Ekspertyzy i opracowania

NARODOWY INSTYTUT SAMORZĄDU TERYTORIALNEGO

Nr 113, 2020

www.nist.gov.pl

Analiza relacji między regulacjami odnoszącymi się do problematyki bezpieczeństwa informacji w jednostce samorządu terytorialnego

dr Krzysztof Świtała,
Wydział Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, Katedra Prawa Informatycznego

Wstęp

Celem ekspertyzy jest przedstawienie relacji instytucji prawnych przewidzianych w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa z innymi, pokrewnymi tematycznie aktami prawnymi, do których należą: ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UKSC), rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (RKRI), 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 (RODO), a także ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (UOIN). Wszystkie te regulacje odnoszą się do zagadnień związanych z problematyką zapewniania bezpieczeństwa informacji w podmiotach publicznych, w tym jednostkach samorządu terytorialnego.

Pojęcie cyberbezpieczeństwa i bezpieczeństwa informacji

Cyberbezpieczeństwo jest terminem prawnym zdefiniowanym w art. 2 pkt 4 UKSC jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. To rozumienie omawianego tu pojęcia odnosi się do rozumienia bezpieczeństwa sieci i systemów informatycznych przedstawionego w art. 4 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS). Implementacją tego aktu w polskim porządku prawnym jest UKSC. Definicje bezpieczeństwa sieci i systemów informatycznych ją w przeważającej mierze tożsame. W kontekście pierwszego terminu ocenie podlega odporność sieci i systemów informatycznych, a nie tylko systemów informacyjnych, na które składają się systemy teleinformatyczne (obejmujące urządzenia informatycznych - tzw. hardware, i oprogramowanie - tzw. software) i przetwarzane w nich dane. W ustawie nie pojawia się wspomniana w dyrektywie przesłanka poziomu zaufania - nadająca wspomnianej odporności charakter względny, uzależniony od ustalonego w konkretnych okolicznościach przekonania o skuteczności przyjętych rozwiązań ochronnych.

Pojęcia cyberbezpieczeństwa w polskim systemie prawnym nie można interpretować w oderwaniu od definicji cyberprzestrzeni, którą odnajdziemy w art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej. Rozumie się przez to przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Możemy zatem mówić o bezpieczeństwie (oznaczającym niezagrożenie, spokój i pewność w określonych okolicznościach) w omawianym obszarze, które rozpatrujemy jako cyberbezpieczeństwo w globalnej sieci przetwarzania zasobów informacyjnych, jaką jest Internet.

Cyberbezpieczeństwo ściśle wiąże się również z pojęciem bezpieczeństwa informacji rozumianego w fundamentalnej dla tej problematyki normie ISO 27000[1] jako zachowanie poufności (właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom), integralności (właściwość zapewnienia dokładności i kompletności zasobów) i dostępności informacji (właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu). Dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność (właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; dotyczy użytkowników, procesów, systemów lub instytucji), rozliczalność (właściwość zapewniająca, że działanie podmiotu może być jednoznacznie tylko jemu przypisane), niezaprzeczalność (właściwość gwarantująca brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie) i niezawodność (właściwość oznaczająca spójne, zamierzone zachowanie i skutki). Omawiany termin odnosi się zatem do atrybutów informacji, których spełnienie gwarantuje jej odpowiednie zabezpieczenie. Warto w tym kontekście zaznaczyć, że bezpieczeństwo coraz częściej jest rozumiane nie jako stan, tylko proces osiągania założonego stopnia pewności co do realizacji wcześniej ustalonych celów[2]. Takie podejście zaproponowano w normach technicznych z rodziny ISO 27001[3] odnoszących się do funkcjonowania systemów zarządzania bezpieczeństwem informacji w organizacjach.

Podsumowując ten wątek rozważań stwierdzić można, że pojęcia cyberbezpieczeństwa i bezpieczeństwa informacji mają ten sam rdzeń znaczeniowy. Odnosi się on do spełnienia atrybutów bezpieczeństwa informacji, których spełnienie pozwala realizować cele organizacji związane z przetwarzaniem podlegających ochronie danych.

