DOI 10.4467/24497800RAP.19.013.11476
http://www.ejournals.eu/RAP/
ISSN 2449-7800 (online), ISSN 2449-7797 (druk), s. 201–215

Łukasz Wojciechowski[1]

Bezpieczeństwo informacji w polskim samorządzie terytorialnym na tle procesu ujednolicania systemu ochrony danych osobowych w Unii Europejskiej

1. Wprowadzenie

Bezpieczeństwo informacji to obszar, który systematycznie zyskuje na znaczeniu. Wynika to przede wszystkim ze wzrostu ilości danych przetwarzanych w systemach informatycznych. Niektórzy badacze wskazują również, że w XXI w. nastąpiła era społeczeństwa informacyjnego[2]. Argumentem za takim poglądem jest systematyczny rozwój przedsiębiorczości, która nie opiera się na produkcji, a na świadczeniu usług związanych z informacją. Jednocześnie obywatele oczekują, że płacone przez nich daniny na rzecz państwa będą przeznaczone m.in. na informatyzację urzędów, co pozwoli im na szybsze, łatwiejsze i bardziej efektywne załatwianie spraw, również za pośrednictwem sieci Internet. Równolegle do funkcjonowania podmiotów, które chcą zarabiać na informacji w sposób uczciwy i innowacyjny, można zaobserwować systematyczny rozwój cyberprzestępczości. Z jednej strony do Internetu przenoszą się działania przestępców, które dotychczas były znane poza cyberprzestrzenią. Z drugiej strony pojawiają się nowe działania cyberprzestępców charakteryzujące się coraz większą kreatywnością, m.in. różne rodzaje cyberprzestępstw typu phishing[3].

Szczególne znaczenie w całym procesie prewencji zagrożeń bezpieczeństwa informacji ma ochrona danych osobowych. Należy ją traktować jako element bezpieczeństwa informacji, które jest pojęciem o szerszym znaczeniu, obejmuje bowiem informacje dotyczące osób fizycznych, takie jak dane osobowe, ale także szerokie spektrum informacji poufnych z innego

1 Dr Łukasz Wojciechowski, Wydział Administracji i Nauk Społecznych, Wyższa Szkoła Ekonomii i Innowacji w Lublinie.

2 G. Nowacji, *Znaczenie informacji w obszarze bezpieczeństwa narodowego*, „Nierówności Społeczne a Wzrost Gospodarczy" 2013, nr 36, s. 107.

3 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.), Poznań 2017, s. 399–400.

zakresu, np. informacji gospodarczych. Dane osobowe to dane osób fizycznych, przez co naruszenia bezpieczeństwa tych danych prowadzą najczęściej do zagrożenia ich praw i wolności. Jednocześnie system ochrony danych osobowych w państwach Unii Europejskiej jest skonstruowany w taki sposób, że zapobieganie tego typu zagrożeniom jest zadaniem wszystkich podmiotów przetwarzających dane osobowe. Są to firmy oraz instytucje administracji publicznej. Każdy administrator danych osobowych ponosi odpowiedzialność za ich przetwarzanie. Żeby przetwarzać dane osobowe w sposób bezpieczny, administrator musi nadać swoim pracownikom uprawnienia do przetwarzania poszczególnych zbiorów danych. Istotne jest także zapewnienie mechanizmów rozliczalności, które prowadzi do budowania indywidualnej odpowiedzialności za podejmowane decyzje i ewentualne błędy.

Jednostki samorządu terytorialnego odgrywają szczególną rolę w procesie ochrony danych osobowych. Wynika to ze specyfiki zadań, jakie wykonują na rzecz osób fizycznych. Z uwagi na rozbudowane struktury kadrowe szczególnym zadaniem jest odpowiednie przygotowanie urzędników do nowych wyzwań związanych z reformą systemu ochrony danych osobowych. Celem artykułu jest analiza funkcjonowania mechanizmów bezpieczeństwa informacji w polskim samorządzie terytorialnym w świetle reformy systemu ochrony danych osobowych we wszystkich państwach Unii Europejskiej. Autor poddaje weryfikacji hipotezę badawczą, że nowe regulacje przyczyniają się do poprawy funkcjonowania systemu ochrony danych osobowych i uporządkowania procedur w tym obszarze w jednostkach samorządu terytorialnego. Do napisania artykułu wykorzystane zostały dwie metody badawcze. Pierwsza z nich to metoda instytucjonalno-prawna, która umożliwiła analizę polskich aktów normatywnych regulujących ochronę danych osobowych, jak również wybranych aktów prawa unijnego. Druga to analiza czynnikowa, dzięki której wyodrębniono spośród zmiennych zależnych i niezależnych najważniejsze elementy kształtujące bezpieczeństwo informacji w jednostkach samorządu terytorialnego. Przedstawione rozważania autor opiera także na własnych doświadczeniach ze współpracy z jednostkami samorządu terytorialnego we wdrażaniu procedur bezpieczeństwa informacji, ze szczególnym uwzględnieniem ochrony danych osobowych.

