Dr hab. Paweł Romaniuk, prof. UWM
Wydział Prawa i Administracji
Uniwersytet Warmińsko-Mazurski w Olsztynie
ORCID: 0000-0002-7217-956X
pawel.romaniuk@uwm.edu.pl

WARUNKI BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH W ADMINISTRACJI PUBLICZNEJ

Streszczenie

W przedmiotowym artykule zwrócono uwagę na szczególną rolę informacji i danych osobowych w systemie zarządzania bezpieczeństwem. Znaczenie informacji, w tym przypadku także i mechanizmów ochrony danych osobowych, wymaga ujęcia systemowego. Dlatego też wskazane zostaną strategiczne obszary i zasady systemem zarządzania bezpieczeństwem informacji w administracji publicznej. Obowiązujące przepisy prawa, regulujące założenia dopuszczalności przetwarzania i ochrony danych osobowych w systemach teleinformatycznych, wyznaczają również odpowiednie poziomy ochrony takich informacji. W warunkach zabezpieczenia danych osobowych, w każdej organizacji publicznej, przetwarzającej i chroniącej takie dane, funkcjonuje administrator danych osobowych, który może wyznaczyć administratora bezpieczeństwa informacji do realizacji takich zadań. W tekście przybliżone zostaną wybrane, z uwagi na złożony charakter poruszanego zagadnienia, te obszary, które wdrażane są przez organy administracji publicznej w obszarze ochrony danych osobowych.

Słowa kluczowe: administracja publiczna, bezpieczeństwo, ochrona, dane osobowe, RODO**.**

WSTĘP

Problematyka dotycząca szeroko rozumianego bezpieczeństwa informacji, nie jest nowym zagadnieniem. Można jednak dostrzec, że próby związane z

przyjmowaniem systemowej standaryzacji polityk bezpieczeństwa informacji, rozpoczęły się tak na poważnie pod koniec ubiegłego tysiąclecia. W praktyce funkcjonowania każdego państwa, kompletna dbałość o bezpieczeństwo informacji, jej skala i zakres zagadnień, powstających w wyniku nieuwzględniania ryzyka utraty strategicznych i prawnie chronionych informacji, nie może zostać niezauważona przez zarządzających informacjami publicznymi. Bezpieczeństwo informacji stało się sferą, która systematycznie zyskuje na znaczeniu. Jest to spowodowane faktem, że wzrasta nieuchronnie i naturalnie liczba danych, które przetwarzane są w różnych w systemach informatycznych. Pojawiają się i głosy, że era praktycznego rozwoju społeczeństwa informacyjnego pojawiła się w obecnym XXI w.[1] Trzeba przy tym zauważyć, że istnieją podmioty, które niestety próbują zarabiać na informacji w sposób nieuczciwy, a przy tym obserwuje się systematyczny wzrost i nieustanny rozwój cyberprzestępczości[2]. Jest to spowodowane faktem, że działania przestępców przenoszą się do Internetu, gdzie widoczne stają się ich nowe działania. Aktywność ta charakteryzuje się coraz większą pomysłowością, czego przykładem mogą być różnego rodzaju cyberprzestępstw typu phishing[3].

Jednakże niezwykle ważne w procesie prawidłowo chronionej informacji, jest ochrona danych osobowych. Administracja publiczna, w tym w szczególności jednostki samorządu terytorialnego, odgrywają niezwykle ważną rolę w procesie ochrony danych osobowych. Uwarunkowane jest to w dużej mierze specyfiką zadań, jakie realizowane są na rzecz osób fizycznych. Z uwagi również na rozbudowane struktury organizacyjne organów administracji publicznej, dużym wyzwaniem nieustannie staje się właściwe przygotowanie funkcjonariuszy publicznych do obowiązków, związanych z prawidłowym zabezpieczaniem i ochroną danych osobowych. Dlatego zgodnie z przyjętą tezą, przegląd celów potwierdza konieczność wzmacniania bezpieczeństwa i

