Jacek BAJOREK[1]

Instytut Zarządzania Bezpieczeństwem Informacji[2]

jacek.bajorek@izbi.pl

OCHRONA I BEZPIECZEŃSTWO DANYCH OSOBOWYCH W ORGANIZACJI

ABSTRAKT: Obecnie obowiązujące przepisy prawa regulują kwestie dopuszczalności przetwarzania danych osobowych w systemach teleinformatycznych oraz określają odpowiednie poziomy ochrony tych informacji. Zobowiązanym do ochrony danych osobowych, w każdej organizacji przetwarzającej dane osobowe, jest administrator danych osobowych, który może wyznaczyć administratora bezpieczeństwa informacji do realizacji tych zadań.

SŁOWA KLUCZOWE: administrator, bezpieczeństwo, dane osobowe, ochrona, polityka, poufność

PROTECTION AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION IN ORGANIZATION

ABSTRACT: The current laws govern the admissibility of the personal data processing in ICT systems and determine appropriate levels of protection of such information. Entrusted with the protection of personal data, in any organization processing personal data, is the administrator of personal data, who can determine the information security administrator to carry out these tasks.

KEYWORDS: administrator, confidentiality, personally identifiable information, politics, protection, security

WPROWADZENIE

Celem niniejszego opracowania jest przedstawienie głównego nurtu rozwiązań z zakresu bezpieczeństwa danych osobowych, przetwarzanych przy użyciu systemów informatycznych w administracji, tj. zapewnienia przez organizację odpowiednich procedur i praktyk

[1] Jacek Bajorek – magister, absolwent Wyższej Szkoły Zarządzania. Doświadczony Administrator Bezpieczeństwem Informacji oraz Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z ISO/IEC 27001. Aktualnie pełni funkcję Dyrektora Generalnego w Instytucie Zarządzania Bezpieczeństwem Informacji. Doradza w zakresie Bezpieczeństwa Informacji w instytucjach samorządowych i prowadzi wykłady w zakresie bezpieczeństwa informacji i technologii informacyjnej w Wyższej Uczelni. Posiada *Certified Internal Controls Auditor* (CICA), Certyfikat Audytora Systemu Zarządzania Bezpieczeństwem Informacji zgodne z ISO/IEC 27001, Certyfikat, Certyfikat Administratora Bezpieczeństwa Informacji TUV Hessen oraz dyplom Trenera Certyfikowanego umiejętności miękkich. Autor licznych artykułów prasowych, wykładów i szkoleń z zakresu norm ISO 27001, systemów bezpieczeństwa informacji, oraz zarządzania ryzykiem

[2] Institute of Information Security Management.

niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych oraz zapewnienia dokumentacji i ciągłości doskonalenia zabezpieczeń[3].

Obecnie systemy teleinformatyczne wspomagają działania niemal we wszystkich dziedzinach życia. Są wykorzystywane w każdej instytucji, zarówno dużej organizacji, jak i w małej firmie. Decydują o poziomie rozwoju państwa, a przede wszystkim jakości działania jego struktur organizacyjno-administracyjnych. Nasilenie działań przestępczych, skierowanych na kradzież i nielegalne wykorzystanie informacji w sieciach informatycznych, systematycznie wzrasta, tak jak wzrasta liczba dostępnych usług i wielkość zgromadzonych zasobów informacyjnych[4].

PODSTAWOWE ZASADY TWORZENIA POLITYKI BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

Dokument określający politykę bezpieczeństwa organizacji winien zawierać:

- Mechanizm umożliwiający współużytkowanie informacji,
- Oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji w odniesieniu do strategii i wymagań biznesowych,
- Strukturę wyznaczania celów stosowania zabezpieczeń, w tym strukturę szacowania i zarządzania ryzykiem,
- Krótkie wyjaśnienie polityki bezpieczeństwa, zasad, norm i wymagań zgodności mających szczególne znaczenie dla organizacji,
- Definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania incydentów związanych z bezpieczeństwem informacji.

Odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dotyczących poszczególnych systemów informatycznych lub zalecanych do przestrzegania przez użytkowników zasad bezpieczeństwa[5].