1 PN-EN ISO/IEC 27000:2017-06 - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Przegląd i terminologia.

2 Stanisław Koziej, Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja, Bezpieczeństwo narodowe 2/2011, s. 20.

3 PN-EN ISO/IEC 27001:2017-06 - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania.

Obowiązki jednostki samorządu terytorialnego wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Katalog obowiązków podmiotów publicznych, do których na podstawie art. 4 pkt 7 UKSC w związku z art. 9 pkt 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych zaliczamy jednostki samorządu terytorialnego przedstawiono w rozdziale 5 UKSC. Są one zobowiązane do podjęcia następujących działań:

- wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa (art. 21 ust. 1 pkt 1 UKSC);
- zgłaszanie i obsługa incydentu, czyli zdarzenia, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo (art. 22 UKSC);
- informowanie właściwego CSIRT, czyli Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (art. 24 UKSC)

Dodatkowo wspomnieć należy o obowiązku informacyjnym wobec podmiotów .na rzecz których zadanie publiczne jest realizowane. Trzeba w tym przypadku zapewnić dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej. Z założenia takie działania mają zwiększyć świadomość społeczeństwa, co do kluczowych ryzyk związanych z przetwarzaniem informacji w sektorze publicznym.

W przypadku, gdy w stosunku do jednostki samorządu terytorialnego wydana została decyzja o uznaniu za operatora usługi kluczowej, stosuje się do tego podmiotu w pierwszej kolejności przepisy rozdziału 3 UKSC. Rozszerzają one przedstawione powyżej obowiązki podmiotu publicznego o:

- wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej (art. 8 UKSC);
- opracowanie, wdrożenie i aktualizacja dokumentacji cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (art. 10 UKSC);
- powołanie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcie umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (art. 14 UKSC).
- przeprowadzenie co najmniej raz na 2 lata audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (art. 15 ust. 1 UKSC).

Incydenty definiujemy jako zdarzenia, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo (art. 2 pkt 5 UKSC). Dodatkowe wskazówki związane z rozumieniem tego pojęcia dostarcza nam norma ISO 27000 precyzując, że jest to pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Zwraca się tu uwagę na szczególne znaczenie prawdopodobieństwa (będącego miarą zdarzenia losowego) wystąpienia skutku zaburzającego normalne funkcjonowanie procesów przetwarzania informacji w organizacji. W przypadku podmiotu publicznego mówimy o konieczności zarządzania incydentem w podmiocie publicznym (art. 22 ust. 1 pkt 1 UKSC), będącym incydentem, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez ten podmiot (art. 2 pkt 9 UKSC). Operator usługi kluczowej jest zaś zobowiązany do zarządzania incydentem poważnym rozumianym bardzo podobnie, lecz odnoszącym się do poważnego obniżenia jakości lub przerwanie ciągłości świadczenia usługi kluczowej (art. 2 pkt 7 UKSC). Wspomniany tu stopień powagi tego zdarzenia należy rozpatrywać w kontekście treści art. 14 ust. 3 dyrektywy NIS precyzującej, że chodzi tu o istotny wpływ na ciągłość świadczonych usług kluczowych (oceniany z punktu widzenia takich parametrów, jak: liczba użytkowników, których dotyczy zakłócenie usługi kluczowej; czas trwania incydentu, zasięg geograficzny związany z obszarem, którego dotyczy incydent).

Zgodnie z normą ISO 27002[4] celem takich czynności zarządczych w organizacji jest zapewnienie spójnego i skutecznego podejścia do zarządzania incydentami związanymi z bezpieczeństwem informacji, z uwzględnieniem informowania o zdarzeniach i słabościach (podatnościach zasobów i procesów). Działania takie obejmują:

- ustalenie odpowiedzialności i procedur;
- zgłaszanie zdarzeń i słabości;
- ocena i podejmowanie decyzji w sprawie zdarzeń;
- reagowanie na incydenty;
- wyciąganie wniosków z incydentów;
- gromadzenie materiału dowodowego.

Odpowiednio zorganizowany proces zarządzania incydentami pozwala nie tylko skuteczniej usuwać ich skutki, ale także szybko identyfikować i oceniać zaobserwowane anomalie. Dzięki utrwaleniu (poprzez udokumentowanie) podejmowanych czynności można budować w podmiocie bazę wiedzy dotyczącą bezpieczeństwa informacji i będącą jednocześnie instrumentem gromadzenia doświadczeń z tego obszaru.

W przypadku jednostek samorządu terytorialnego incydenty związane z cyberbezpieczeństwem są zgłaszane do Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzonego przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy (CSIRT NASK). Wyjątek stanowią podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym - w takiej sytuacji omawiane zgłoszenie jest przekazywane do Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzonego przez Szefa Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV).