[1] Por. G. Nowacki, Znaczenie informacji w obszarze bezpieczeństwa narodowego, „Nierówności Społeczne a Wzrost Gospodarczy", 2013, nr 36, s. 107-108.
[2] Por. M. Karpiuk, The Local Government's Position in the Polish Cybersecurity System, „Lex Localis - Journal of Local Self-Government", 2021, nr 3, s. 610-615.
[3] Patrz szerzej: Ł. Wojciechowski, Działania typu phishing jako zagrożenie cyberbezpieczeństwa obywateli Rzeczypospolitej Polskiej [w:] W trosce o bezpieczne jutro. Reminiscencje i zamierzenia, S. Niedzwiecki, N. Starik (red.), Wydawnictwo Wyższej Szkoły Bezpieczeństwa w Poznaniu, Poznań 2017, s. 399-401.

należytej ochrony danych osobowych w niezakłóconym funkcjonowaniu administracji publicznej. W artykule wykorzystano metodę dogmatyczno-prawną, której celem była przede wszystkim analiza przepisów normatywnych oraz odniesienie się do wybranej literatury przedmiotu.

WARUNKI KSZTAŁTOWANIA SYSTEMU OCHRONY DANYCH OSOBOWYCH

Na wstępie należy zaznaczyć, że działania administracji publicznej czy jednostek administrujących, w dużej mierze skupione są na realizacji zadań, traktowanych równocześnie jako sposób osiągania celów publicznych. Przywołany cel usytuowany jest w kategorii dobra i interesu wspólnego[4]. Obowiązkiem organów administracji publicznej jest wydawanie różnego rodzaju aktów prawnych, przy jednoczesnym świadczeniu usług publicznych na rzecz mieszkańców, gdzie interes ogólny przyjmuje niezależny charakter i ma wymierne wykorzystanie w indywidualnych przypadkach, także dotyczących ochrony praw jednostki, w tym ochrony danych osobowych[5].

Głównym źródłem prawa w obszarze ochrony danych osobowych są regulacje Konstytucji Rzeczypospolitej Polskiej. W art. 51 ust. 1 Konstytucji RP określono, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji, dotyczących jego osoby[6]. Przepis ten zapewnia możliwość wyodrębnienia trzech kluczowych wymiarów prawa prywatności, tj. prawa do decydowania o swojej cielesności; prawa do prywatności (autonomii) informacyjnej oraz prawa do prywatności lokalnej (autonomicznego stwierdzenia relacji i zachowań w np. w rodzinie, domu czy społeczności)[7]. Ponadto ustawa zasadnicza wyznacza, że władze publiczne nie

[4] Patrz szerzej: M. Czuryk, Bezpieczeństwo jako dobro wspólne, „Zeszyty Naukowe KUL", 2018, nr 3, s. 15.
[5] Por. Z. Duniewska, Cel publiczny, interes publiczny i dobro wspólne [w:] Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie, M. Stahl (red.), Wolters Kluwer, Warszawa 2013, s. 76-78.
[6] Patrz art. 51 ust. 1 Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483, ze zm.), zwana dalej Konstytucją RP.
[7] Patrz więcej: A. Młynarska-Sobaczewska, Trzy wymiary prywatności. Sfera prywatna i publiczna we współczesnym prawie i teorii społecznej, „Przegląd Prawa Konstytucyjnego" 2013, Nr 1(13), s. 35-36.

mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach, niż te, niezbędne w demokratycznym państwie prawnym a przy tym każdy obywatel ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych oraz ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą[8].

Kilka lat temu, w 2016 r. - zostały uchwalone przepisy unijne o ochronie danych osobowych, zwane jako RODO, którego wejście w życie w krajach Unii Europejskiej zaplanowano na dzień 25 maja 2018 r. [9]. Było to spowodowane faktem, że Unia chciała dać dwuletni czas na dostosowanie krajów członkowskich do nowych wymagań, związanych z przetwarzaniem danych osobowych. Nadrzędnym celem tej regulacji stało się wyznaczenie podstaw a także zasad przetwarzania i ochrony danych osobowych we wszystkich krajach Unii. Rozporządzenie to zastąpiło obowiązującą w Polsce od 1997 r. ustawę o ochronie danych osobowych, która była pierwotnym aktem normatywnym, wyznaczającym właśnie polskie normy, zasady przetwarzania i ochrony danych osobowych. W tamtym okresie dane osobowe już były objęte szczególną ochroną. Było to spowodowane faktem, że należały one do zbioru danych wrażliwych i prawnie chronionych (np. informacje dotyczące zdrowia pacjenta)[10]. Przywołane przetwarzanie danych było niemożliwe bez pisemnej i wyraźnej zgody podmiotu, który te dane posiadał. Obecne były również inne okoliczności udostępnienia takich danych. Przykładem może być pojawienie się warunków w zakresie dochodzenia praw przed sądem czy prowadzenia badań naukowych[11].