Za realizację polityki bezpieczeństwa ochrony danych osobowych odpowiedzialnymi są administratorzy, natomiast za zadania z zakresu opracowywania i realizacji taktyk odpowiadają administratorzy i użytkownicy Dane osobowe w organizacji są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Agencji na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji[6].

Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada administrator danych osobowych. Kierownicy komórek

[3] PN-ISO/IEC 27001:2007 Polski Komitet Normalizacyjny.
[4] L. Kępa, *Dane osobowe w firmie*, Warszawa 2012, s. 60.
[5] W.R. Wiewiórowski, *Prywatność pacjenta musi być chroniona*, „IT w Administracji" 2/2013, s. 11-12.
[6] L. Kępa, *Ochrona danych osobowych w praktyce*, Warszawa 2011, s. 99-109.

organizacyjnych obowiązani są zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą utratą uszkodzeniem lub zniszczeniem.

Administrator danych może wyznaczyć administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony. Prowadzi on dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych.

Administrator bezpieczeństwa informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, iż wyłącznie autoryzowany personel ma dostęp do systemów informatycznych i tradycyjnych. Ponadto, w uzgodnieniu z kierownikami komórek organizacyjnych, określa warunki oraz sposób przydzielania użytkownikom kont i haseł. Administrator bezpieczeństwa informacji posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.

Polityka bezpieczeństwa definiuje metody zapewniania odpowiednio wysokiego poziomu bezpieczeństwa organizacji w związku z czym nie powinna zawierać szczegółów technicznych, które powinny być zawarte w opisie strategii i taktyk zapewniania bezpieczeństwa organizacji[7].

Każda organizacja ma pewną specyfikę, którą powinna uwzględniać polityka bezpieczeństwa. Bezkrytyczne kopiowanie elementów z polityk innych organizacji jest stanowczo odradzane. Oczywiście można wykorzystać w organizacji te elementy, które mają swoje uzasadnienie wynikające z teorii organizacji i zarządzania[8].

Główne elementy polityki bezpieczeństwa ochrony danych osobowych[9]:

- Określenie osób posiadających uprawnienia do kont w systemie informatycznym, istnienie kont typu „gość", uprawnienia do kont pracowników innych organizacji np. dostawców oprogramowania, konserwatorów oprogramowań itp.
- Określenie liczby osób korzystających z jednego konta (należy pamiętać nie tylko o pracownikach instytucji ale także o ich rodzinach, przyjaciołach itp.).
- Precyzyjne określenie warunków pozbawienia użytkownika prawa do korzystania z konta.
- Zdefiniowanie wymagań dotyczących identyfikowania haseł, przestrzegania ich anonimowości oraz okresów ich ważności.
- Określenie zasad przyłączania i korzystania z globalnej sieci komputerowej oraz określenie osób do tego uprawnionych. Określenie zakresu i zasad udostępniania informacji instytucji użytkownikom globalnej sieci komputerowej (np. przez www czy ftp).

[7] M. Polok, *Zarys prawa Bezpieczeństwo danych osobowych*, Warszawa 2008, s. 90-91.
[8] A. Grzelak, *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości*, Warszawa 2015 s. 56.
[9] L. Kępa, *Dane osobowe…*, *op. cit.*, s. 201.

- Zobligowanie pracowników do wyrażenia zgody na wykonywanie przez administratorów czynności związanych z bezpieczeństwem informacji.
- Określenie zasad korzystania z połączeń modemowych z instytucją; opisanie zasad korzystania z systemu przez osoby znajdujące się w oddaleniu od niego (czy przez sieć globalną czy przez łącza telefoniczne).
- Określenie metod ochrony informacji o finansach i pracownikach organizacji.
- Określenie zasad sporządzania i przechowywania wydruków informacji dotyczących organizacji.
- Konieczność ciągłego dostosowywania polityki bezpieczeństwa do zmieniających się realiów organizacji.

