Zeszyty Naukowe Politechniki Częstochowskiej
Zarządzanie Nr 23 t.1 (2016) s. 104–117
dostępne na: http://www.zim.pcz.pl/znwz

OCENA KOMPARATYWNA POLITYK ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W WYBRANYCH ORGANIZACJACH

Grzegorz Chmielarz

Politechnika Częstochowska
Wydział Zarządzania

Streszczenie: W niniejszym artykule, na bazie kwerendy literaturowej, dokonano zestawienia aktów legislacyjnych w zakresie obowiązku zarządzania bezpieczeństwem informacji, w tym danych osobowych. Następnie, w odniesieniu do wymagań aktów prawnych w tym zakresie, przedstawiono w nim proces tworzenia dokumentacji ochrony danych osobowych, która powinna znaleźć się w jednostkach, gdzie przetwarzane są dane osobowe. Zwrócono uwagę na dostosowanie powyższej dokumentacji do specyfiki danej jednostki organizacyjnej.

W części empirycznej, na podstawie analizy dokumentów zastanych, dokonano porównania polityki bezpieczeństwa wybranej uczelni wyższej z politykami bezpieczeństwa innych jednostek organizacyjnych w tym zakresie. Ocena komparatywna została przeprowadzona według przyjętych kryteriów. Na bazie dokonanej oceny porównawczej zestawiono podobieństwa i różnice w konstrukcji podstawowego elementu dokumentacji danych osobowych.

Słowa kluczowe: ochrona danych osobowych, ochrona informacji, system zarządzania bezpieczeństwem informacji, zarządzanie bezpieczeństwem informacji

DOI: 10.17512/znpcz.2016.3.1.11

Wprowadzenie

Organizacje należy traktować jako systemy otwarte wchodzące w interakcje z otoczeniem. Otoczenie oddziałuje na organizacje przez swoją zmienność, złożoność, współdziałanie sił konkurencyjnych oraz zakłóceń. Organizacje usiłują wpływać na swoje otoczenie poprzez zarządzanie informacją i jej bezpieczeństwem, reakcję strategiczną, fuzje, przejęcia lub zakupy innych firm, sojusze, projektowanie organizacji lub bezpośrednio (Kiełtyka 2002, s. 499). W organizacjach, które nie posiadają wdrożonych standardów pomiaru stopnia i efektywności wykonywanych przez nie zadań, nie może być mowy o prawdziwej ocenie zdolności i wyko-nywalności oraz efektywności ich misji, ich wydajności i produktywności. Bez posiadania odpowiednich kryteriów pomiaru, które stanowić będą bazę tego typu przedsięwzięć, wszelkie procesy, których celem jest szacowanie bezpieczeństwa, jego audyty lub inspekcje, stanowić będą zaledwie ćwiczenie z zakresu marnotrawienia czasu, pieniędzy i zasobów, przyniosą rezultaty w postaci krępujących opinii własnych i spekulacji w miejscu, gdzie powinny znaleźć się obiektywne