Wdrożenie RODO było spowodowane potrzebą uregulowania zasad przetwarzania danych osobowych, wynikających z szybkiego postępu

[8] Art. 51 ust. 2-4 Konstytucji RP.
[9] Rozporządzenia 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) (Dz. Urz. UE L 119 z 04.05.2016), zwana dalej rozporządzeniem 2016/679.
[10] D. 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, „Młody Jurysta", 2019 Nr 1, s. 43-44.
[11] Patrz A. Krasuski, Dane osobowe w obrocie tradycyjnym i elektronicznym. Praktyczne problemy, Wolters Kluwer, Warszawa 2012, s. 83-84.

technicznego i globalizacji, które niosło również za sobą obecność nowych zagrożeń. Osoby fizyczne coraz częściej zaczęły przy tym udostępniać swoje dane. Wzrastająca przy tym liczba przetwarzanych danych osobowych i rozwój technologiczny, przyczyniły się do zmian w gospodarce i życiu społecznym. Tego rodzaju zmienne uwarunkowania, w dalszym ciągu powinny sprzyjać swobodnemu przepływowi danych osobowych w całej Unii Europejskiej i bezpiecznemu ich przekazywaniu państwom trzecim, gdzie nieustannie powinien być zagwarantowany wysoki stopień ochrony danych osobowych[12]. Przy czym, zarówno podmioty prywatne, jak i organizacje publiczne, wykorzystujące w swojej codziennej pracy dane osobowe, muszą posiadać właściwie zabezpieczony mechanizm ochrony danych osobowych. Musi być on z jednej strony oparty nie tylko na założeniach RODO, ale również powinien uwzględniać, w ramach przyjętej ochrony, zastosowanie nowoczesnych technologii informacyjno-komunikacyjnych, wzmacniających zastosowanie przyjmowanych a następnie wdrażanych rozwiązań technicznych[13].

Kształtując instrumenty prawidłowo funkcjonującej administracji publicznej, należy zwracać szczególną uwagę na zasady tworzenia polityki bezpieczeństwa ochrony danych osobowych. Polityka ta powinna zawierać m.in.:

- definicje ogólnych i konkretnych obowiązków w systemie zarządzania bezpieczeństwem informacji, w tym reakcji na pojawiające się incydenty dotyczące naruszenia bezpieczeństwa informacji;
- mechanizmy zapewniające współużytkowanie informacji;
- strukturę wyznaczania celów wdrażania zabezpieczeń, w tym struktury szacowania, identyfikowania oraz zarządzania ryzykiem.
- szczegółowe polityki bezpieczeństwa i procedury, związane z systemami informatycznymi;
- warunki przestrzegania zasad bezpieczeństwa[14].

[12] Por. T. Banyś, J. Łuczak, Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych, Wydawnictwo Presscom, Wrocław 2017, s. 43-61.
[13] Por. M. Kawecki, Główne cele ogólnego rozporządzenia o ochronie danych osobowych, [w:] M. M. Kawecki, T. Osiej (red.), Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia, C.H. Beck, Warszawa 2017, s. 20-23.
[14] W. R. Wiewiórowski, Prywatność pacjenta musi być chroniona, „IT w Administracji", Nr 2/2013, s. 10-12.