Restrukturyzacja organizacji polegająca na zmianach struktury, wielkości zatrudnienia, systemów informatycznych lub otoczenia (np. rozwój globalnej sieci komputerowej i wzrost liczby związanych z nim zagrożeń) powinny być na bieżąco uwzględniane przy aktualizowaniu polityki bezpieczeństwa. Opracowywanie i realizacja polityki bezpieczeństwa ma ścisły związek ze sposobem zarządzania organizacją. Bezpieczeństwo organizacji zależy od zapewnienia ciągłości zadań w obszarze bezpieczeństwa jak również wymaga zabezpieczenia odpowiednich nakładów finansowych na ewentualne zagrożenia. Brak świadomości kierownictwa organizacji o zagrożeniach i potencjalnych stratach wynikających z procedur regulujących bezpieczeństwo informacji może przyczynić się do nadużyć a nawet przestępstw w obiegu informacji.

ASPEKTY PRAWNE TWORZENIA POLITYKI BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

Kierownictwo organizacji, wdrażając Politykę Bezpieczeństwa ODO wraz z towarzyszącymi jej aktami prawa wewnętrznego, spełniło wymóg ochrony informacji wynikający z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[10] oraz rozporządzenia 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[11], jak również przepisów wynikających z członkostwa w Unii Europejskiej.

Gwarancją sprawnej i skutecznej ochrony informacji jest zapewnienie odpowiedniego poziomu kultury ochrony informacji w Instytucji. Mając powyższe na względzie,

[10] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz. U z 2002 r., nr 101, poz. 926, z późn. zm.

[11] Rozporządzenia 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 z 2004r., nr 100, poz.1024.

wprowadzono Politykę Bezpieczeństwa[12], rozumianą jako zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz organizacji.

Do tworzenia i rozwijania zasad Polityki Bezpieczeństwa wykorzystano obowiązujące w tym zakresie normy i standardy oraz doświadczenia płynące ze sprawdzonych rozwiązań praktycznych. Zasady te są zgodne z obowiązującymi przepisami prawa, nakładającymi obowiązek ochrony określonych rodzajów informacji, w szczególności: tajemnicy danych osobowych, informacji niejawnych, tajemnic przedsiębiorstwa. Celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zabezpieczeń przed nieuprawnionymi zmianami, ujawnieniem nieupoważnionym osobom, zniszczeniem, utratą lub uszkodzeniem pozyskiwanych i przetwarzanych danych[13].

Warunkiem zapewnienia bezpieczeństwa informacji jest zaangażowanie pracowników organizacji w bezpieczeństwo systemów informacyjnych oraz określenie kierunków rozwoju zarządzania bezpieczeństwem tych systemów oraz informacji w nich przetwarzanych, przy jednoczesnym spełnieniu wszelkich wymogów obowiązującego prawa oraz zagwarantowaniu sprawnego funkcjonowania instytucji.

Polityka Bezpieczeństwa uwzględnia uwarunkowania zawarte w Polskiej Normie ISO/IEC 27001. określającej zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji.

Przez bezpieczeństwo informacji należy rozumieć zachowanie poufności, integralności dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności. Wymienione właściwości, wg definicji zawartych w normie polegają odpowiednio PN-ISO/IEC 27001:2007 Polski Komitet Normalizacyjny. Poprzez poszczególne pojęcia należy rozumieć:

- poufność – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
- integralność – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- dostępność – zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
- rozliczalność – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko jednemu podmiotowi,
- autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka jak deklarowana i dotyczy użytkowników, procesów, systemów i informacji,
- niezaprzeczalność – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,

[12] PN-ISO/IEC 27001:2007 Polski Komitet Normalizacyjny.
[13] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U z 2002 r., nr 101, poz. 926.

– niezawodność – zapewnienie spójności oraz gwarancja realizacji zamierzonych zachowań i skutków[14].

Wdrożona w organizacji Polityka Bezpieczeństwa ochrony danych osobowych dotyczy:

– zabezpieczeń fizycznych i bezpieczeństwa środowiska,
– ochrony systemów informatycznych i sieci[15].