analizy, łatwe do obronienia fakty oraz profesjonalne osądy (Sullivant 2016, s. 77-89). Dane, w tym dane osobowe, podobnie jak zasoby ludzkie w organizacji, stanowią ważne aktywa większości współczesnych organizacji. Współczesna organizacja jest jak góra lodowa, w której część wystająca to zasoby materialne, natomiast to, co jest pod lustrem wody, to informacja i wiedza. Straty materialne są widoczne i mierzalne, natomiast straty informacji i wiedzy są bardzo trudne do zauważenia (Kisielnicki 2015, s. 14). Dlatego też kwestia ochrony informacji nie stanowi obowiązku jedynie firmowego działu IT, ale wymaga wdrożenia niezbędnych technologii i procesów ochrony wszelkich danych oraz zapewnienia ich zgodności z odpowiednimi regulacjami prawnymi. Sytuacja, w której dane osobowe zostają ujawnione, oznacza realne niebezpieczeństwo dla nieprzerwanego i sprawnego dalszego funkcjonowania organizacji. Szczególnie istotną kwestią wpływającą na bezpieczeństwo przetwarzania danych jest powszechne wykorzystywanie przez organizacje dostępu do sieci globalnej. Internet oddziałuje na otoczenie rynkowe organizacji od początku swojego powstania, ale obecnie siła i zakres tych zmian jest ogromny. Dynamiczny rozwój nowych funkcjonalności Internetu determinuje po pierwsze – zmiany w otoczeniu, a po drugie – coraz bardziej powszechny dostęp i rosnące zainteresowanie możliwościami wykorzystania Internetu w działalności biznesowej (Jelonek 2013, s. 310-311). Dlatego też, szczególnie w czasach społeczeństwa informacyjnego i ogromnej roli, jaką odgrywają informacje i dane w zarządzaniu nowoczesnymi organizacjami, bardzo istotną kwestią jest zapewnienie bezpieczeństwa danych znajdujących się w repozytoriach organizacji, w tym danych osobowych. Efektywna ochrona danych i informacji powinna przeciwdziałać niepowołanemu dostępowi do nich, ale również umożliwiać kontynuację sprawnego ich wykorzystywania w działalności organizacji. Chociaż kontrola transferu danych może skutkować wzrostem ich podstawowego bezpieczeństwa, często wdrożenie bardzo restrykcyjnych środków ograniczających ich przepływ może mieć duży wpływ na efektywność procesów biznesowych organizacji. Warto zauważyć, że również koncepcja e-admini-stracji zakłada w dużym stopniu wykorzystanie elektronicznych form komunikacji z organizacjami gospodarczymi w kwestiach takich jak: ubezpieczenia społeczne dla osób fizycznych zatrudnionych przez pracodawcę, rozliczania podatku dochodowego od osób prawnych, rozliczanie podatku VAT, proces rejestracji działalności gospodarczej, przekazywanie danych statystycznych do GUS, przekazywanie deklaracji celnych do urzędów celnych, uzyskiwanie pozwoleń i realizacji płatności za korzystanie ze środowiska naturalnego, obsługa zamówień publicznych oraz składanie deklaracji PIT (Chmielarz 2008, s. 25-32). Operacje te, w ogromnej większości związane z przetwarzaniem danych osobowych stanowią duże wyzwanie w odniesieniu do ich zabezpieczenia. Konieczne więc staje się wdrożenie rozwiązań, które zapewnią zrównoważone podejście do kwestii bezpieczeństwa oraz możliwości efektywnego wykorzystania posiadanych danych. Rozwiązanie takie stanowią systemy zarządzania bezpieczeństwem informacji i danych. Zarządzanie bezpieczeństwem danych osobowych stanowi część szerszego zagadnienia związanego z zarządzaniem bezpieczeństwem informacji, które posiada zdecydowanie większy charakter interdyscyplinarny i uwzględnia wielorakie aspekty bezpieczeństwa,

takie jak: teleinformatyczne, fizyczne, osobowe, organizacyjne, prawne, społeczne, psychologiczne oraz kulturowe.

Legislacyjne uwarunkowanie polityki bezpieczeństwa danych osobowych

Organizacje, które w toku prowadzonej przez siebie działalności gospodarczej sprzedają towary lub usługi osobom fizycznym czy też zatrudniają pracowników, stają się administratorami danych osobowych. Oznacza to, że praktycznie każda organizacja objęta jest obowiązkiem prowadzenia dokumentacji wymaganej w tym zakresie. Nawet jeśli pewne organizacje zwolnione są z obowiązku rejestrowania danych osobowych znajdujących się w ich posiadaniu w GIODO, nadal zobowiązane są one do prowadzenia stosownej dokumentacji. W przepisach prawnych dotyczących tej kwestii nie przewidziano żadnych wyjątków. Poniżej zestawiono chronologiczne wyszczególnienie najważniejszych aktów prawnych dotyczących ochrony danych osobowych (http://www.sabi.org.pl/page7.php):

- Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych 95/46/WE;
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 poz. 922);
- 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. 2004 nr 100 poz. 1024, z późn. zm.);
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. 2008 nr 229 poz. 1536);
- Wniosek w sprawie Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) z dnia 25 stycznia 2012 r.;
- Rozporządzenie Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej;
- Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 7 sierpnia 2014 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania (Dz.U. 2014 poz. 1145);
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz.U. 2014 poz. 1934);

- 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. 2015 poz. 745);
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015 poz. 719);
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW;
- 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).