Odpowiedzialnymi za realizację polityki bezpieczeństwa ochrony danych osobowych są administratorzy, natomiast za zadania z zakresu opracowywania i realizację konkretnych działań odpowiadają zarówno administratorzy, jak i ich użytkownicy[15]. Wszelkie dane osobowe w podmiotach administracji publicznej są gromadzone, przechowywane, edytowane, archiwizowane w różnorodnych kartotekach, skorowidzach, księgach, czy wykazach, zarówno na dokumentach papierowych, jak również rejestrowane są w systemach informatycznych na elektronicznych nośnikach informacji[16]. Należy przy tym zgodzić się założeniem, że prawo ochrony danych osobowych realizuje pięć funkcji, tj. ochronną, kontrolną, regulacyjną, edukacyjną oraz prewencyjną[17]. Pierwsza funkcja dotyczy ochrony słusznych interesów osób fizycznych w związku z przetwarzaniem ich danych osobowych. Druga polega na umiejętnym i prawidłowym kontrolowaniu przez właściwe organy administracji publicznej procesu przetwarzania danych osobowych. Trzecia funkcja polega na objęciu regulacją prawną stosunków społecznych w zakresie przetwarzania danych osobowych. Wskazuje ona również na zapewnienie minimalnych standardów przetwarzania takich danych wraz z gwarancją zapewnienia im odpowiedniej ochrony. Czwarta funkcja skierowana jest na popularyzację i rozpowszechnienie koncepcji ochrony danych osobowych oraz zwiększanie świadomości społecznej na temat wagi ochrony danych osobowych. Ostatnia, piąta funkcja, zmierza do zapobieganie niezgodnemu z obowiązującym prawem przetwarzaniu danych osobowych[18].

WYBRANE MECHANIZMY ZASTOSOWANIA ŚRODKÓW OCHRONY DANYCH OSOBOWYCH

[15] J. Bajorek, Ochrona i bezpieczeństwo danych osobowych w organizacji, „De Securitate et Defensione.
O Bezpieczeństwie i Obronności", Nr 1 (2) 2016, s. 41.
[16] Por. L. Kępa, Ochrona danych osobowych w praktyce, C. H. Beck, Warszawa 2011, s. 101-109.
[17] J. Behr, Wyodrębnianie się prawa ochrony danych osobowy [w:] Środki prawne ochrony danych osobowych, M. Błażewski, J. Behr (red.), Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2016, s. 25.
[18] Patrz: T. Banyś, Funkcje prawa ochrony danych osobowych, [w:] Prawo ochrony danych osobowych, T. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak (red.), Difin, Warszawa 2016, s. 21-22.

Osoby zarządzające podmiotami administracji publicznej, otrzymały niezwykle ważne zadania w zakresie przygotowania swoich jednostek do przyjęcia proceduralnego i wdrażania RODO. Tego typu obowiązki wiązały się z dostosowywaniem swoich instytucji do przyjęcia nowych regulacji prawnych w obszarze obowiązywania zasad ochrony danych osobowych. Można wspomnieć o kilku ważnych działaniach, do których należało m.in.:
- odpowiednie przygotowanie pracowników urzędów do nowych wymogów prawnych;
- przygotowanie systemów informatycznych do prawidłowego i bezpiecznego przetwarzania danych osobowych;
- weryfikacja obowiązującej infrastruktury technicznej i organizacyjnej w zakresie ograniczenia jednoczesnej liczby petentów przebywających przy jednym stanowisku pracy;
- dokonanie przeglądu i inwentaryzacji dokumentów pod kątem ochrony danych wraz z anonimizacją danych osobowych[19].

W związku z wprowadzeniem do polskich instytucji publicznych zasad w zakresie funkcjonowania RODO, ważnym obszarem działania stał się proces ujednolicenia formularzy i innych elementów dokumentacji wraz z całą procedurą zapewniającą właściwą ochronę danych osobowych wszystkich petentów. Dużą w tym rolę odegrał art. 5 RODO, gdzie dane osobowe muszą być m.in. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Muszą być również zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami a także muszą być wykorzystywane w adekwatny i uzasadniony sposób oraz ograniczone do tego, co jest niezbędne do celów, w których są przetwarzane. Ponadto dane osobowe powinny być prawdziwe i w razie potrzeby konieczności ich zmiany, należy podjąć wszelkie rozsądne działania, aby dane osobowe, które zawierają nieaktualne lub nieprawdziwe informacje, w świetle celów ich przetwarzania, zostały niezwłocznie sprostowane lub usunięte. Wiąże się z tym również odpowiednie

[19] Por. Ł. Wojciechowski, Bezpieczeństwo informacji w polskim samorządzie terytorialnym na tle procesu ujednolicania systemu ochrony danych osobowych w Unii Europejskiej, „Rocznik Administracji Publicznej", Nr 5, 2019, s. 206.

przechowywane takich danych, w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane[20]. Tego typu polityka staje się równocześnie tzw. egzemplifikacją ochrony proaktywnej (ang. *privacy by design*), która swoje odzwierciedlenia ma w art. 25 RODO[21]. Przywołane określenie jest wdrażane w odniesieniu do ochrony danych osobowych już na etapie projektowania konkretnych działań w tych zakresie[22].

