L&W

LEŚNY & WSPÓLNICY
KANCELARIA PRAWNA

PROFESJONALIZM, RZETELNOŚĆ, DOŚWIADCZENIE

Bezpieczeństwo Informacji

SPRAWOZDANIE Z AUDYTU

sporządzono dla

Powiat Policki

Audyt Bezpieczeństwa Informacji przeprowadzony dla Starostwa Powiatowego w Policach

WSTĘP

Na podstawie przeprowadzonej analizy ryzyka szczegółowej analizie zostały poddane poszczególne dokumenty niezbędne w realizacji zadania tj.:

Zarządzenie wewnętrzne nr 14/2010 starosty polickiego z dnia 10 września 2010 r. w sprawie wyznaczenia administratora bezpieczeństwa informacji

Zarządzenie wewnętrzne nr 17/2010 starosty polickiego z dnia 10 września 2010 r. w sprawie ustalenia instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w starostwie powiatowym w policach

Zarządzenie wewnętrzne nr 16/2010 starosty polickiego z dnia 10 września 2010 r. w sprawie polityki bezpieczeństwa w starostwie powiatowym w policach

Zarządzenie wewnętrzne nr 15/2010 starosty polickiego z dnia 10 września 2010 r. w sprawie powołania administratora systemu informatycznego

W trakcie realizacji niniejszego zadania podjęto szereg czynności sprawdzających tj.:

- sprawdzenie lokalizacji serwerowni,
- sprawdzenie lokalizacji stanowisk informatyków,
- analizę struktury organizacyjnej Starostwa Powiatowego w Policach przez pryzmat realizacji obowiązków w zakresie obsługi informatycznej.
- szczelność systemu ochrony danych osobowych w Urzędzie,
- praktyczne stosowanie przez pracowników Starostwa Powiatowego w Policach dyspozycji wynikających z obowiązujących instrukcji,
- zgodność zabezpieczeń różnych form przechowywania danych osobowych (elektroniczna i papierowa) z obowiązującym prawem i instrukcjami,

- realizację zadań przez Administratora Bezpieczeństwa Informacji.

W czynnościach zebrania dokumentacji, sprawdzania na miejscu zabezpieczeń , bieżącego wyjaśniania faktycznej realizacji obowiązków w zakresie niniejszego zadania wyznaczonych ustawą oraz wewnętrznymi regulacjami systematycznie uczestniczyły merytorycznie odpowiedzialne za audytowany obszar osoby tj. Pan Adam Sadowski Kierownik Referatu Informatyki Starostwa Powiatowego w Policach, oraz pracownicy odpowiedzialni za przetwarzanie danych osobowych na różnych szczeblach. Przyjęcie określonego programu zadania audytowego zdeterminowało również paletę narzędzi, jakimi posłużono się przy dokonywaniu poszczególnych etapów zadania.

Z uwagi na zakres zadania szczególną uwagę poświęcono instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Policach, zakresom czynności Administratora Bezpieczeństwa Informacji, udzielonym upoważnieniom w zakresie przetwarzania danych osobowych oraz polityce bezpieczeństwa.

W ramach czynności audytorskich odbywały się spotkania z kierownictwem Referatu Informatyki Starostwa Powiatowego w Policach oraz prowadzono intensywną wyminę informacji i dokumentów drogą internetową, pocztową oraz podczas podejmowania czynności audytorskich na miejscu.

Wybór obszaru, z jakiego wywodzi się niniejsze zadanie został poprzedzony przeprowadzeniem analizy ryzyka dla wyodrębnionego zbioru zamkniętego obszarów działalności jednostki samorządu terytorialnego. Celem przeprowadzenia analizy ryzyka dokonano również czynności identyfikacji, wartościowania aktywów, zagrożeń, zabezpieczeń, podatności i następstw z uwagi na uprzedni brak analizy ryzyka w obszarze objętym audytem.