BEZPIECZEŃSTWO DANYCH OSOBOWYCH

W organizacji plan ochrony opracowywany jest głównie przez osoby nadzorujące pracę systemów informatycznych. Spisane strategie bezpieczeństwa tworzą dokument zwany planem ochrony. Bieżąca realizacja planu ochrony ciąży zarówno na administratorach, jak i na pozostałych użytkownikach systemu. W planie bezpieczeństwa powinny być zawarte następujące elementy:

– opis realizacji metod kontroli dostępu do systemu,
– opis realizacji metod kontroli dostępu do zasobów systemu,
– opis metod okresowego lub stałego monitorowania systemu,
– dokładny (na poziomie technicznym) opis metod reagowania na wykrycie zagrożenia[16].

Jedna z podstawowych strategii bezpieczeństwa strategii ochrony danych osobowych polega na zapewnianiu bezpieczeństwa przez stosowanie wielowarstwowych mechanizmów ochrony. Strategia ta jest równie oczywista jak zakładanie wielu warstw odzieży w zimne dni. Znany jest fakt, że lepiej założyć dwa cieńsze swetry niż jeden dwa razy grubszy. Analogia ta również odnosi się do systemów ochrony.

Pierwszą linię obrony stanowi ograniczanie fizycznego dostępu do systemu teleinformatycznego. Jest to stosowane w Organizacji poprzez zamykanie komputerów w pomieszczeniach, do których dostęp odbywa się przy uwierzytelnieniu pracownika za pomocą karty magnetycznej. Dodatkowo dostęp do drzwi pomieszczenia jest chroniony przez kolejne punkty wartownicze z pracownikami ochrony. W powyższy sposób chronione są systemy wymagające największego poziomu bezpieczeństwa Serwerownia i Gabinet Prezesa.

Następnym mechanizmem ochrony jest zasada uwierzytelniania pracownika organizacji rozpoczynającego pracę w systemie. Zasada ma na celu ochronę przed nieautoryzowanym dostępem do systemu.

Procedura wykonywana jest z wykorzystaniem haseł, tokenów, podpisu elektronicznego. Procedura zapewniała odpowiedni poziom bezpieczeństwa, hasło ponieważ jest kontrolowane na etapie tworzenia przez administratora. Hasło powinno wykazywać odpowiedni stopień trudności (nie powinno być łatwe), np. powinno się nie dopuszczać haseł, które wywodzą się z nazwy lub opisu użytkownika, są zbyt krótkie, zawierają zbyt mało znaków, były już stosowane, wynikają z kodu klawiatury itp.

[14] M. Polok, *op. cit.*, s. 156-158.
[15] M. Jendra, *Ochrona danych medycznych w 2015*, Warszawa 2015, s. 40.
[16] B. Iwaszko, *Ochrona informacji niejawnych w praktyce*, Wrocław 2012, s. 46.

Kolejną warstwą kontroli trudnością haseł związany jest z faktem, iż pracownicy nie zmieniają haseł (jest to niewygodne) i w związku z tym mają dwa na zmianę. Utrudniając takie działanie użytkownikom, w systemie tworzona jest lista historii haseł. Rozwiązanie takie oczywiście sprawdzi się, jeżeli jest dostatecznie silne ograniczenie na czas używania haseł[17].

Dodatkowo do uwierzytelniania stosowane są metody wykorzystujące inteligentne karty. Karty takie mogą mieć różnorakie postacie; mogą przypominać karty telefoniczne czy tokeny. Do rozpoczęcia działania karty się, konieczne jest podanie przez użytkownika osobistego numeru identyfikacyjnego *Personal Identification Number*. Karty te działają na różnorakie sposoby. Najpopularniejszy to protokół typu wezwanie – odpowiedź. System generuje pewną losową liczbę i podaje ją użytkownikowi. Ten wprowadza ją do karty, która szyfruje liczbę i rezultat szyfrowania zwracany jest do systemu. System sprawdza, czy liczba została zaszyfrowana poprawnie (metoda ta oparta jest na tzw. kryptograficznym protokole uwierzytelniania ze współdzielonym kluczem)[18].