2. Proces ujednolicenia systemu ochrony danych osobowych w państwach Unii Europejskiej

Analizę procesu ujednolicania systemu ochrony danych osobowych w państwach Unii Europejskiej warto rozpocząć od dygresji, że do momentu wejścia w życie Traktatu lizbońskiego 1 grudnia 2009 r. Unia Europejska nie miała osobowości prawnej i funkcjonowała jako Wspólnota

Europejska[4]. Dlatego działania koncepcyjne, legislacyjne i analityczne podejmowane w ramach Wspólnoty Europejskiej zapoczątkowały proces ujednolicenia systemu ochrony danych osobowych w obecnie funkcjonującej Unii Europejskiej. Warto też podkreślić, że przystąpienie Polski do Wspólnoty miało miejsce 1 maja 2004 r., jednak poprzedziły je wieloletnie przygotowania o charakterze wielowymiarowym. Dlatego wdrażanie i implementacja wielu rozwiązań i procedur rozpoczęło się przed tą datą.

Proces ujednolicenia systemu ochrony danych osobowych odbywał się kumulatywnie w dwóch obszarach. Wszczęto działania legislacyjne mające na celu uporządkowania prawodawstwa w zakresie ochrony danych osobowych, a jednocześnie podjęto próbę opracowania rozwiązań mających na celu prewencję zagrożeń wynikających z dynamicznego rozwoju sieci Internet. W obydwu przypadkach konieczne było intensywne tempo prac z uwagi na szerokie spektrum różnorodnych i dynamicznych interakcji w Internecie oraz wzrost znaczenia przetwarzania danych osobowych, co korelowało z koniecznością ich adekwatnej ochrony.

Proces ujednolicenia systemu ochrony danych osobowych w państwach Unii Europejskiej zapoczątkowała 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[5]. W tym przypadku można jednak mówić zaledwie o częściowym ujednoliceniu systemu. Specyfika dyrektywy polega bowiem na tym, że państwa członkowskie (w tym przypadku także państwa aspirujące do członkostwa) dokonują jej implementacji w formie odrębnego krajowego aktu normatywnego. Umożliwia to elastyczne modyfikowanie przepisów dyrektywy oraz dodawanie własnych procedur. Dopiero podmioty, które czują się pokrzywdzone przez swoje państwo z powodu braku właściwej implementacji dyrektywy, mogą dochodzić swoich praw w organach unijnego wymiaru sprawiedliwości. Jest to jednak procedura skomplikowana i długoterminowa.

Warto podkreślić, że Polska była jednym z państw, które uchwaliły akt prawny wiernie odwzorowujący założenia dyrektywy – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[6], która obowiązywała przez ponad dwadzieścia lat – do 24 maja 2018 r. W tym okresie ustawa była kilkakrotnie nowelizowana. Z perspektywy czasu uchwalenie ustawy w 1997 r. w ówczesnym kształcie uznać należy za działanie nieadekwatne. Większość podmiotów przetwarzających dane osobowe nie była przygotowana do realizowania przepisów tej ustawy. Jednocześnie dopiero w 2004 r., niemal w przeddzień akcesji Polski do Wspólnoty Europejskiej, weszło

4 M. Rewizorski, *Podmiotowość prawnomiędzynarodowa Wspólnot Europejskich oraz Unii Europejskiej*, „Środkowoeuropejskie Studia Polityczne" 2011, nr 1, s. 60.

5 Dz.Urz. WE L 281, s. 31, ze zm.

6 Tekst pierwotny: Dz.U. z 1997 r. Nr 133, poz. 883, ostatni tekst jedn.: Dz.U. z 2016 r. poz. 922 ze zm.

w życie rozporządzenie wykonawcze do ustawy, które dawało precyzyjną instrukcję w zakresie wymaganej dokumentacji (procedur) ochrony danych osobowych oraz minimalnych wymogów w zakresie zabezpieczeń technicznych[7]. Wówczas podmioty przetwarzające dane osobowe, w tym jednostki samorządu terytorialnego, otrzymały listę kontrolną w zakresie wymagań, jakie są przed nimi stawiane przez uprawnione organy państwowe.

Organy Wspólnoty Europejskiej podejmowały jednocześnie działania mające na celu efektywne zwalczanie przestępczości w cyberprzestrzeni. Proces mający priorytetowe znaczenie w tym zakresie rozpoczął się w 1996 r. Była to próba przeciwdziałania wykorzystaniu Internetu do celów związanych z rozpowszechnianiem informacji zakazanych przez prawo. Komisja Europejska, wezwana przez ministrów do spraw kultury i telekomunikacji podczas nieformalnego spotkania w Bolonii, opracowała przyjęty 16 października 1996 r. komunikat Komisji dla Rady, Parlamentu Europejskiego, Komitetu Ekonomiczno-Społecznego i Regionów na temat nielegalnej i szkodliwej treści w Internecie. Wraz z komunikatem przyjęto „Zielony Dokument" dotyczący ochrony małoletnich i poszanowania godności ludzkiej w usługach informacyjnych i audiowizualnych[8]. Podczas opracowywania dokumentu dokonano analizy aktów prawnych szesnastu państw członkowskich. Jedną z konkluzji było występowanie istotnych różnic w zakresie definiowania konkretnych przestępstw i zjawisk, np. pornografii. Od tamtej pory zaczęto podejmować systematyczne działania mające na celu wprowadzenie standardów kryminalizacji cyberprzestępstw. Jednocześnie mandat Wspólnoty Europejskiej w tym zakresie był ograniczony, ponieważ brakowało akceptacji państw członkowskich dla ingerencji w systemy prawne państw członkowskich – preferowano wówczas decyzje ramowe, a nie dyrektywy. Jednak nie ulegało wątpliwości, że również w kwestii cyberprzestępczości skuteczne działania były możliwe tylko w przypadku ujednolicenia procedur. Stąd też kolejne inicjatywy koncentrowały się na opracowywaniu wytycznych dla państw członkowskich w zakresie zmian legislacyjnych. Natomiast kluczowym momentem stało się wejście w życie Traktatu z Lizbony. Wówczas prawo karne stało się osobną polityką współpracy.