Projektując model ochrony danych osobowych, zwracając przy tym uwagę na ważną rolę, jaką ma pełnić odpowiedni poziom bezpieczeństwa takich informacji, instytucje publiczne zastosowały proste mechanizmy proceduralne, dotyczące np. namalowania na podłodze w urzędzie linii, określające odległość oczekiwania na załatwienie sprawy pomiędzy poszczególnymi osobami. Później pojawiły się nowatorskie rozwiązania, dotyczące wprowadzenia, co stało się już obecnie powszechną praktyką, elektronicznego systemu kolejkowego. Za pomocą takich prostych metod, petenci załatwiają swoją sprawę w uzgodnionym czasie powodując, że zmniejsza się realne ryzyko, że usłyszą dane osobowe innej osoby. Proces ten bywa niejednokrotnie monitorowany, aby przepisy z zakresu ochrony danych osobowych faktycznie były wdrażane i przestrzegane[23]. Nie można również zapominać, że jedną z ważniejszych zmian, jakie wprowadził nowy system ochrony danych osobowych w państwach członkowskich Unii Europejskiej,

[20] Szczegółowo zasady dotyczące przetwarzania danych osobowych reguluje: art. 5 ust. 1 RODO.

[21] W odniesieniu do przywołanego art. 25 RODO należy mieć na względzie, że uwzględniając 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, administrator, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń. Ponadto administrator jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania, gdzie obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

[22] Dla przykładu ciekawą propozycję w planowaniu działań przedstawia: E. Everson, Privacy by Design: Taking CTRL of Big Data, „Cleveland State Law Review", 2017, Vol. 65, Iss. 1, s. 27-28.

[23] Por. M. Mędrala-Natkaniec, Jakie zmiany w zakresie ochrony danych osobowych pracowników wprowadza RODO, PWN, Warszawa 2018, s. 12-13.

stał się prawny obowiązek wyodrębnienia stanowiska inspektora ochrony danych we wszystkich organach administracji publicznej. Osoba taka zastąpiła wcześniej funkcjonującego w instytucjach publicznych administratora bezpieczeństwa informacji[24].

Uwzględniając powyższe argumenty, trzeba zaznaczyć, że wprowadzenie nawet najlepszych zabezpieczeń, nie daje całkowitej pewności co do ochrony danych osobowych. Coraz bogatsze doświadczenie podmiotów publicznych, wykorzystujących nawet elementy kontroli zarządczej, wyznaczającej możliwość np. wdrożenia analizy ryzyka, nie zawsze dostarcza zapewnienia, że wszystkie obszary, w tym sfera ochrony danych osobowych, są należycie zabezpieczone[25]. Stąd w ramach ujednolicenia mechanizmów należytej ochrony danych osobowych w państwach członkowskich Unii Europejskiej, pojawił się obowiązek raportowania i reagowania na naruszenia, którym z różnych względów nie udało się właściwie zareagować i zapobiec konsekwencjom ich zmaterializowania się. Zatem każdy podmiot administracji publicznej, który zajmuje się przetwarzaniem danych osobowych, ma prawny obowiązek poinformowania o naruszeniu bezpieczeństwa danych osobowych do właściwej instytucji w swoim kraju, odpowiadającym za ochronę danych osobowych. W Polsce rolę takiego organu pełni Urząd Ochrony Danych Osobowych.

W związku z obowiązkiem właściwej reakcji na tego typu naruszenia, należy zastosować kilka rozwiązań prawnych. Zgodnie z art. 44 ustawy ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem różnych nieprawidłowości, to właśnie na administratorów, przetwarzających dane osobowe, w związku z zapobieganiem

[24] Patrz: Ł. Wojciechowski, Rola administratorów bezpieczeństwa informacji w kształtowaniu bezpieczeństwa informacyjnego w Rzeczypospolitej Polskiej [w:] Społeczno-prawne problemy bezpieczeństwa wewnętrznego III Rzeczypospolitej. Wybrane Zagadnienia, M. Gąska (red.), Wydawnictwo Naukowe Innovatio Press, Lublin 2017, s. 123-124.

[25] Proceduralną ochronę w zakresie kontroli zarządczej zapewnia art. 68 ust. 1-2 ustawy z dnia 27 sierpnia 2009 r. o ustawie finansów (t.j. Dz. U. z 2024 r. poz. 1530 ze zm.), gdzie kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy, zaś celem kontroli zarządczej jest zapewnienie w szczególności: 1) zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi; 2) skuteczności i efektywności działania; 3) wiarygodności sprawozdań; 4) ochrony zasobów; 5) przestrzegania i promowania zasad etycznego postępowania;6) efektywności i skuteczności przepływu informacji; 7) zarządzania ryzykiem.

i zwalczaniem przestępczości - nałożono taki sam obowiązek, jak na administratorów w trybie art. 33 ust. 1 rozporządzenia 2016/679[26]. Identyczne obowiązki pojawiają się w zakresie terminu zawiadomienia naruszenia, gdzie w sytuacji naruszenia ochrony danych osobowych, administrator, bez zbędnej zwłoki, nie później jednak niż w ciągu 72 godzin po stwierdzeniu naruszenia, zgłasza naruszenie Prezesowi Urzędu Ochrony Danych Osobowych (Prezes Urzędu)[27]. W przypadku niedotrzymania wskazanego terminu, administrator niezwłocznie zgłasza naruszenie oraz sporządza i przekazuje Prezesowi Urzędu uzasadnienie niedotrzymania tego terminu, zaś podmiot przetwarzający, po stwierdzeniu naruszenia ochrony danych osobowych, jest zobowiązany do przekazania takich danych administratorowi, bez zbędnej zwłoki, nie później jednak niż w ciągu 48 godzin[28]. Trzeba także odnieść się do art. 45 powyższej ustawy, w którym na administratorów nałożono tożsamy obowiązek, jaki istnieje na gruncie art. 34 rozporządzenia 2016/679. Jest to obowiązek zawiadomienia osób, których dane dotyczą o naruszeniu ochrony danych osobowych w sytuacji wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Są jednak okoliczności, które mogą obejmować opóźnienie, ograniczenie bądź odstępstwo od wskazanego obowiązku. Zastosować je można wyłącznie w przypadku, gdzie przekazanie informacji mogłoby przyczyniać się do:

- ujawnienia informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;
- utrudnienia lub uniemożliwienia rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
- utrudnienia prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;

[26] Patrz art. 44 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2023 r., poz. 1206).
[27] Por. M. Toumi, Nowe obowiązki administratorów danych osobowych, „Teka Komisji Prawniczej PAN Oddział w Lublinie", T. XII, 2019, Nr 2, s. 379-383.
[28] Kwestie tę reguluje art. 44 ust. 1-3 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

- zagrożenia życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;
- zagrożenia bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;
- istotnego naruszenia dóbr osobistych innych osób[29].

Innym aktem prawnym, mającym przedmiotowe zastosowanie jest Rozporządzenie (UE) w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym[30]. Zgodnie z art. 19a ust. 1 rozporządzenia eIDAS, nałożono także określone wymogi dla niekwalifikowanych dostawców usług zaufania. Muszą oni posiadać m.in. odpowiednie polityki bezpieczeństwa i wprowadzać odpowiednie środki w celu zarządzania ryzykiem prawnym, biznesowym, operacyjnym oraz innymi bezpośrednimi lub pośrednimi ryzykami dla świadczenia niekwalifikowanej usługi zaufania. Ponadto taki dostawca musi powiadomić organ nadzoru bądź inne odpowiednio właściwe organy o wszelkich naruszeniach bezpieczeństwa, które mają znaczący wpływ na świadczoną usługę zaufania lub na przetwarzane w jej ramach dane osobowe, bez zbędnej zwłoki. Tego typu reakcja powinna być podjęta nie później niż w terminie 24 godzin po otrzymaniu informacji o wszelkich naruszeniach bezpieczeństwa lub zakłóceniach.