ZADANIA ADMINISTRATORA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH

Zgodnie z treścią Ustawy o ochronie danych osobowych, administrator danych powinien wyznaczyć osobę, zwaną dalej administratorem bezpieczeństwa informacji, odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń[19]. Wymieniony wyżej zakres odpowiedzialności administratora bezpieczeństwa i ochrony danych osobowych sprawia, że do jego głównych obowiązków należy nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe oraz kontrolą przebywających w nich osób, jak również zabezpieczenie ich przed dostępem osób nieposiadających uprawnień do przetwarzania danych osobowych. Osoby nie posiadające takich uprawnień mogą przebywać w nich jedynie w obecności osób uprawnionych. Na czas nieobecności zatrudnionych tam osób, pomieszczenia te powinny być odpowiednio zabezpieczone. W celu zabezpieczenia pomieszczeń należy zastosować odpowiednie zamki do drzwi oraz sprawować właściwy nadzór nad kluczami do tych pomieszczeń.

Zapewnienie awaryjnego zasilania komputerów, serwerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania jest kolejnym zadaniem administratora bezpieczeństwa. Komputery, serwery oraz urządzenia powinny być zasilane poprzez

[17] M. Kluska, G. Wanio, *Ochrona danych osobowych w działach kadr*, Wrocław 2013, s. 99-109.
[18] *Ibidem*, s. 78-81.
[19] B. Iwaszko, *op. cit.*, s. 50-53.

zastosowanie urządzeń podtrzymujących zasilanie[20]. UPS-y powinny być wyposażone w oprogramowanie umożliwiające bezpieczne wyłączenie komputera, serwera lub innego urządzenia. Jest to wyłączenie, w którym przed zanikiem zasilania zostaną prawidłowo zakończone rozpoczęte działanie w ramach pracujących aplikacji i oprogramowania systemowego. Dba również o zagwarantowanie aby urządzenia mobilne, w których przetwarzane są dane osobowe, zabezpieczone były hasłem przed nieautoryzowanym uruchomieniem oraz aby komputery przenośne nie były udostępniane osobom nieupoważnionym do przetwarzania danych osobowych.

Odpowiedzialny jest on także za szkolenie pracowników posiadających urządzenia mobilne z zapisanymi w nich danymi chronionymi. Odbywane szkolenie ma na celu uwrażliwienie na sprzęt, szczególnie podczas transportu, oraz na to, aby urządzenia przenośne przechowywane były we właściwy sposób. Dodatkowo sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe: dyski i inne informatyczne nośniki danych zawierające dane osobowe przeznaczone do likwidacji, należy pozbawić zapisu tych danych, a w przypadku gdy nie jest to możliwe należy uszkodzić w sposób uniemożliwiający ich odczyt, natomiast urządzenia teleinformatyczne przekazywane do serwisu należy pozbawić twardego dysku z danymi osobowymi lub naprawiać w obecności osoby upoważnionej.

Kolejnym jego zadaniem jest zarządzanie hasłami pracowników i nadzór nad stosowaniem procedur określających częstotliwość ich zmiany zgodnie z zasadami, które powinny być zawarte procedurze zarządzania systemem informatycznym służącym do przetwarzania danych, z uwzględnieniem wymogów bezpieczeństwa informacji. Nadzór nad zadaniami związanymi z nadzorowaniem systemu pod kątem obecności wirusów komputerowych, sprawdzeniem wykonywania procedur uaktualniania systemów antywirusowych i ich konfiguracji. Administrator bezpieczeństwa sprawuje nadzór nad wykonywaniem kopii awaryjnych, przechowywaniem oraz okresowym kontrolowaniem pod kątem ich przydatności do odtwarzania danych w przypadku awarii systemu. Sprawuje nadzór nad przeglądami, konserwacją oraz uaktualnieniami systemów służących do przetwarzania danych[21] oraz wszystkich innych czynności wykonywanych w bazach danych. Nadzoruje systemem komunikacji w sieci teleinformatycznej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji.