Krajowy System Cyberbezpieczeństwa a rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

Jednostki samorządu terytorialnego na podstawie art. 2 ust. 1 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne są zobowiązane do stosowania tej regulacji. Jej aktem wykonawczym wydanym na podstawie art. 18 rzeczonej ustawy jest rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Na podstawie § 20 ust. 1 RKRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Zgodnie z normą ISO 27000 stanowi on uporządkowane podejście do zarządzania bezpieczeństwem

4 PN-EN ISO/IEC 27002:2017-06 - Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji.

informacji w organizacji dla osiągania przez nią założonych celów biznesowych. System taki obejmuje polityki, procedury, wytyczne oraz związane z nimi zasoby i aktywności, wspólnie zarządzane w ramach organizacji, podejmowane w celu ochrony zasobów informacyjnych organizacji. Tworzenie takich zabezpieczeń jest zaś oparte o wykorzystanie analizy ryzyka i wyznaczenie na tej podstawie poziomu akceptacji ryzyka pozwalającego na efektywne postępowanie i zarządzanie nim.

W katalogu zawartym w § 20 ust. 2 RKRI odnoszącym się do wymagań dla systemu zarządzania bezpieczeństwem informacji dominują wymagania związane z zabezpieczeniami organizacyjnymi:

- polityka bezpieczeństwa i prowadzenie bieżącej dokumentacji dotyczącej bezpieczeństwa informacji (zapisy) - zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.
- organizacja bezpieczeństwa informacji - ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych; ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość; zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.
- zarządzanie zasobami (aktywami) - utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację.
- polityka kontroli dostępu - podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji; bezzwłocznej zmiany uprawnień, w przypadku zmiany osobie zakresu powierzonych zadań.
- bezpieczeństwo zasobów ludzkich i edukacja - zapewnienie szkoleń dla osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, stosowanie środków zapewniających bezpieczeństwo informacji.
- zarządzanie incydentami związanymi z bezpieczeństwem informacji - bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.
- zgodność - zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok; kontrola zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

Zabezpieczenia techniczne służące zapewnianiu odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych (§ 20 ust. 2 pkt 12 RKRI) powinny zaś obejmować:

- dbałość o aktualizację oprogramowania,
- minimalizowanie ryzyka utraty informacji w wyniku awarii,
- ochronę przed błędami, utratą, nieuprawnioną modyfikacją,
- stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
- zapewnienie bezpieczeństwa plików systemowych,
- redukcję ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
- niezwłoczne podejmowanie działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
- kontrolę zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

Dodatkowo § 21 odnosi się do obowiązków związanych z zapewnianiem rozliczalności procesów przetwarzania danych w podmiocie publicznym. Zgodnie z ust. 1 podlega ona wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów teleinformatycznych (tzw. logach).

Zgodnie z art. 15 ust. 6 UKSC operator usługi kluczowej, u którego w danym roku w stosunku do systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej został przeprowadzony przez osoby spełniające warunki określone w ust. 2 pkt 2 tej ustawy audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (mowa tu o RKRI), nie ma obowiązku przeprowadzania audytu przez 2 lata. W normach technicznych odnoszących się audytu pojęcie to jest rozumiane jako systematyczny, niezależny i udokumentowany proces przeprowadzany w celu uzyskania dowodów z kontroli i ich późniejszej oceny, która pozwoli obiektywnie określić zakres, w jakim spełnione są ustalone wcześniej kryteria.

Regulacje krajowych ram interoperacyjności i minimalnych wymagań dla systemów teleinformatycznych w odniesieniu do bezpieczeństwa informacji w jednostkach samorządu terytorialnego mają w praktyce nawet szerszy zakres przedmiotowy niż obowiązki podmiotów publicznych ujęte w UKSC, będąc zatem ich naturalnym uzupełnieniem. W przypadku operatorów usług kluczowych ta ustawa i jej akty wykonawcze stanowią niejako uszczegółowienie norm wynikających z RKRI.

Problematyka cyberbezpieczeństwa w kontekście regulacji 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

Omówienie problematyki relacji norm związanych z cyberbezpieczeństwem i ochroną prywatności osób fizycznych rozpoczniemy od przedstawienia wspólnych cech rozwiązań prawnych chroniących Krajowy System Cyberbezpieczeństwa (UKSC) i czynności przetwarzania danych osobowych (RODO). Podobieństwa te obejmują następujące kwestie:

- podejście oparte na ryzyku;
- prowadzenie dokumentacji przetwarzania zasobów informacyjnych (w tym danych osobowych);
- strukturę organizacyjną odpowiedzialną za zarządzanie bezpieczeństwem zasobów informacyjnych (w tym osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa/ inspektora ochrony danych);
- zgłaszanie i zarządzanie incydentami/naruszeniami;
- proaktywne podejście do zarządzania bezpieczeństwem zasobów informacyjnych (uwzględnianie ochrony danych w fazie projektowania, ciągłe doskonalenie).