Zarówno prace nad uregulowaniami prawnymi ochrony danych osobowych, jak również pozostałe wspólne działania w innych obszarach, m.in. opracowywanie strategii i procedur w zakresie zwalczania cyberprzestępczości, doprowadziły do uchwalenia nowego aktu prawa unijnego. Warto zwrócić uwagę, że przyjęto inne rozwiązanie niż w 1995 r. Wskazana wcześniej dyrektywa została zastąpiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie

7 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. Nr 100, poz. 1024.

8 M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 37.

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)[9]. Oznaczało to, że nowe przepisy prawa nie będą wymagały implementacji przez państwa członkowskie Unii Europejskiej. Jednocześnie można prognozować, że nowe uregulowania prawne ukształtują system ochrony danych osobowych na kilkadziesiąt kolejnych lat[10]. Po wejściu w życie nowych przepisów prawa przewidziano dwuletni okres przejściowy, a następnie RODO zaczęło bezwzględnie obowiązywać we wszystkich państwach członkowskich (25 maja 2018 r.). Jest to data, którą można uznać za finalizację procesu ujednolicenia systemu ochrony danych osobowych. Podkreślenia wymaga fakt, że RODO nie było aktem prawnym stworzonym wyłącznie na podstawie doświadczeń ze stosowania przepisów dyrektywy poprzedzającej rozporządzenie. Przepisy zostały także przygotowane w oparciu o doświadczenia różnego rodzaju gremiów i elementów struktury Unii Europejskiej, m.in. w zakresie prac nad penalizacją cyberprzestępstw i analizy wieloaspektowego bezpieczeństwa informacji w państwach członkowskich.

Decyzja o nadaniu aktowi normatywnemu regulującemu system ochrony danych osobowych rangi rozporządzenia wiązała się z tym, że niezależnie od porządku prawnego w poszczególnych państwach wszystkie podmioty przetwarzające dane osobowe musiały stosować nowe regulacje podczas ich przetwarzania. Jednocześnie obywatele mogą dochodzić swoich praw sankcjonowanych w RODO zarówno w sądach powszechnych, jak również składając skargę do nowego organu ochrony danych. Nowa polska ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[11], której wejście w życie skorelowano z datą bezwzględnego obowiązywania RODO, w przeciwieństwie do swojej poprzedniczki nie zawiera już takich elementów jak definicje i zasady legalnego przetwarzania. Celem tego aktu prawnego stało się natomiast doprecyzowanie przepisów RODO w kontekście ich realizacji w Polsce oraz powołanie nowego organu ochrony danych – Prezesa Urzędu Ochrony Danych Osobowych (UODO). Nowy organ zastąpił Generalnego Inspektora Ochrony Danych Osobowych (GIODO), jednak w praktyce zmieniła się tylko jego nazwa. Zastosowano bowiem rozwiązanie polegające na pełnym następstwie prawnym. Osoba pełniąca funkcję GIODO objęła również stanowisko Prezesa UODO.

W przypadku samorządu terytorialnego w Polsce wyzwaniem stało się przede wszystkim dostosowanie poszczególnych jednostek do nowych regulacji. Warto podkreślić, że przepisy RODO odnoszą się do funkcjo-

9 Dz.Urz. UE L 119, s. 1, ze zm., dalej: RODO.

10 E. Bielak-Jomaa, P. Drobek, D. Krajewska-Kekusz, M. Młotkiewicz, M. Kawecki, T. Soczyński, A. Kaczmarek, K. Hildebrandt, *Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych w świetle ogólnego rozporządzenia o ochronie danych*, Warszawa 2016, s. 11.

11 Dz.U. poz. 1000 ze zm.

nowania korporacji dysponujących znaczącymi zasobami finansowymi, ministerstw i urzędów centralnych. Jednocześnie wymogi w zakresie przetwarzania danych osobowych muszą być także spełnione przez podmioty prywatne i publiczne dysponujące niewielkimi środkami finansowymi i zasobami ludzkimi, w tym niewielkie jednostki samorządu terytorialnego. Ustawodawca zmniejszył także potencjalne obciążenia finansowe w przypadku nałożenia kary przez Prezesa UODO na instytucje publiczne. Maksymalny wymiar kary wynosi 100 tys. zł (z wyjątkiem instytucji kultury, dla których jest to 10 tys. zł) i jest znacznie mniejszy niż wielomilionowe kary, które mogą zostać nałożone na firmy.

3. Konieczność zastosowania technicznych i organizacyjnych środków ochrony danych osobowych w jednostkach samorządu terytorialnego

Kadra kierownicza jednostek samorządu terytorialnego z związku z rozpoczęciem bezwzględnego obowiązywania RODO otrzymała trudne zadanie dostosowania funkcjonowania urzędów i innych jednostek do nowych uregulowań prawnych. Wyzwanie to miało charakter wielowymiarowy i dotyczyło m.in.:

- odpowiedniego przygotowania merytorycznego pracowników jednostek samorządu terytorialnego,
- dostosowania formularzy i innych dokumentów funkcjonujących w instytucjach,
- odpowiedniego przygotowania systemów informatycznych, w których są przetwarzane dane osobowe,
- przeglądu i dostosowania infrastruktury służącej do załatwiania spraw w instytucjach (np. ograniczającej liczbę petentów przebywających przy jednym stanowisku),
- inwentaryzacji dokumentów przechowywanych w instytucjach pod kątem adekwatności wynikającej z wymogu minimalizacji danych.

Jednym z priorytetowych działań było umożliwienie zdobycia teoretycznej i praktycznej wiedzy w zakresie ochrony danych osobowych pracownikom samorządowym. W tym przypadku istotne znaczenie miał aspekt finansowy. Jak wskazuje R. Kamiński: „W systemie zdecentralizowanej administracji publicznej finanse jednostek samorządu terytorialnego stanowią podstawowy element zarządzania dla realizacji przypisanych ustawą zadań publicznych”[12]. Jednak nawet jeśli zaplanowano i wygospodarowano środki finansowe, w niektórych obszarach Polski pojawił się problem ze znalezieniem profesjonalnych trenerów. Jest to naturalne zjawisko w przypadku znaczącego wzrostu zapotrzebowania na usługi sektorowe,

12 R. Kamiński, *Dochody, wydatki i wyniki budżetowe miast na prawach powiatu. Wybrane aspekty* [w:] *Samorząd miasta na prawach powiatu. Struktury, aktorzy, działanie*, A. Jarosz, B. Springer (red.), Zielona Góra 2018, s. 279.

który prowadzi do perturbacji na rynku usług. Nawet przy dużym zaangażowaniu i maksymalnym zwiększeniu wydajności pracy przez ekspertów w zakresie bezpieczeństwa informacji i ochrony danych osobowych nie byli oni w stanie przyjąć wszystkich oferowanych zleceń. Dodatkowym problemem była konieczność przygotowania pracowników samorządowych do reformy ochrony danych osobowych przez trenerów, którzy znają specyfikę samorządu terytorialnego. Eksperci zajmujący się ochroną danych osobowych w innych branżach nie byli bowiem w stanie odpowiedzieć na wszystkie wątpliwości pracowników samorządowych, nie znając przepisów sektorowych i praktyki funkcjonowania urzędów i innych jednostek. Problemy ze znalezieniem profesjonalnego wsparcia merytorycznego stały się skutkiem ubocznym ujednolicenia systemu ochrony danych osobowych nie tyle we wszystkich państwach Unii Europejskiej, co w każdym z tych państw z osobna. Jednocześnie słabą stroną funkcjonowania niektórych jednostek samorządu terytorialnego były wieloletnie zaniedbania w procesie budowania kapitału ludzkiego posiadającego odpowiednie kompetencje w zakresie bezpieczeństwa informacji, jak również negatywne nastawienie pracowników samorządowych do reformy. Warto zwrócić uwagę, że praca w jednostkach samorządu terytorialnego wiąże się z koniecznością systematycznej adaptacji wykonywanych zadań do zmieniającej się rzeczywistości legislacyjnej. Prowadzi to do sytuacji, w której niektórzy pracownicy samorządowi są zmęczeni koniecznością ciągłego dostosowywania swojej pracy do zmieniających się aktów normatywnych.

Kolejnym obszarem wymagającym dostosowania się do nowych, ujednoliconych regulacji stały się formularze i inne elementy dokumentacji oraz procedura przyjmowania dokumentów od petentów. W tym przypadku kluczowe znaczenie miało zastosowanie art. 5 RODO, w którym określono sześć zasad przetwarzania danych osobowych. Wśród nich znalazły się zasady ograniczenia przechowywania i minimalizacji danych. Oznaczają one, że twórcy formularzy muszą szczegółowo przeanalizować, jakie pola informacyjne będą uzupełniać petenci oraz zdecydować, jaki będzie okres przechowywania tych danych. Jest to jednocześnie egzemplifikacja ochrony proaktywnej (ang. *privacy by design*), wskazanej w art. 25 RODO. Pojęcie to oznacza uwzględnienie ochrony danych osobowych już na etapie projektowania poszczególnych działań[13].