Administrator bezpieczeństwa sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny. W zakresie nadzoru, o którym mowa wyżej administrator bezpieczeństwa informacji powinien dopilnować, aby osoby zatrudnione przy przetwarzaniu danych osobowych miały dostęp do niszczarki dokumentów w celu niszczenia błędnie utworzonych lub niepotrzebnych już wydruków komputerowych z danymi osobowymi.

[20] L. Kępa, *Ochrona danych… op. cit.*, s. 67-72.
[21] B. Iwaszko, *op. cit.*, s. 35-45

Kolejnym jego zadaniem jest nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do danych osobowych.

Nadzorowanie, o którym mowa wyżej powinno obejmować: ustalenie identyfikatorów użytkowników i ich haseł (identyfikatory użytkowników należy wpisać do ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych[22]) oraz dopilnowanie aby hasła użytkowników były zmieniane co najmniej raz na miesiąc, dopilnowanie aby dostęp do danych osobowych przetwarzanych w systemie był możliwy wyłącznie po podaniu identyfikatora i właściwego hasła, dopilnowanie, aby hasła użytkowników były trzymane w tajemnicy (również po upływie terminu ich ważności), dopilnowanie, aby identyfikatory osób, które utraciły uprawnienia do przetwarzania danych osobowych zastały natychmiast wyrejestrowane, a ich hasła unieważnione[23].

Dopilnowanie, aby jeżeli istnieją odpowiednie możliwości techniczne, ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie się wyłączały po upływie ustalonego czasu nieaktywności użytkownika jest następnym elementem odpowiedzialności administratora bezpieczeństwa. Zalecanym rozwiązaniem powyższego problemu jest zastosowanie takich wygaszaczy ekranowych, które po upływie określonego czasu bezczynności użytkownika wygaszają monitor i jednocześnie uruchamiają blokadę, która uniemożliwia kontynuowanie pracy na komputerze bez podania właściwego hasła. Wygaszasz taki oprócz ochrony danych, które przez dłuższy okres czasu wyświetlane były by na ekranie monitora, chroni system przed przechwyceniem sesji dostępu do danych przez nieuprawnioną osobę[24].

Do jego obowiązków należy również przestrzeganie, aby w pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych były ustawione w taki sposób aby uniemożliwić tym osobom wgląd w dane. Podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego, w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych. Działania, o których mowa wyżej powinny mieć na celu wykrycie przyczyny lub sprawcy zaistniałej sytuacji i jej usunięcie. Szczegółowe zasady postępowania w przypadku naruszeniu zabezpieczeń powinny być określone w instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych[25].

W przypadku, gdy zaistnieje podejrzenie, iż naruszenie bezpieczeństwa danych osobowych spowodowane zostało zaniedbaniem lub naruszeniem dyscypliny pracy, zadaniem administratora bezpieczeństwa informacji powinno być przedstawienie wniosku administratorowi danych

[22] Art. 39 ust. 1 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
[23] J. Barta, R. Markiewicz, P. Fajgielski, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, s. 24-37.
[24] L. Kępa, *Dane osobowe…*, *op. cit.*, s. 181.
[25] A. Krasuski, *Outsourcing danych osobowych w działalności przedsiębiorstw*, Warszawa 2010, s. 44-49.

o wszczęcie postępowania wyjaśniającego i ukaranie odpowiedzialnych za to osób. Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych (jeśli takie wystąpiło) i przygotowanie oraz przedstawienie administratorowi danych odpowiednich takich zmian do instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

Zmiany te powinny być takie, aby pozwalały wyeliminować lub ograniczyć wystąpienie podobnych sytuacji w przyszłości. Obowiązek śledzenia skuteczności zabezpieczeń, o którym mowa wyżej, oraz obowiązek ich udoskonalania, nałożony na administratora bezpieczeństwa, wynika bezpośrednio z obowiązku podejmowania odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń[26].