Nie można przy tym zapominać o przepisach ustawy o krajowym systemie cyberbezpieczeństwa. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT GOV) prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, pełni rolę Zespołu CSIRT poziomu krajowego, który odpowiada za właściwą koordynację procesu reagowania na incydenty komputerowe. Także w oparciu o art. 34 ust. 2 tej ustawy, nakłada się na Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego, (tj. CSIRT MON, CSIRT NASK i CSIRT GOV), koordynujące obsługę incydentu, który doprowadził do naruszenia ochrony danych osobowych, obowiązek

[29] Założenia te reguluje art. 26 ust. 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.
[30] Patrz: Rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE. L. 2014.257.73), zwane dalej jako Rozporządzenie eIDAS.

współpracy z Prezesem Urzędu Ochrony Danych Osobowych[31]. W sytuacji, gdy takie incydenty stanowią rzeczywiste naruszenie ochrony danych osobowych w oparciu o rozporządzenie 2016/679 lub w momencie, gdy się nimi stają, operatorzy usług kluczowych, w trybie art. 33 ust.1 rozporządzenia 2016/679, są zobligowani do zawiadomienia organu nadzorczego, niezależnie od wymogów, które związane są ze zgłoszeniem incydentu na podstawie przepisów przywołanej ustawy o krajowym systemie cyberbezpieczeństwa[32].

ZAKOŃCZENIE

Bezpieczeństwo informacji, w tym bezpieczeństwo ochrony danych osobowych, jest niezwykle istotnym obszarem zarządzania każdą organizacją publiczną[33]. Zważywszy na fakt, że może przyjmować dość krytyczny charakter z uwagi na niezwykle cenną wartość rynkową, może wpływać na konieczność zastosowania ważnych mechanizmów ochronnych. Dane osobowe w każdym indywidualnym przypadku, z racji usytuowania ich w grupie danych wrażliwych, powinny być poddane wyjątkowej chronione, szczególnie z uwagi na wymagania wyznaczone w wielu w aktach prawnych. Zatem w takich warunkach, odpowiedzią na potrzeby prawno-organizacyjne, stworzono w podmiotach administracji publicznej systemowe rozwiązania w zakresie zarządzania ochroną danych osobowych.

Nie bez powodu, za prawidłowe zarządzanie bezpieczeństwem ochrony danych osobowych, odpowiada nie tylko zarządzający instytucją publiczną, ale również i funkcjonujący w każdym podmiocie odpowiedni poziomu kultury ochrony informacji. Jednak należy zaznaczyć, że nawet najlepiej skonstruowane mechanizmy, procedury, czy inwestycje w najnowsze technologie zabezpieczeń systemów informatycznych, nie są w stanie ochronić dane osobowe, w warunkach, gdzie kultura bezpieczeństwa ochrony danych osobowych nie stanie się priorytetem wśród pracowników całej administracji

[31] Art. 34 ust. 2 ustawy z dnia 15 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 ze zm.), zwana dalej u.k.s.c.
[32] Patrz założenia dotyczące operatora usługi kluczowej wskazanej w art. 5 ust. 1 u.k.s.c.
[33] Por. M. Karpiuk, Normatywno-aksjologiczne aspekty bezpieczeństwa, „Cybersecurity and Law", nr 1 (13) 2025, s. 15-18.

publicznej. Należy także pamiętać, że system bezpieczeństwa i przetwarzania ochrony danych osobowych, stanowi kluczowy element realizacji obowiązków administracji publicznej, bez którego konkretne zadanie publiczne nie może zostać zrealizowane na podstawie obowiązujących przepisów prawa.

Bibliografia

Literatura

Bajorek J., Ochrona i bezpieczeństwo danych osobowych w organizacji, „De Securitate et Defensione. O Bezpieczeństwie i Obronności", Nr 1 (2) 2016.

Banyś T., Funkcje prawa ochrony danych osobowych, [w:] Prawo ochrony danych osobowych, T. A. J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak (red.), Difin, Warszawa 2016.

Banyś T., Łuczak J., Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych, Wydawnictwo Presscom, Wrocław 2017.

Behr J., Wyodrębnianie się prawa ochrony danych osobowy [w:] Środki prawne ochrony danych osobowych, M.

Błażewski, J. Behr (red.), Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2016.

Czuryk M., Bezpieczeństwo jako dobro wspólne, „Zeszyty Naukowe KUL" 2018, nr 3.

Duniewska Z., Cel publiczny, interes publiczny i dobro wspólne [w:] Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie, M. Stahl (red.), Wolters Kluwer, Warszawa 2013.