Podkreślenia wymaga fakt, że w związku z wejściem w życie przepisów RODO na administratorów danych osobowych zostały nałożone nowe obowiązki, ale też część wymogów funkcjonujących wcześniej została zlikwidowana. Dotyczy to przede wszystkim szerokiego spektrum zabezpieczeń systemów informatycznych, których zastosowanie przed 25 maja 2018 r. miało charakter obligatoryjny z uwagi na obowiązek prawny wyni-

13 Por. E. Everson, *Privacy by Design: Taking CTRL of Big Data*, „Cleveland State Law Review" 2017, vol. 65, iss. 1, s. 28.

kający z rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Ujednolicenie procedur polega w tym przypadku na wprowadzeniu dowolności wyboru środków zabezpieczających przez administratorów danych osobowych. Jednocześnie poszczególne podmioty zostały zobligowane do prowadzenia analizy ryzyka i oceny skutków dla ochrony danych. Oznacza to, że poszczególne jednostki samorządu terytorialnego mają stosować zabezpieczenia systemów informatycznych, które są adekwatne z punktu widzenia potencjalnych zagrożeń. Jeżeli przed reformą systemu ochrony danych osobowych nie dochodziło do naruszeń bezpieczeństwa, to najprawdopodobniej zastosowane zabezpieczenia, np. programy antywirusowe lub procedury nadawania uprawnień, użytkownikom systemu funkcjonowały prawidłowo. W RODO, oprócz analizy ryzyka, jako skuteczny środek ochrony danych wskazano także pseudonimizację. Jest to działanie funkcjonujące w administracji publicznej niektórych państw Unii Europejskiej, stosowane również w Stanach Zjednoczonych Ameryki. Polega na rozbiciu zbioru danych na mniejsze elementy. Zakres zbioru danych można odczytać dopiero po odpowiednim połączeniu poszczególnych elementów, najczęściej z zastosowaniem odpowiedniego klucza[14].

Ostatnim z kluczowych obszarów w zakresie technicznych i organizacyjnych środków ochrony danych osobowych jest infrastruktura służąca do załatwiania spraw przez petentów. W niektórych obiektach jednostek samorządu terytorialnego rozwiązania w tym zakresie przyjęły najprostszą formę, np. namalowanie na podłodze linii, które wskazują minimalną odległość oczekiwania na załatwienie sprawy przy stanowisku urzędnika. Reforma systemu ochrony danych osobowych stała się również czynnikiem motywującym kierownictwo jednostek do zastosowania bardziej zaawansowanych rozwiązań, np. elektronicznego systemu kolejkowego. Dzięki takim rozwiązaniom petenci nie muszą oczekiwać przy konkretnym stanowisku i zmniejsza się ryzyko, że usłyszą dane osobowe osoby załatwiającej swoją sprawę. Ponadto wraz z ujednoliceniem systemu ochrony danych osobowych przeprowadzono liczne audyty, które pomogły zidentyfikować obszary deficytowe. Wówczas dla ochrony danych osobowych zaczęto stosować rozwiązania, które nie wymagały znaczących nakładów finansowych, m.in. zmiany ustawienia monitorów stacji roboczych lub zakup filtrów prywatyzujących, przesunięcie mebli w pomieszczeniach i inna organizacja stanowisk pracy oraz zakup niszczarek lub szaf zamykanych na klucz.

14 C. Achatz, S. Hubbard, *US vs. EU Guidelines For De-Identification, Anonymization, and Pseudonymization*, „Journal of Internet Law" 2017, vol. 20, iss. 11, s. 7.

4. Prewencja zagrożeń i adekwatne reagowanie na naruszenia ochrony danych osobowych przez jednostki samorządu terytorialnego

Przepisy RODO mają na celu zagwarantowanie praw osób fizycznych m.in. w oparciu o Kartę praw podstawowych Unii Europejskiej. W sytuacjach spornych, zgodnie z art. 47 Karty: „Każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem”[15]. Jednocześnie każdy podmiot przetwarzający dane osobowe jest zobowiązany zapewnić osobie, której dane dotyczą, m.in. prawo dostępu do danych, prawo do sprostowania danych, prawo do bycia zapomnianym (prawo do usunięcia danych), prawo do ograniczenia przetwarzania danych, prawo do przenoszenia danych i prawo do sprzeciwu oraz do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu. W przypadku jednostek samorządu terytorialnego realizacja tych praw wymaga specjalistycznej, sektorowej wiedzy, ponieważ nie są to prawa bezwzględne, które należy realizować natychmiast, bez wymaganej refleksji. W RODO zostały wskazane przesłanki ograniczenia lub braku realizacji tych praw, m.in. w związku z zapewnieniem bezpieczeństwa narodowego lub publicznego oraz kiedy prawa osób, których dane dotyczą, utrudniają wypełnienie celów gospodarczych lub finansowych państwa członkowskiego lub Unii Europejskiej. Przykładem może być realizacja prawa do bycia zapomnianym wynikającego z art. 17 RODO. Jeżeli nie ma możliwości usunięcia wszystkich danych osoby fizycznej, np. z powodu obowiązku prawnego przechowywania danych przez określony czas wynikającego z obowiązującego aktu normatywnego, to pracownik samorządowy musi zadecydować, które dane może usunąć, a które muszą pozostać w zasobach jednostki. Niezależnie od decyzji konieczne jest przygotowanie odpowiedzi na wniosek osoby, której dane dotyczą i która zwróciła się z prośbą o realizację prawa do bycia zapomnianym, uzasadniającej decyzję o usunięciu lub nieusunięciu poszczególnych danych.