Wymieniony wyżej katalog odpowiedzialności administratora bezpieczeństwa informacji wskazują jedynie w sposób ogólny zagadnienia dotyczące bezpieczeństwa danych w systemach gdzie są przetwarzane dane osobowe. Niezależnie od wymienionych tam czynności, zadaniem administratora bezpieczeństwa informacji jest śledzenie osiągnięć w dziedzinie zabezpieczania systemów informatycznych w ogóle i wdrażanie takich narzędzi, metod pracy oraz sposobów zarządzania systemem informatycznym, które bezpieczeństwo to wzmocnią. Działania szczegółowe, jakie administrator bezpieczeństwa informacji powinien podejmować w celu realizacji określonych wyżej zadań uzależnione są od:

- architektury systemu informatycznego, w którym dane są przetwarzane,
- zastosowanych narzędzi w ramach oprogramowania systemowego,
- użytych narzędzi do zarządzania bazą danych,
- przyjętych rozwiązań w stosowanych aplikacjach użytkowych.

PODSUMOWANIE

Jak zostało wykazane, stanowisko administratora bezpieczeństwa jest niezbędne w każdej organizacji nie tylko ze względów formalnych, lecz również praktycznych. Skuteczny administrator dba o wysoką jakość ochrony informacji i danych osobowych, co może wpływać na społeczną czy rynkową ocenę danej organizacji.

Sukces we wprowadzaniu bezpieczeństwa informacji w każdej organizacji zależy od wewnętrznego poziomu kultury ochrony informacji. Nawet najlepiej stworzone procedury i regulaminy, czy inwestycje w najnowsze technologie zabezpieczeń systemów informatycznych czy pomieszczeń, nie ochronią informacji, jeżeli kultura ochrony informacji nie będzie priorytetem wśród pracowników organizacji. Kultury przedsiębiorstwa nie tworzy się przez przypadek, jest to wynik wszystkich ludzkich postaw, akceptowanych wartości i norm postępowania, którą tworzą wszyscy pracownicy, to jednak największa odpowiedzialność spoczywa na tych osobach, które rekrutują pracowników i na kadrze zarządzającej organizacją. Jednym z elementów kultury nowoczesnych przedsiębiorstw jest

[26] J. Barta, R. Markiewicz, P. Fajgielski, *op. cit.*, s. 134-137.

Polityka Bezpieczeństwa Informacji wdrażana w ich struktury. Aby jednak ten ambitny cel został osiągnięty, zasady Polityki Bezpieczeństwa Informacji muszą stać się normami przestrzeganymi przez wszystkich pracowników i współpracowników a szczególności zgodnie z literą prawa powinna być w obszarze szczególnego zainteresowania najwyższego kierownictwa.

BIBLIOGRAFIA

Barta Janusz, Markiewicz Ryszard, Fajgielski Paweł. 2011. Ochrona danych osobowych Komentarz. Warszawa: Wolters Kluwer Polska.

Grzelak Agnieszka, 2015. Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości, Warszawa: Oficyna Wydawnicza SGH.

Iwaszko Borys. 2012. Ochrona informacji niejawnych w praktyce, Wrocław: PRESSCOM.

Jendra Mariusz. 2015. Ochrona danych medycznych w 2015. Warszawa: Wiedza i Praktyka.

Kępa Leszek. 2011. Ochrona danych osobowych w praktyce. Warszawa: Difin.

Kępa Leszek. 2012. Dane osobowe w firmie. Warszawa: Difin.

Kluska Michał, Wanio Grzegorz. 2013. Ochrona danych osobowych w działach kadr. Wrocław: PRESSCOM.

Krasuski, Andrzej. 2010. Outsourcing danych osobowych w działalności przedsiębiorstw. Warszawa: LexisNexis.

Polok Mariusz. 2008. Zarys prawa Bezpieczeństwo danych osobowych. Warszawa: CH Beck.

Wiewiórowski, Wojciech Rafał. „Prywatność pacjenta musi być chroniona", IT w Administracji 2/2013 : 11-12.

AKTY PRAWA

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, (Dz. U z 2002r., nr 101, poz. 926 z późn. zm).

Rozporządzenia 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 z 2004r., nr 100, poz.1024.

PN-ISO/IEC 27001:2007, Polski Komitet Normalizacyjny - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji.