowanych. Rozporządzenie o ochronie danych osobowych wskazuje na elementy mające priorytetowe znaczenie, takie jak: zbieranie informacji ze względu na wyraźny i konkretny cel, który jest niezbędny do osiągnięcia wymaganych rezultatów, gwarancje przetwarzania zgodnie z prawem, przez czas nie dłuższy niż to potrzebne oraz na integralność i poufność zachowania danych. Oprócz szeregu obowiązków informacyjnych i rejestracyjnych, spoczywających na administratorze, ogromną uwagę zwrócono na kwestie bezpieczeństwa. W tym obszarze najważniejsze jest wprowadzenie zasad pseudonimizacji i szyfrowania danych, a także badanie systemów i usług przetwarzania oraz zapobieganie czy niwelowanie skutków ich niewłaściwego działania. Należy zaznaczyć jednak, że przepisy rozporządzenia wyznaczają jedynie ramy ogólne, umożliwiając administratorowi użycie takich środków, jakie uzna on za stosowne w danej sytuacji, przyznając mu pomoc w postaci inspektora ochrony danych.

Dodatkowym czynnikiem ugruntowującym założenia unijnego rozporządzenia jest nowa ustawa z 10.5.2018 r. o ochronie danych osobowych. Z jej treści wynikają m.in. podstawowe zadania Prezesa Urzędu Ochrony Danych Osobowych czy procedura wyznaczenia Inspektora Ochrony Danych. Najważniejsze kwestie, jak dokonywanie certyfikacji, postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych, czy czynności kontrolne, a także procedura nałożenia kar pieniężnych, zostały w ustawie opisane w sposób na tyle transparentny, aby umożliwić ich pojęcie przez każdego użytkownika czy administratora danych.

Zasadność wcielenia założeń prawodawstwa unijnego i nowej ustawy będzie można ocenić dopiero po dłuższym zastosowaniu regulacji prawnych i w stosunku do konkretnych przypadków. Jednakże już dzisiaj wiadomo, że to na administratorach, którymi są najczęściej organy administracji publicznej, spoczywa obowiązek wdrożenia i zastosowania zasad ustawy i rozporządzenia, zapewnienia bezpieczeństwa, dobrej jakości oraz elektronicznej weryfikacji informacji w systemach teleinformatycznych. Efektem podejmowanych działań będzie kompleksowe i skuteczne realizowanie zadań korzystnych dla większości społeczeństwa.

Responsibilities of public administration bodies in the field of data processing in IT systems before and after the entry into force of the GDPR and amendment of the Act on the Protection of Personal Data

Summary:

The aim of this article is to point out the legal consequences in terms of ensuring the security of personal data processing in IT systems. The legislator appointed personal data administrators specific duties on the question of setting organizational, personal, material and technical adequate means which they have to make it impossible to use personal details by unauthorized entities for them in the illegal destination. From May 2018 General Data Protection Regulation of the European Parliament and of the Council 2016/679 applies. It introduces new legal regulations, e.g. establish a data protection officer. The first part of the paper shows the tasks of data administrators consisting in the use of personal data security measures in IT systems, before the entry into force of the GDPR and the Act of 10 May 2018 on the Protection of Personal Data. The second contains the most important changes referring to the personal data administrators, specified in the GDPR and the Act on the Protection of Personal Data. Research methods contain basic legal acts together with publications in the field (comparative-legal method was used).

Dominika Skoczylas

Absolwentka Wydziału Prawa i Administracji Uniwersytetu Szczecińskiego, asystentka w Katedrze Prawa i Postępowania Administracyjnego US. Główne zainteresowania: prawo administracyjne, prawo komunikacji elektronicznej, prawo gospodarcze.