Najważniejszym krajowym aktem prawnym regulującym zasady ochrony danych osobowych jest Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 nr 101 poz. 926), nowelizowana kilkakrotnie, z czego ostatnia nowelizacja miała miejsce 28 czerwca 2016 r. (Dz.U. 2016 poz. 922). Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy 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 danych (Dz. Urz. WE L 281 z 23.11.1995, s. 31, z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, s. 355, z poźń. zm.). Ustawa ta przede wszystkim definiuje, jakie dane osobowe podlegają ochronie, jak również podmioty, które podlegają obowiązkowi ochrony przetwarzanych informacji oraz danych osobowych. Treść ustawy stanowi, że:

- Zarządy organizacji mają obowiązek podjęcia szeregu działań o charakterze organizacyjnym i technicznym w zakresie ochrony przetwarzanych informacji i danych osobowych.
- Ustawę stosuje się do organów państwowych oraz samorządu terytorialnego, a także do innych państwowych i komunalnych jednostek organizacyjnych oraz podmiotów niepaństwowych realizujących zadania publiczne.
- Ustawę stosuje się również do osób fizycznych i prawnych oraz jednostek organizacyjnych niemających osobowości prawnej, które przetwarzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych.
- Ustawę stosuje się do podmiotów, które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczpospolitej Polskiej, nie mają siedziby albo miejsca zamieszkania na terytorium Rzeczpospolitej Polskiej, a przetwarzają dane przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczpospolitej Polskiej.

Obok przepisów ustawy o ochronie danych osobowych omawianą problematykę regulują akty wykonawcze do tej ustawy:
1) 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. 2015 poz. 745). Rozporządzenie to określa tryb i sposób:
- sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania w tym zakresie;
- nadzorowania:
  a) opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną,
  b) przestrzegania zasad określonych w dokumentacji, o której mowa w lit. a.

2) Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z dnia 10 października 2011 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. 2011 nr 225 poz. 1350).
3) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. 2008 nr 229 poz. 1536). Określa ono wzór zgłoszenia zbioru danych do rejestracji GIODO, który stanowi załącznik do rozporządzenia.
4) 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. 2004 nr 100 poz. 1024). Zawiera ono informacje o wymaganej dokumentacji zwanej polityką bezpieczeństwa informacji oraz dokładne wskazówki odnośnie wymagań, jakie muszą spełnić systemy informatyczne przetwarzające dane osobowe. Obejmują one informacje o (art. 32 i 33 ustawy i § 7):
- dacie, od kiedy przetwarza się w zbiorze jej dane osobowe, oraz treści tych danych;
- źródle, z którego pochodzą dane jej dotyczące, chyba że administrator jest obowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej;
- sposobie i zakresie udostępniania jej danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;
- sposobie, w jaki zebrano dane.

5) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. 2004 nr 94 poz. 923).

Innym dokumentem legislacyjnym zawierającym wymagania dotyczące ochrony danych osobowych jest *Kodeks pracy* (k.p.). Artykuł 22 § 1-5 zawiera informa-

cje dotyczące zakresu danych osobowych, jakich może zażądać przedsiębiorca od kandydata do pracy. Jego uzupełnienie stanowi Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 28 maja 1996 r. Ma ono na celu uzupełnienie art. 22 k.p. oraz obowiązku nałożonego na pracodawców zgodnie z art. 94 pkt 9a k.p., tj. obowiązku pracodawcy do prowadzenia dokumentacji w sprawach związanych ze stosunkiem zatrudnienia oraz akt osobowych pracownika.

Dostosowanie wymogów legislacyjnych do charakterystyki organizacji

Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. 2002 nr 101 poz. 926) była pierwszym aktem prawnym wprowadzającym obowiązek stworzenia polityki bezpieczeństwa, która dotyczy określenia celu, strategii i polityki zabezpieczeń systemów informatycznych, w których przetwarzane są dane osobowe. Jest to „dokument wyjściowy", który formalnie rozpoczyna proces zabezpieczania danych osobowych w organizacji. To pierwszy dokument, który musi powstać w organizacji, zostać zaakceptowany przez organ zarządzający. Określa on cele, strategię i politykę zabezpieczenia danych osobowych przetwarzanych w organizacji. Obowiązek posiadania polityki bezpieczeństwa, jak również wytyczne odnośnie jej zawartości są przewidziane w następujących przepisach:

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 nr 133 poz. 883), dalej: u.o.d.o.;
- 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. 2004 nr 100 poz. 1024), dalej: Rozporządzenie w sprawie dokumentacji;
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015 nr 0 poz. 719);
- 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. 2015 nr 0 poz. 745).

Na mocy ustawy o ochronie danych osobowych organ zarządzający organizacji staje się administratorem danych osobowych (ADO), którego podstawowym zadaniem jest przygotowanie dokumentacji ochrony danych osobowych. Zgodnie z obowiązującym prawem polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych są elementem obowiązkowym w każdym podmiocie, który przetwarza dane osobowe (nawet jeżeli nie jest zobowiązany do zgłaszania zbiorów do GIODO). Wymienione dokumenty stanowią minimum dokumentacji (określone w Rozporządzeniu 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), jaka powinna znajdować się w każdej organizacji przetwarzającej dane osobowe. Jednak rodzaj dokumentacji i jej zawartość muszą każdorazowo zostać dostosowane do specyfiki działalności danej organizacji. Przykładowa dokumentacja ochrony danych osobowych może zawierać łącznie następujące dokumenty:

– politykę bezpieczeństwa;
– instrukcję zarządzania systemami informatycznymi;
– ewidencję upoważnień;
– wzory upoważnień;
– wzory sprawozdań ze sprawdzenia oraz planów sprawdzeń (Zegarek 2016).

W dużej liczbie organizacji ich pracownicy wielokrotnie stają przed koniecznością przetwarzania danych osobowych. Legalność i zgodność tych działań z przepisami zapewnia nadanie im odpowiednich uprawnień. Zasady nadawania upoważnień określone zostają w polityce bezpieczeństwa organizacji. Upoważnienie do przetwarzania danych osobowych powinno stanowić odrębny dokument, którego wzór powinien znaleźć się w formie załącznika do polityki bezpieczeństwa. Upoważnienie do przetwarzania danych osobowych jest nadawane każdemu pracownikowi w stosownym zakresie przez administratora danych osobowych. Możliwe jest również nadawanie upoważnień w formie elektronicznej. obowiązek nadawania upoważnień może również zostać przeniesiony z ADO na innego pracownika (np. ABI – administratora bezpieczeństwa informacji czy dział kadr). Wymaga to jednak wyraźnego zaznaczenia w polityce bezpieczeństwa i odbywać się może na mocy oficjalnego umocowania nadanego przez ADO konkretnej osobie.

Dodatkowy załącznik do polityki bezpieczeństwa powinien stanowić rejestr wszystkich zawartych umów powierzenia danych osobowych, ze szczególnym uwzględnieniem umów z podmiotami zewnętrznymi. Brak takiej umowy z podmiotem zewnętrznym, który ma dostęp do prowadzonego przez organizację zbioru, stanowi zagrożenie prawne. Zaletą prowadzenia rejestru jest zachowanie porządku i przejrzystości w temacie umów powierzenia.

Kontrola nad ochroną przetwarzanych danych osobowych jest zadaniem upoważnionego przez ADO administratora bezpieczeństwa informacji. Wytyczne w tym zakresie określone zostały w Rozporządzeniu 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. 2015 poz. 745). Zgodnie z powyższym rozporządzeniem wyróżnia się dwie formy sprawowania kontroli: sprawdzenie oraz rzeczywiste sprawowanie nadzoru. Sprawdzenie to weryfikacja zgodności przetwarzania danych osobowych z przepisami ustawy. W polityce bezpieczeństwa muszą pojawić się odpowiadające wytycznym ww. rozporządzenia zasady przeprowadzania sprawdzeń, ich planowania oraz ich częstotliwość (nie częściej niż raz na kwartał, nie rzadziej niż raz na rok). Samo sprawowanie nadzoru przez ABI obejmuje weryfikację aktualności dokumentacji ochrony danych osobowych oraz badanie zgodności ze stanem faktycznym przewidzianych w dokumentacji środków technicznych i organizacyjnych oraz ogólnych zasad i obowiązków określonych w dokumentacji. Tryb przeprowadzania tych wszyst-

kich działań kontrolnych powinien zostać szczegółowo zdefiniowany w polityce bezpieczeństwa, podobnie jak częstotliwość przeprowadzania danych procedur. Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji ochrony danych osobowych. Wzór protokołu z kontroli lub czynności sprawdzających powinien znaleźć się w polityce bezpieczeństwa.

W Rozporządzeniu 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 (dalej: Rozporządzenie w sprawie dokumentacji), wprost wskazano, że niezbędnym elementem polityki bezpieczeństwa jest wykaz zbiorów danych osobowych. Jednocześnie jednym z najczęstszych błędów popełnianych przez administratorów danych przy tworzeniu polityki bezpieczeństwa jest brak wykazu zbiorów danych osobowych. Brak wyróżnienia zbiorów danych osobowych, które podlegają przetwarzaniu, oznacza brak upoważnień dla pracowników. Trudno również odpowiednio zabezpieczyć poszczególne zbiory danych lub zbadać, czy są one przetwarzane w oparciu o jedną z przesłanek legalności (art. 23 lub 27 u.o.d.o.), jeśli zbiory te nie zostały wyróżnione.

Nowelizacja ustawy o ochronie danych osobowych z roku 2015 wprowadziła nową formę „zgłoszenia" zbiorów danych osobowych. Dotyczy ona tych administratorów danych, którzy zdecydowali się powołać administratora bezpieczeństwa informacji. ABI prowadzi jawny rejestr zbiorów, zawierający opis zbiorów, dotychczas wymagających zgłoszenia do GIODO. Polityka bezpieczeństwa powinna uwzględnić zasady funkcjonowania nowego rozwiązania, jeśli znajduje ono zastosowanie. Wytyczne w tym zakresie można znaleźć w Rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych.

Ocena komparatywna polityk bezpieczeństwa wybranych jednostek organizacyjnych

Na podstawie analizy dokumentów zastanych oraz wywiadu osobistego z pełnomocnikiem ADO ustalono, że dokumentacja ochrony danych osobowych wybranej jednostki szkolnictwa wyższego, która stanowi przedmiot porównania w niniejszym artykule z innymi badanymi organizacjami obejmuje następujące dokumenty:

- *Polityka bezpieczeństwa w zakresie ochrony danych osobowych* w analizowanej uczelni,
- *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych* w analizowanej uczelni,
- zarządzenie rektora uczelni wprowadzające w życie powyższe dokumenty,

– zarządzenie rektora uczelni w sprawie powołania pełnomocnika administratora danych osobowych w analizowanej uczelni.

Dokument *Polityka bezpieczeństwa w zakresie danych osobowych* w analizowanej jednostce szkolnictwa wyższego zawiera następujące elementy:

– *Wprowadzenie do Polityki bezpieczeństwa* – zawierające informacje dotyczące celów zapewnienia bezpieczeństwa informacji oraz zagrożeń, na które narażona jest jednostka przetwarzająca dane osobowe;
– *Podstawa prawna*;
– *Postanowienia ogólne* – dotyczące praktycznych aspektów implementacji *Polityki bezpieczeństwa*;
– *Udostępnianie danych osobowych*;
– *Osoby przetwarzające dane osobowe*;
– *Prawa osób, których dane są przetwarzane*;
– *Budynki, pomieszczenia i części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe*;
– *Zbiory danych osobowych tworzone w jednostce*;
– *Zabezpieczenie danych osobowych*;
– załączniki do *Polityki bezpieczeństwa*, które dotyczą:
  – *Załącznik 1 - Miejsca przetwarzania danych osobowych,*
  – *Załącznik 2 - Wykaz obowiązujących nazw zbiorów danych osobowych przetwarzanych w jednostkach organizacyjnych uczelni,*
  – *Załącznik 3 - Zawartość informacyjna zbiorów,*
  – *Załącznik 4 - Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w uczelni,*
  – *Załącznik 5 - (1) Upoważnienie do przetwarzania danych osobowych,*
    (2) Upoważnienie do przetwarzania danych osobowych – aktualizacja,
    (3) Upoważnienie do przetwarzania danych osobowych – odwołanie.

W celu przeprowadzenia analizy komparatywnej polityki bezpieczeństwa wybranej uczelni wyższej posłużono się dziesięcioma wybranymi dokumentami (dobór losowy) polityk bezpieczeństwa organizacji, które podzielono na następujące grupy:

– uczelnie wyższe – 2 dokumenty,
– szkoły średnie – 2 dokumenty,
– urzędy miasta – 2 dokumenty,
– urzędy gminy – 2 dokumenty,
– przedsiębiorstwo produkcyjno-handlowe – 2 dokumenty.

Badanie przeprowadzono w lipcu 2016 r. Celem badania było ustalenie, jak w odniesieniu do aktów legislacyjnych skonstruowane są polityki bezpieczeństwa heterogenicznych organizacji, w jakim stopniu są one spójne i czy ich zapisy uwarunkowane są rodzajem prowadzonej przez organizację działalności. Polityka bezpieczeństwa wybranej jednostki szkolnictwa wyższego charakteryzuje się szczegółowymi i kompletnymi zapisami dotyczącymi wszystkich aspektów ochrony

informacji, dlatego zdecydowano, że będzie ona stanowić wzorzec do porównania z innymi dokumentami tego typu. Badanie przeprowadzono na podstawie kwerendy dokumentów zastanych – polityk bezpieczeństwa wybranych organizacji według kryteriów wyszczególnionych w *Tabeli 1*, która zawiera również wyniki porównania elementów składowych polityk bezpieczeństwa wybranych organizacji z porównywaną uczelnią wyższą.

Tabela 1. Zestawienie elementów obecnych w politykach bezpieczeństwa organizacji

Składowe polityki bezpieczeństwa	***Wybrana uczelnia***	Uczelnia 1	Uczelnia 2	Szkoła 1	Szkoła 2	UM 1	UM 2	UG 1	UG 2	Prz. 1	Prz. 2
Wprowadzenie do Polityki bezpieczeństwa / Informacje o zagrożeniach / Cele polityki bezpieczeństwa	***X***	--	X	--	--	--	X	X	--	--	--
Podstawa prawna	***X***	X	X	X	X	X	X	X	X	X	X
Postanowienia ogólne	***X***	X	X	X	X	X	X	X	X	--	X
Udostępnianie danych osobowych	***X***	--	--	X	--	X	--	--	X	--	X
Osoby przetwarzające dane osobowe	***X***	--	X	--	--	--	X	--	X	--	X
Prawa osób, których dane są przetwarzane	***X***	--	--	--	--	X	--	--	--	--	--
Budynki, pomieszczenia i części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe	***X***	X	--	X	X	--	--	X	X	--	X
Zbiory danych osobowych tworzone w jednostce	***X***	X	X	X	X	X	--	X	X	--	X
Zabezpieczenie danych osobowych	***X***	X	--	X	X	X	X	X	X	--	X
Instrukcja postępowania w przypadku naruszenia danych osobowych	***X***	X	X	X	--	X	X	X	X	--	X
Upoważnienia do przetwarzania danych osobowych	***X***	X	X	--	X	--	--	X	X	--	X

Źródło: Opracowanie własne

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. stanowi podstawę opracowania polityki bezpieczeństwa informacji w organizacji, jednak jej ostateczna forma uzależniona jest od specyfiki jednostki przetwarzającej dane osobowe. Rezultaty analizy komparatywnej polityk bezpieczeństwa zestawionych organizacji ukazują różny zakres informacji na temat działań realizowanych w zakresie ochrony przetwarzanych przez nie danych.

W politykach bezpieczeństwa wszystkich porównywanych organizacji zawarta została informacja o podstawie prawnej, która determinuje konieczność utworzenia wspomnianego dokumentu. Mniej niż połowa z nich (4 spośród 10) wyraźnie definiuje w swoich politykach bezpieczeństwa cele wprowadzenia rzeczonego dokumentu. Elementem wyróżniającym wybraną uczelnię wyższą w tym aspekcie jest zawarcie w treści dokumentu opisu zagrożeń mogących mieć w miejsce w procesie przetwarzania danych osobowych. Natomiast większość organizacji (9 spośród 10) zawiera w swoich dokumentach informacje odnośnie praktycznych aspektów aplikacji zapisów dotyczących ochrony danych osobowych, jednak tylko mniej niż połowa z nich (4 spośród 10) określa zasady, na których przetwarzane przez nie dane osobowe mogą zostać udostępniane zarówno wewnątrz organizacji, jak i do podmiotów zewnętrznych. W żadnym z przypadków zasady udostępnienia danych osobowych nie są zdefiniowane w równie kompleksowy sposób, jak ma to miejsce w wybranej jednostce szkolnictwa wyższego. W podobny sposób analizowane organizacje definiują, kto w organizacji przetwarza dane osobowe. Tylko 4 z 10 organizacji posiadają stosowne zapisy w tym zakresie. Należy podkreślić, że w większości przypadków zapisy te odnoszą się jedynie do roli ADO i ABI w tej kwestii. Tylko wybrana uczelnia wyższa w wyczerpujący sposób zawiera w swoim dokumencie polityki bezpieczeństwa informacje o osobach przetwarzających te dane. Dodatkowo tylko polityka bezpieczeństwa analizowanej uczelni zawiera informacje o prawach osób, których dane osobowe są przez nią przetwarzane. Określenie obszaru, w którym są przetwarzane dane osobowe (budynki, pomieszczenia i części pomieszczeń, w których zachodzi przetwarzanie danych osobowych), stanowi zapis polityk bezpieczeństwa 6 spośród 10 porównywanych organizacji, w przypadku 2 z nich informacje takie zostały zawarte w załączniku do rzeczonego dokumentu. Jest to o tyle dziwne, iż wymagania w tym zakresie zostały wyraźnie określone w wytycznych dotyczących opracowywania polityki bezpieczeństwa (Kaczmarek b.r.). W zdecydowanej większości organizacji (8 spośród 10) w ich politykach bezpieczeństwa zawarte zostały informacje o zbiorach danych tworzonych w organizacjach, ich strukturze oraz programach wykorzystywanych do przetwarzania tych danych. Taka sama liczba organizacji (8 spośród 10) określa również w swoich dokumentach, w jaki sposób zabezpieczane są gromadzone dane. Zapisy te dotyczą zarówno sposobów zabezpieczenia danych osobowych w trakcie ich przetwarzania przez systemy informatyczne, jak również zabezpieczenia zbiorów tradycyjnych. W tym przypadku również oznacza to brak zgodności z wymogami rozporządzenia regulującego kwestię zabezpieczeń danych osobowych. W przypadku wybranej uczelni wyższej polityka bezpieczeństwa zawiera również szczegółowe zapisy dotyczące polityki haseł oraz wykonywania kopii zapasowych danych. Dodatkowo w dokumencie tym znajdują się informacje doty-

czące sposobów zabezpieczenia zbiorów danych osobowych w przypadku ich udostępniania poza obszar jednostki. Ponadto w dokumencie tym zawarte zostały precyzyjne informacje odnośnie niszczenia zbędnych zbiorów danych osobowych oraz przewidziane sankcje za niestosowanie się do zapisów stanowiących treść dokumentu. Podobny poziom szczegółowości w tym zakresie prezentuje również polityka bezpieczeństwa drugiej szkoły średniej będącej przedmiotem porównania. Jednak należy zauważyć, że w tym przypadku zapisy te zawarte zostały w rozdziale *Instrukcja zarządzania systemem informatycznym*. W przypadku wybranej uczelni wyższej zapisy te stanowią treść oddzielnego dokumentu, który jeszcze bardziej szczegółowo determinuje zakres i sposób wykorzystania narzędzi informatycznych w przetwarzaniu i ochronie danych osobowych. Analizowane organizacje w zdecydowanej większości (8 spośród 10) posiadają w swoich politykach bezpieczeństwa instrukcje postępowania w przypadku naruszenia danych osobowych, które definiują działania osób, które stwierdzają zaistnienie sytuacji naruszenia ochrony danych osobowych. Upoważnienie do przetwarzania danych osobowych, dołączane do *Polityki bezpieczeństwa* w formie załącznika, stanowi element dokumentacji w przypadku połowy porównywanych organizacji (5 spośród 10), co jest relatywnie niskim wynikiem, zważywszy na fakt, że zgodnie z wytycznymi legislacyjnymi upoważnienie do przetwarzania danych osobowych powinno stanowić odrębny dokument, którego wzór powinien znaleźć się w formie załącznika do *Polityki bezpieczeństwa*, gdyż obecność tego dokumentu zapewnia legalność przetwarzania danych osobowych.

Analiza elementów składowych polityk bezpieczeństwa wybranych organizacji pod kątem rodzaju prowadzonej przez nie działalności pokazuje, że największe podobieństwo w zakresie konstrukcji tego dokumentu nie jest warunkowane samym rodzajem działalności. W przypadku polityki bezpieczeństwa wybranej jednostki szkolnictwa wyższego, większość kryteriów będących jej składowymi znalazło się również w dokumentach Urzędu Gminy 1 oraz Przedsiębiorstwa 2, które zawierają odpowiednio 9 spośród 11 rzeczonych kryteriów. Wartym podkreślenia może być w tym przypadku fakt, że o ile drugi z porównywanych urzędów gmin zanotował zgodność na poziomie 7 spośród 11 kryteriów, o tyle drugie spośród przedsiębiorstw odnotowało tylko zgodność na poziomie 1 spośród 11 kryteriów. Dodatkowo polityka bezpieczeństwa tego przedsiębiorstwa nie zawiera żadnych szczegółowych zapisów, powiela tylko ogólne wytyczne ustawy o ochronie danych osobowych. Sytuacja taka może być spowodowana faktem, że ponieważ posiadanie analizowanego dokumentu stanowi wymóg prawa, część organizacji wychodzi z założenia, że samo przedstawienie podstawy prawnej i nazwanie tak powstałego dokumentu „polityką bezpieczeństwa" wystarcza do spełnienia wymogów ustawowych w tym zakresie. W przypadku pozostałych grup organizacji – ich polityki bezpieczeństwa prezentują wysoki poziom zgodności z dokumentem wybranej uczelni wyższej. W tym odniesieniu polityki bezpieczeństwa obu urzędów miasta wybranych do porównania prezentują zgodność na poziomie 7 z 11 kryteriów każdy, szkół średnich 8 i 6 spośród 11 kryteriów, a uczelni wyższych 6 i 7 spośród 11 kryteriów.

Podsumowanie

Na bazie przeprowadzonej oceny komparatywnej polityki bezpieczeństwa wybranej jednostki szkolnictwa wyższego oraz polityk bezpieczeństwa dziesięciu losowo wybranych organizacji można zauważyć, że forma tych dokumentów nie jest uzależniona od rodzaju prowadzonej przez nie działalności oraz specyfiki samej organizacji w ramach branży, w której ona działa. Większość organizacji będących przedmiotem porównania w niniejszym artykule uzyskała w tym odniesieniu zbliżone rezultaty. Jedynym odstępstwem od tej normy okazała się grupa przedsiębiorstw, gdzie jedno z nich prezentuje bardzo dobrze skonstruowaną politykę bezpieczeństwa, zawierającą bardzo precyzyjne i szczegółowe informacje dotyczące poszczególnych elementów składowych będących przedmiotem analizy, drugie zaś z nich nie ujmuje w swoim dokumencie nic poza podstawą prawną do jego stworzenia. Zauważone w trakcie analizy podobieństwa i różnice będą stanowić przedmiot dalszych badań, m.in. w wywiadzie bezpośrednim przeprowadzonym wśród ABI wskazanych organizacji, określone zostaną wagi składowych polityki bezpieczeństwa oraz mechanizmy i zadania związane z ich realizacją.

Literatura

1. Chmielarz W. (2008), *Stadium rozwoju systemów e-administracji w Polsce*, [w:] Gołuchowski J., Frączkiewicz-Wronka A. (red.), *Technologie wiedzy w zarządzaniu publicznym 2007*, Prace Naukowe Akademii Ekonomicznej w Katowicach, Wydawnictwo Akademii Ekonomicznej w Katowicach, Katowice.
2. Chmielarz W. (2009), *Zaawansowane realizacje e-administracji w Polsce na tle tendencji światowych*, [w:] Frączkiewicz-Wronka A., Gołuchowski J. (red.), *Technologie wiedzy w zarządzaniu publicznym 2009*, Prace Naukowe Akademii Ekonomicznej w Katowicach, Wydawnictwo Akademii Ekonomicznej w Katowicach, Katowice.
3. http://www.sabi.org.pl/page7.php (dostęp: 06.07.2016).
4. Jelonek D. (2013), *Przestrzeń internetowa w otoczeniu organizacji. Implikacje dla zarządzania strategicznego*, „Prace Naukowe Wałbrzyskiej Wyższej Szkoły Zarządzania i Przedsiębiorczości", t. 22(2): *Zarządzanie Strategiczne Quo Vadis?*.
5. Kaczmarek A. (b.r.), *Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa*, GIODO, http://www.giodo.gov.pl/163/id_art/1063/j/pl/ (dostęp: 06.07.2016).
6. Kiełtyka L. (2002), *Komunikacja w zarządzaniu*, Agencja Wydawnicza Placet, Warszawa.
7. Kisielnicki J. (2015), *Technologia informacyjna jako narzędzie wspomagania systemu zarządzania – analiza trendów*, „Problemy Zarządzania", vol. 13, nr 2(52).
8. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. 2015 poz. 719).
9. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. 2015 poz. 745).
10. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz.U. 2008 nr 229 poz. 1536).
11. 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. 2004 nr 100 poz. 1024 z późn. zm.).
12. Sullivant J. (2016), *Building a Corporate Culture of Security. Strategies for Strengthening Organizational Resiliency*, Butterworth-Heinemann, Nashua.
13. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 poz. 922, z późn. zm.).
14. Zegarek P. (2016), *Wzory i szablony dokumentacji ochrony danych osobowych: Polityka bezpieczeństwa*, http://blog-daneosobowe.pl/wzory-i-szablony-dokumentacji-ochrony-danych-osobowych-polityka-bezpieczenstwa/ (dostęp: 08.07.2016).

COMPARATIVE EVALUATION OF INFORMATION SECURITY MANAGEMENT POLICIES IN CHOSEN ORGANIZATIONS

Abstract: In the present paper, on the basis of the literature analysis, the author summarizes legislative acts in the scope of information security management, including personal data management. Then, the process of preparing documents protecting personal data with reference to the requirements of legal regulations has been presented in it. Attention has been paid to adjustment of these documents to the specificity of the given organizational unit. The empirical part includes a comparative evaluation, conducted on the basis of the existing documents, concerning the information security policy of the selected university and other organizational units in this respect. The comparative evaluation has been conduced according to the assumed criteria. On its basis similarities and differences in constructing the basic element of personal data documents have been summarized.

Keywords: information security, information security management, information security management systems, personal data security