Jedną z najbardziej spektakularnych form ujednolicenia systemu ochrony danych osobowych w państwach Unii Europejskiej stał się obowiązek wyznaczenia inspektora ochrony danych (IOD) we wszystkich organach lub podmiotach publicznych[16]. W praktyce oznaczało to, że każda jednostka samorządu terytorialnego musiała zatrudnić taką osobę, wyznaczyć osobę już pracującą w jednostce bądź też skorzystać z usług firmy zewnętrznej w tym zakresie. Funkcja IOD zastąpiła stanowisko administratora bezpieczeństwa informacji (ABI), znane wcześniej w polskim samorządzie terytorialnym[17]. Zasadniczą różnicą jest jednak to, że wyznaczenie ABI było

15 Dz.Urz. UE z 2016 r. C 202, s. 389.

16 Art. 37 RODO.

17 Ł. Wojciechowski, *Rola administratorów bezpieczeństwa informacji w kształtowaniu bezpieczeństwa informacyjnego w Rzeczypospolitej Polskiej* [w:] *Społeczno-prawne*

fakultatywne i to kierownik jednostki decydował, czy widzi potrzebę takiego działania. Biorąc pod uwagę deficyty w zakresie bezpieczeństwa informacji, ze szczególnym uwzględnieniem ochrony danych osobowych w administracji publicznej państw Unii Europejskiej, twórcy nowych uregulowań prawnych nie pozostawili już w tym zakresie wyboru. Sama koncepcja pojawienia się ekspertów w zakresie ochrony danych osobowych w każdym urzędzie i w innych jednostkach samorządu terytorialnego zasługuje na uznanie. Obiektywny ogląd sytuacji wymaga jednak konstatacji, że 25 maja 2018 r. nie było na rynku pracy wystarczającej liczby specjalistów gotowych przyjąć na siebie obowiązki IOD. Stąd też pojawienie się firm, które świadczyły usługi na niewystarczającym poziomie oraz wyznaczanie do pełnienia funkcji IOD pracowników samorządowych, którzy wraz z rozpoczęciem sprawowania tych funkcji rozpoczynali naukę przepisów i rozwiązań praktycznych w zakresie ochrony danych osobowych. Można jednak prognozować, że sytuacja w tym zakresie będzie się poprawiać, ponieważ reforma systemu wzbudziła zainteresowanie tą problematyką, a praca w branży ochrony danych osobowych jest postrzegana jako atrakcyjna i potrzebna w przyszłości. Stąd też znacząca popularność wartościowych szkoleń dla IOD, studiów podyplomowych oraz innych form podnoszenia kwalifikacji. Zagadnienia w tym zakresie pojawiają się również w programach studiów pierwszego i drugiego stopnia. Czynnikiem sprzyjającym takiej popularyzacji zagadnienia jest jego interdyscyplinarny charakter. Można więc przypuszczać że wraz z pojawieniem się większej liczby fachowców na rynku, poprawi się również jakość wykonywanych usług.

Niektórym jednostkom samorządu terytorialnego udało się już na początku funkcjonowania zreformowanego systemu pozyskać ekspertów lub osoby, które systematycznie i efektywnie podnoszą swoje kwalifikacje, pełniąc funkcję IOD. W takich jednostkach wzrasta potencjał w zakresie podnoszenia jakości ochrony danych osobowych. Zakres zadań IOD, którzy prawidłowo sprawują swoją funkcję, można podzielić na trzy obszary. Pierwszy to udzielanie wskazówek i wytycznych dla kierownictwa jednostki i pracowników. Takie działania mogą odbywać się w formie szkoleń, lecz także systematycznych konsultacji. Drugi obszar to wykonywanie sprawdzeń i audytów. Przed reformą systemu sprawdzenia odbywały się według wytycznych zawartych w rozporządzeniu[18], będącym aktem wykonawczym do ówczesnej ustawy o ochronie danych osobowych. Obecnie niektórzy IOD stosują nieobowiązujące już rozporządzenie jako dobrą praktykę. Nie jest to jednak konieczne i wobec braku uregulowań prawnych dotyczących

problemy bezpieczeństwa wewnętrznego III Rzeczypospolitej. Wybrane Zagadnienia, M. Gąska (red.), Lublin 2017, s. 123.

18 Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji, Dz.U. poz. 745.

metodyki przeprowadzania sprawdzeń i audytów każdy IOD może zastosować własne rozwiązania[19]. W tym kontekście warto podkreślić, że efektywna praca IOD nie jest możliwa, jeżeli osoba pełniąca tę funkcję nie ma odpowiedniego miejsca w strukturze instytucji. Inspektor powinien podlegać bezpośrednio kierownikowi jednostki samorządu terytorialnego i mieć swobodny dostęp do wszystkich spraw związanych z przetwarzaniem danych osobowych. Praca IOD może w znaczący sposób przyczynić się do wprowadzenia i stosowania właściwych mechanizmów prewencji zagrożeń bezpieczeństwa informacji w jednostce samorządu terytorialnego. Nadzór profesjonalnego i przygotowanego do wykonywania swoich obowiązków IOD umożliwia również zastosowanie właściwych środków technicznych i organizacyjnych ochrony danych osobowych.

Nawet najlepiej zorganizowana ochrona danych osobowych w jednostce samorządu terytorialnego nie może w pełni zagwarantować braku naruszeń bezpieczeństwa. Doświadczenia analizy ryzyka przeprowadzanej przez jednostki od 2010 r. w ramach kontroli zarządczej wynikającej z ustawy o finansach publicznych[20] prowadzą również do konkluzji, że zaplanowanie (przewidzenie) wszystkich możliwych ryzyk *de facto* nie jest możliwe. Dlatego w ramach ujednolicenia systemu ochrony danych osobowych w państwach Unii Europejskiej stworzono obowiązek prawny adekwatnego reagowania na naruszenia, którym nie udało się zapobiec. Każdy podmiot przetwarzający dane osobowe ma obowiązek zgłoszenia naruszenia bezpieczeństwa danych osobowych do organu ochrony danych w swoim kraju. W przypadku jednostek samorządu terytorialnego w Polsce organem właściwym jest Prezes UODO. Zgłoszenie musi nastąpić bez zbędnej zwłoki, jednak nie później niż w ciągu 72 godzin. Należy zgłaszać wszystkie naruszenia, z wyjątkiem tych, w których zachodzi niewielkie prawdopodobieństwo naruszenia praw i wolności osób fizycznych. Zgłoszenie należy przesłać drogą elektroniczną na formularzu udostępnionym na stronie internetowej UODO i powinno ono:

– opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
– zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
– opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

19 Warto podkreślić, że systematycznie na popularności zyskują audyty oparte na normie PN-ISO/IEC 27001:2014-12 z aktualizacją wg PN-EN ISO/IEC 27001:2017-06, na której wzorowali się także w wielu aspektach twórcy RODO.

20 Art. 68 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, tekst jedn.: Dz.U. z 2019 r. poz. 869 ze zm.

– opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki użyte w celu zminimalizowania jego ewentualnych negatywnych skutków[21].

Ujednolicenie raportowania incydentów prowadzi do dwóch pozytywnych zjawisk. Z jednej strony Prezes UODO ma systematyczną informację na temat obszarów deficytowych w funkcjonowaniu systemu. Z drugiej raportowanie stanowi czynnik motywujący dla podmiotów przetwarzających dane osobowe, w tym jednostek samorządu terytorialnego, do tego, aby naruszeń unikać. Nie jest bowiem uregulowana kwestia korelacji otrzymania przez Prezesa UODO informacji o naruszeniu oraz wszczęcia ewentualnego postępowania kontrolnego w siedzibie podmiotu, który zgłoszenia dokonał. Istnieje więc prawdopodobieństwo, że w obliczu dużej liczby zgłoszeń Prezes może skierować pracowników UODO do siedziby administratora w celu przeprowadzenia stosownej inspekcji. Warto też zwrócić uwagę, że obowiązek prawny dotyczy nie tylko zgłoszenia naruszenia do Prezesa UODO, konieczne jest także poinformowanie osób, których dane dotyczą, o tym, co się stało i jakie mogą być konsekwencje naruszenia. Zgodnie z RODO taki komunikat musi być napisany prostym językiem, żeby mogła go zrozumieć każda osoba fizyczna, również nie posiadająca fachowej wiedzy w zakresie bezpieczeństwa informacji i ochrony danych osobowych.

5. Podsumowanie

Przedstawione rozważania pozwoliły na pozytywną weryfikację hipotezy badawczej, że nowe regulacje przyczyniają się do poprawy funkcjonowania systemu ochrony danych osobowych i uporządkowania procedur w tym obszarze w jednostkach samorządu terytorialnego. Warto jednak podkreślić, że rzetelna i szczegółowa ocena stopnia i zakresu zmian będzie możliwa dopiero w dalszym etapie funkcjonowania systemu. Jest to spowodowane przede wszystkim opóźnieniem w realizowaniu reformy, wynikającym z czynników instytucjonalno-prawnych. 25 maja 2018 r. to dzień, w którym po dwuletnim okresie przejściowym zaczęło bezwzględnie obowiązywać RODO. W rzeczywistości jest to jednak data rozpoczęcia, a nie zakończenia zmian. Tego dnia rozpoczął funkcjonowanie UODO i dopiero w kolejnych miesiącach pojawiły się pierwsze wytyczne i komunikaty. Przesunięto też termin wyznaczania IOD. Jednocześnie kompleksowa ocena skutków reformy nie jest możliwa w pierwszych miesiącach jej funkcjonowania. W tym kontekście warto dodać, że dopiero 4 maja 2019 r. weszła w ży-

21 Art. 33 ust. 3 RODO.

cie ustawa zapewniająca stosowanie RODO[22], mocą której wprowadzono zmiany w 168 aktach prawnych regulujących funkcjonowanie istotnych obszarów funkcjonowania państwa. Przedstawiona analiza umożliwia jednak zidentyfikowanie pozytywnych zjawisk i zmian, jak również sformułowanie kilku konkluzji.

Po pierwsze, jednostki samorządu terytorialnego bez wątpienia potrzebowały impulsów do wprowadzania efektywnych zmian w swoich procedurach i narzędziach ochrony danych osobowych. Samorząd terytorialny w Polsce wykonuje różnorodne zadania i z tego powodu przetwarza szerokie spektrum danych osobowych. Bardzo istotne jest, aby duża liczba zadań nie przeszkadzała w kształtowaniu adekwatnego systemu ochrony informacji, ze szczególnym uwzględnieniem danych osobowych.