Zarządzanie ryzykiem jest jednym z kilku elementów procesu zarządzania bezpieczeństwem systemów teleinformatycznych, których celem jest udzielenie odpowiedzi na następujące pytania:

- co złego może się wydarzyć?
- jakie jest prawdopodobieństwo, że wydarzy się coś złego?
- jakie skutki dla systemu informacyjnego organizacji będą miały te wydarzenia?
- jak i na ile możemy zmniejszyć straty?

Na podstawie norm z rodziny ISO 27000 ryzyko rozpatrujemy jako wpływ niepewności na cele. W kontekście problematyki bezpieczeństwa informacji wiąże się ono z możliwością zaistnienia sytuacji, w której zagrożenia będą wykorzystywały podatności zasobu (aktywa) informacyjnego lub ich grupy, a tym samym będą powodować szkodę dla organizacji Ryzyko jest mierzone jako kombinacja prawdopodobieństwa zdarzenia nieporządanego i jego następstw (konsekwencji). Takie rozumienie tego pojęcia jest tożsame z jego definicją legalną, którą odnajdziemy w art. 2 pkt 12 UKSC. Stosowanie podejścia opartego na ryzyku pozwala dobrać zabezpieczenia chronionych informacji w taki sposób, aby odpowiadały one aktualnym potrzebom w tym obszarze odnoszącym się do specyfiki procesów przetwarzania tych zasobów. W kontekście obowiązków jednostek samorządu terytorialnego w zakresie tej problematyki możemy wyróżnić dwie sytuacje. Jeśli ten podmiot jest operatorem usługi kluczowej to jest on obowiązany na podstawie art. 8 pkt 1 UKSC do prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem. W sytuacji, gdy omawiana przesłanka nie jest spełniona, to w przepisach UKSC nie odnajdziemy wprost wskazanego obowiązku prowadzenia uporządkowanego procesu zarządzania ryzykiem. Jednakże wykładnia norm odnoszących się do zapewniania zarządzania incydentem w podmiocie publicznym (art. 22 ust. 1 pkt 1) i obsługi incydentu (art. 22 ust. 1 pkt 3) zakłada podejmowanie aktywnych działań przeciwdziałających tym negatywnym sytuacjom nie tylko w danym momencie, ale również w przyszłości. Aby osiągnąć ten stan konieczne jest prowadzenie uporządkowanych działań w zakresie postępowania z zaobserwowaną tu niepewnością i do tego celu służy nam właśnie podejście oparte na ryzyku. Dodatkowo w kontekście ochrony prywatności osób fizycznych normy RODO jego zastosowanie wprost przewidują art. 24 ust. 1, art. 25 ust. 1, art. 32 tego aktu odnoszące się do obowiązków administratora danych. W przypadku wystąpienia naruszenia ochrony danych na podstawie art. 33 ust. 1 taki podmiot jest obowiązany do uwzględnienia ryzyka naruszenia praw lub wolności osób fizycznych przy ocenie skutków takiego zdarzenia i wyborze dalszych metod postępowania.

Prowadzenie dokumentacji procesów związanych z zapewnianiem bezpieczeństwa informacji pozwala stosować odnoszące się do niego uporządkowane podejście, jak również pozwala na weryfikację jego skuteczności. Możemy w niej wyodrębnić dokumenty strategiczne, takie jak polityki, tworzące ramy dla podejmowanych działań, i zapisy, które stanowią potwierdzenie realizacji określonych czynności.

Zgodnie z regulacjami odnoszącymi się do przetwarzania danych osobowych związana z tymi procesami dokumentacja powinna obejmować następujące elementy:

- polityki ochrony danych - zgodnie z art. 24 ust. 2 RODO jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki organizacyjne i techniczne stosowane w celu zabezpieczenia danych obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych;
- rejestr czynności przetwarzania - na podstawie art. 30 ust. 1 RODO każdy administrator będący podmiotem

publicznym prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada.

Na podstawie wytycznych z normy ISO 27001 można stwierdzić, że podstawowym celem stosowania polityk ochrony danych osobowych jest wskazanie kierunku zarządzania i wsparcia dla bezpieczeństwa tych zasobów w zgodzie z wymaganiami biznesowymi i odpowiednimi przepisami powszechnie obowiązującymi i innymi regulacjami.

Warto również dodać, że dokumentowanie czynności przetwarzania danych osobowych jest w praktyce przejawem zastosowania podejścia procesowego Wskazuje ono, że organizacje powinny identyfikować swoje działania w celu zapewnienia sobie skutecznego i efektywnego funkcjonowania. Każda czynność realizowana przy użyciu zasobów informacyjnych winna być zarządzana w celu umożliwienia przekształcenia wejść w wyjścia, stosując przy tym zestaw powiązanych ze sobą i współzależnych działań – rozumianych jako proces. Dzięki zastosowaniu takiego podejścia możliwe jest obserwowane realnego funkcjonowania organizacji i sposobu wykorzystania przez nią zasobów, którymi dysponuje, a nie wyłącznie odnoszenie się do ich statycznego katalogu.

Prowadzenie dokumentacji jest w istocie warunkiem sine qua zobiektywizowanej weryfikacji działań określonego podmiotu związanych z zapewnianiem bezpieczeństwa informacji. To na podstawie jej treści możemy porównywać realnie obserwowany stan faktyczny z jego założeniami przedstawionymi w dokumentach strategicznych. Dodatkowo zapisy pozwalają udowodnić podejmowanie wcześniejszych działań kontrolnych i stosowanie określonych reakcji na zidentyfikowane przy tej okazji odchylenia. Ma to kluczowe znaczenie w kontekście możliwości weryfikacji realizacji obowiązków określonego podmiotu w czasie.

Normy odnoszące się do problematyki zapewniania prywatności osób fizycznych odnoszą się również do określonych w nich struktur organizacyjnych związanych z zagwarantowaniem bezpieczeństwa danych osobowych:

- administrator danych (art. 4 pkt 7 RODO) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
- inspektor ochrony danych (art. 37 RODO ust. 1 lit a) - administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy przetwarzania dokonują organ lub podmiot publiczny.
- upoważnienie do przetwarzania danych osobowych (art. 32 ust. 4 RODO) - administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

Zastosowanie odpowiednich ram organizacyjnych umożliwia skuteczniejszą realizację wyznaczonych ról i obowiązków związanych z ochroną danych osobowych, cyberbezpieczeństwem i bezpieczeństwem informacji, a także ułatwia monitorowanie wykonywania tych powinności. W przepisach odnoszących się do Krajowego Systemu Cyberbezpieczeństwa na podmioty publiczne nałożono wyłącznie obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z innymi podmiotami tego systemu. W przypadku operatorów usług kluczowych są one dodatkowo zobowiązane do powołania wewnętrznych struktur odpowiedzialne za cyberbezpieczeństwo lub zawarcia umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa, które we własnym zakresie zapewnią odpowiednie wsparcie merytoryczne.

W ramach unijnej reformy UE ram prawnych ochrony danych osobowych wprowadzono nowe obowiązki notyfikacyjne nałożone na administratorów danych w stosunku do organów nadzorczych (art. 33 ust. 1 RODO) i podmiotów danych (art. 34 RODO). Zgodnie z art. 33 RODO przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

Grupa Robocza art. 29 w 2017 r. wydała dla administratorów wytyczne w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679 (3.10.2017, 17/EN WP250). Ponadto ENISA w swoim dokumencie zawierającym opis metodologii oceny dotkliwości naruszeń danych osobowych określiła następujące kryteria ich oceny[5]:

- Kontekst przetwarzania danych (ang. Data Processing Context) - opisuje rodzaj naruszonych danych wraz z szeregiem czynników związanych z ogólnym kontekstem przetwarzania.

5 Recommendations for a methodology of the assessment of severity of personal data breaches (ENISA 2013), s. 8.

- Łatwość identyfikacji (ang. Ease of Identification) - określa, jak łatwo można wydedukować tożsamość osób na podstawie danych związanych z naruszeniem.
- Okoliczności naruszenia (ang. Circumstances of breach) - odnosi się do konkretnych okoliczności naruszenia, które są związane z rodzajem naruszenia, w tym głównie do utraty bezpieczeństwa naruszonych danych, a także wszelkich powiązanych zamiarów napastników.

Kryteria te rozpatruje się z punktu widzenia zachowania poufności, integralności i dostępności danych osobowych, a także biorąc pod uwagę intencje napastnika.

Informowanie o naruszeniach ochrony danych w podmiocie publicznym ma w istocie węższy zakres przedmiotowy niż obowiązki związane ze zgłaszaniem incydentów cyberbezpieczeństwa na podstawie UKSC. Zdarzenia takie odnoszą się do systemów informacyjnych obejmujących wszystkie systemy teleinformatyczne, wraz z całokształtem przetwarzanych w nich danych w postaci elektronicznej, zaś naruszenia bezpieczeństwa danych osobowych odnoszą się wyłącznie do sytuacji niepożądanych związanych z przetwarzaniem danych osobowych. Dodać należy, że w przypadku naruszeń ochrony danych osobowych mamy 72 godziny od momentu stwierdzenia takiego zdarzenia na jego zgłoszenie do organu nadzorczego, zaś w przypadku incydentów cyberbezpieczeństwa są to tylko 24 godziny.

Zapewnianie cyberbezpieczeństwa a zagadnienie bezpieczeństwa teleinformatycznego z ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

Podmioty publiczne - w tym jednostki samorządu terytorialnego - w ramach swojej działalności przetwarzają informacje niejawne, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania (art. 1 ust. 1 UOIN). Zgodnie z art. 48 ust. 1 UOIN systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego, opierającej się na procedurach audytu, którego podstawą jest przede wszystkim treść dokumentacji bezpieczeństwa systemu teleinformatycznego, obejmująca dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego. Pierwszy z nich zawiera systematyczny opis sposobu zarządzania bezpieczeństwem systemu teleinformatycznego (art. 2 pkt 7 UOIN) i obejmuje wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określa przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo (art. 49 ust. 1 UOIN). Drugi z przytoczonych dokumentów odnosi się zaś do opisu, sposobu i trybu postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz zakres odpowiedzialności użytkowników systemu teleinformatycznego i pracowników mających do niego dostęp (art. 2 pkt 8 UOIN). Dokument procedur bezpiecznej eksploatacji opracowuje się na etapie wdrażania oraz modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym (art. 49 ust. 3 UOIN).

W kontekście struktury organizacyjnej podmiotu kierownik jednostki wyznacza inspektora bezpieczeństwa teleinformatycznego, odpowiedzialnego za weryfikację i bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji (art. 52 ust. 1 pkt 1 UOIN). Administratorem systemu zaś będzie osoba lub zespół osób odpowiedzialnych za funkcjonowanie systemu teleinformatycznego (art. 52 ust. 1 pkt 2 UOIN).

Problematyka cyberbezpieczeństwa w podmiocie publicznym bardzo ściśle wiąże się z zagadnieniem ochrony informacji niejawnych, w przypadku, gdy do ich przetwarzania wykorzystuje się systemy teleinformatyczne. Omówione powyżej rozwiązania ujawniły szereg analogii do instytucji (przede wszystkim w odniesieniu do ról i dokumentacji) przewidzianych w normie ISO 27001 i regulacjach odnoszących się do Krajowego Systemów Cyberbezpieczeństwa.

Podsumowanie

Problematyka zapewniania bezpieczeństwa informacyjnego w jednostkach samorządu terytorialnego jest ujęta w wielu aktach prawnych. W ramach niniejszego opracowania analizie poddano te akty prawne, które dotyczą bezpośrednio procesów przetwarzania informacji w podmiotach publicznych. W odniesieniu do zagadnień bezpieczeństwa informacyjnego, cyberbezpieczeństwa, ochrony danych osobowych i informacji niejawnych w jednostce samorządu terytorialnego możemy odnaleźć następujące wspólne koncepcje związane z podejmowaniem działań w tych obszarach:

- uwzględnianie takich atrybutów bezpieczeństwa informacji jak: poufność, integralność i dostępność,

- podejście procesowe,
- zarządzanie ryzkiem,
- wewnętrzne zorganizowanie struktur odpowiedzialnych z bezpieczeństwo,
- dokumentacja,
- zarządzanie naruszeniami/incydentami.

Bezpieczeństwo informacji jest zatem tematyką przekrojową i niniejsze opracowanie jest próbą przedstawienia najważniejszych regulacji z nią związanych, a odnoszących się do sytuacji prawnej jednostek samorządu terytorialnego.

Narodowy Instytut Samorządu Terytorialnego powstał w 2015 r.
Jest państwową jednostką budżetową podległą MSWiA.
Działa na rzecz dalszej profesjonalizacji samorządu terytorialnego i administracji publicznej.

EKSPERTYZY NIST, ul. Zielona 18, Łódź 90-601
Sekretariat tel. +48 42 633 10 70
e-mail: sekretariat@nist.gov.pl