Everson E., Privacy by Design: Taking CTRL of Big Data, „Cleveland State Law Review", 2017, Vol. 65, Iss. 1.

Kawecki M., Główne cele ogólnego rozporządzenia o ochronie danych osobowych, [w:] M. M. Kawecki, T. Osiej (red.), Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia, C.H. Beck, Warszawa 2017.

Karpiuk M., Normatywno-aksjologiczne aspekty bezpieczeństwa, „Cybersecurity and Law", nr 1 (13) 2025.

Karpiuk M., The Local Government's Position in the Polish Cybersecurity System, „Lex Localis - Journal of Local Self-Government", nr 3, 2021.

Kępa L., Ochrona danych osobowych w praktyce, C. H. Beck, Warszawa 2011.

Krasuski A., Dane osobowe w obrocie tradycyjnym i elektronicznym. Praktyczne problemy, Wolters Kluwer, Warszawa 2012.

Mędrala-Natkaniec M., Jakie zmiany w zakresie ochrony danych osobowych pracowników wprowadza RODO, PWN, Warszawa 2018.

Młynarska-Sobaczewska A., Trzy wymiary prywatności. Sfera prywatna i publiczna we współczesnym prawie i teorii społecznej, „Przegląd Prawa Konstytucyjnego" 2013, Nr 1(13).

Nowacki G., Znaczenie informacji w obszarze bezpieczeństwa narodowego, „Nierówności Społeczne a Wzrost Gospodarczy", 2013, nr 36.

Skoczylas D., 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, „Młody Jurysta", 2019, Nr 1.

Toumi M., Nowe obowiązki administratorów danych osobowych, „Teka Komisji Prawniczej PAN Oddział w Lublinie", T. XII, 2019, Nr 2.

Wiewiórowski W. R., Prywatność pacjenta musi być chroniona, „IT w Administracji", Nr 2/2013.

Wojciechowski Ł., Działania typu phishing jako zagrożenie cyberbezpieczeństwa obywateli Rzeczypospolitej Polskiej [w:] W trosce o bezpieczne jutro. Reminiscencje i zamierzenia, S. Niedzwiecki, N. Starik (red.), Wydawnictwo Wyższej Szkoły Bezpieczeństwa w Poznaniu, Poznań 2017.

Wojciechowski Ł., Bezpieczeństwo informacji w polskim samorządzie terytorialnym na tle procesu ujednolicania systemu ochrony danych osobowych w Unii Europejskiej, „Rocznik Administracji Publicznej", Nr 5, 2019.

Wojciechowski Ł., Rola administratorów bezpieczeństwa informacji w kształtowaniu bezpieczeństwa informacyjnego w Rzeczypospolitej Polskiej [w:] Społeczno-prawne problemy bezpieczeństwa wewnętrznego III Rzeczypospolitej. Wybrane Zagadnienia, M. Gąska (red.), Wydawnictwo Naukowe Innovatio Press, Lublin 2017.

Akty normatywne

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483, ze zm.).

Ustawa z dnia 27 sierpnia 2009 r. o ustawie finansów (t.j. Dz. U. z 2024 r. poz. 1530 ze zm.).

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (t.j. Dz. U. z 2023 r., poz. 1206).

Ustawa z dnia 15 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 ze zm.).

Rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE. L. 2014.257.73).

Rozporządzenia 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) (Dz. Urz. UE L 119 z 04.05.2016).

CONDITIONS OF SECURITY AND PROTECTION OF PERSONAL DATA IN PUBLIC ADMINISTRATION

Abstract

This article draws attention to the special role of information and personal data in the security management system. The importance of information, in this case also of personal data protection mechanisms, requires a systemic approach. Therefore, strategic areas and principles of the information security management system in public administration will be indicated. The applicable legal provisions regulating the assumptions of the admissibility of processing and protection of personal data in teleinformatic systems also determine the appropriate levels of protection of such information. In the conditions of securing personal data, in each public organization processing and protecting such data, there is a personal data administrator who can appoint an information security administrator to perform such tasks. The text will approximate selected areas, due to the complex nature of the issue discussed, which are implemented by public administration bodies in the area of personal data protection.

Keywords: public administration, security, protection, personal data, RODO.