Inny wniosek dotyczy specyficznego aspektu ujednolicenia systemu ochrony danych osobowych. Zbliżone lub jednolite wymogi wobec podmiotów przetwarzających dane osobowe mogą przyczynić się do rozwoju współpracy międzynarodowej. Jednostki samorządu terytorialnego mogą czerpać pozytywne wzorce i kopiować dobre praktyki nie tylko w wymiarze krajowym, ale również z innych państw Unii Europejskiej (np. wykorzystując doświadczenia miast partnerskich).

Wśród konkluzji nie może zabraknąć również tej dotyczącej osoby pełniącej funkcję IOD w każdej jednostce samorządu terytorialnego. Nie ulega wątpliwości, że w największych urzędach i innych jednostkach zatrudniających dużą liczbę pracowników taka osoba jest bardzo potrzebna. Trudno jednak prognozować, że najmniejsze podmioty samorządowe, np. jednoosobowe biblioteki gminne, kiedykolwiek będą miały rzeczywistą potrzebę zatrudniania IOD i nie będzie to dla nich nadmierne obciążenie finansowe, tak jak jest obecnie. Dlatego w tym zakresie najprawdopodobniej będzie konieczna nowelizacja RODO. Być może kolejne lata funkcjonowania systemu będą wiązały się z ujawnieniem innych obszarów deficytowych, w których również będzie należało wprowadzić zmiany.

Warto też sformułować postulat dalszych badań nad ewolucją systemu bezpieczeństwa informacji i ochrony danych osobowych w jednostkach samorządu terytorialnego. Autor nie wyczerpał bowiem zagadnienia, które wymaga dalszych analiz o charakterze interdyscyplinarnym.

22 Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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.U. poz. 730.

Bibliografia

Achatz C., Hubbard S., *US vs. EU Guidelines For De-Identification, Anonymization, and Pseudonymization*, „Journal of Internet Law" 2017, vol. 20, iss. 11.

Bielak-Jomaa E., Drobek P., Krajewska-Kekusz D., Młotkiewicz M., Kawecki M., Soczyński T., Kaczmarek A., Hildebrandt K., *Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych w świetle ogólnego rozporządzenia o ochronie danych*, Warszawa 2016.

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

Kamiński R., *Dochody, wydatki i wyniki budżetowe miast na prawach powiatu. Wybrane aspekty* [w:] *Samorząd miasta na prawach powiatu. Struktury, aktorzy, działanie*, A. Jarosz, B. Springer (red.), Zielona Góra 2019.

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

Rewizorski M., *Podmiotowość prawnomiędzynarodowa Wspólnot Europejskich oraz Unii Europejskiej*, „Środkowoeuropejskie Studia Polityczne" 2011, nr 1.

Siwicki M., *Cyberprzestępczość*, Warszawa 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.), Poznań 2017.

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.), Lublin 2017.

Akty prawne

Karta Praw Podstawowych Unii Europejskiej, Dz.Urz. UE z 2016 r. C 202, s. 389.

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, Dz.Urz. WE L 281, s. 31, ze zm.

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), Dz.Urz. UE L UE L 119, s. 1.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, tekst pierwotny: Dz.U. z 1997 r. Nr 133, poz. 883, ostatni tekst jedn.: Dz.U. z 2016 r. poz. 922 ze zm.

Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych, Dz.U. poz. 869 ze zm.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. poz. 1000 ze zm.

Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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 prze-

pływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. poz. 730.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. Nr 100, poz. 1024.

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji, Dz.U. poz. 745.

Streszczenie

Celem opracowania jest analiza bezpieczeństwa informacji w samorządzie terytorialnym w świetle nowych uregulowań prawnych Unii Europejskiej (RODO). Zmiany w systemie ochrony danych osobowych zakładają centralizację wybranych aspektów przetwarzania i raportowania błędów do centralnych organów nadzorczych. Jednocześnie jednostki samorządu terytorialnego uzyskują samodzielność w doborze środków bezpieczeństwa danych osobowych oraz metodyce przeprowadzania analizy ryzyka. Nowe uregulowania prawne stanowią istotne wyzwanie dla jednostek samorządu terytorialnego. Oprócz zastosowania adekwatnych mechanizmów organizacyjnych i technicznych w zakresie ochrony danych osobowych muszą one także zapewnić właściwy proces podnoszenia kwalifikacji pracowników w tym zakresie.

Słowa kluczowe: bezpieczeństwo informacji, dane osobowe, ochrona danych osobowych, samorząd terytorialny, RODO

Information Security in the Polish Local Government in the Light of the Process of the Unification of the Personal Data Protection System in the European Union

Abstract

The aim of the paper is to analyse information security at the local government level in the light of new EU regulations (GDPR). Changes to the system of personal data protection involve the centralisation of selected aspects of processing and reporting inaccuracies to the central supervision authority. At the same time, local government units gain independence in choosing personal data security measures and methods of conducting risk assessment. New regulations pose a major challenge to local government units which must both apply adequate organisational and technical mechanisms in the fields of personal data protection and appropriately increase their employees' qualifications regarding this matter.

Keywords: information security, personal data, personal data protection, local government, GDPR