Zakres przedmiotowego zadania określony szczegółowo w programie zadania audytowego wynikał ze zbieżności oczekiwań kierownictwa urzędu z dążeniem

do możliwie efektywnego wykorzystania mechanizmów audytu i znalazł odzwierciedlenie w analizie ryzyka zadania audytowego.

ROZDZIAŁ I

1.OKREŚLENIE OBSZARU AUDYTU

Audyt Bezpieczeństwa Informacji w Starostwie Powiatowym w Policach

2.DATA SPORZĄDZENIA

28 sierpnia 2013 r.

3. NAZWA I ADRES JEDNOSTKI AUDYTOWANEJ

Powiat Policki- Starostwo Powiatowe w Policach

4. AUDYTOR WEWNĘTRZNY

W składzie zespołu audytorskiego działającego pod kierownictwem Michała Pruskiego czynności audytorskie wykonywały następujące osoby:

1. Michał Pruski-Audytor wewnętrzny nr 2037/2006.
2. Marek Nowak- specjalista ds. audytu wewnętrznego.
3. Tomasz Gorczycki- Audytor wewnętrzny.

5. CEL PRZEPROWADZENIA ZADANIA AUDYTOWEGO

Podstawowym celem audytu jest dostarczenie kierownikowi jednostki samorządu terytorialnego – Staroście Powiatowemu w Policach niezależnej informacji, racjonalnego zapewnienia i opinii na temat:

- zasad przetwarzania danych osobowych,
- zabezpieczenia danych osobowych,
- rejestracji zbiorów danych osobowych,
- spełnienia standardów w zakresie bezpieczeństwa sprzętu,

- spełnienia standardów w zakresie zarządzania systemami i sieciami.

6. ZAKRES PRZEDMIOTOWY ZADANIA AUDYTOWEGO

W zakresie podmiotowym, audytem objęte było Starostwo Powiatowe w Policach.

W zakresie przedmiotowym audyt objął:

1. Zgodność wewnętrznych aktów obowiązujących w Starostwie Powiatowym z obowiązującym prawem.
2. Weryfikację i ocenę faktycznej realizacji obowiązujących aktów wewnętrznych w Starostwie Powiatowym w Policach.
3. Wypełnienie dyspozycji ustawowych przez Starostwo Powiatowe w Policach w zakresie zasad przetwarzania danych osobowych.
4. Zgodność realizacji przez Starostwo Powiatowe w Policach dyspozycji normatywnych w zakresie zabezpieczenia danych osobowych.
5. Sprawdzenie realizacji obowiązku zgłaszania do rejestracji przez Starostwo zbiorów danych osobowych.
6. Bezpieczeństwo fizyczne i środowiskowe (na podstawie normy PN-ISO/EC 27001:2007)-analiza występujących incydentów.
7. Zakresy czynności osób odpowiedzialnych za bezpieczeństwo informacji (w tym kwestia zgodnego z prawem rozdziału kompetencji, ewentualnego łączenia funkcji na podstawie normy PN-ISO/EC 27001:2007).
8. Zarządzanie dostępem do systemu.

7. TERMINY, W KTÓRYCH PRZEPROWADZONO AUDYT

Od 1 czerwca do 28 sierpnia 2013 roku.

ROZDZIAŁ II

1. PODJĘTE DZIAŁANIA I ZASTOSOWANE TECHNIKI PRZEPROWADZENIA ZADANIA

Podczas przeprowadzania zadania audytowego wykorzystano następujące techniki i dokumenty robocze audytu:

testy przeglądowe - identyfikacja zasad funkcjonowania badanego systemu i jego podsystemów oraz potwierdzenie istnienia (lub nie) kontroli, poprzez użycie niżej wymienionych technik:

- zapoznanie się z dokumentami służbowymi,
- uzyskanie wyjaśnień i informacji od kierownictwa i pracowników audytowanej jednostki w oparciu o rozmowy, wywiady z pracownikami i dostarczone dokumenty.

testy zgodności - analiza wszystkich zidentyfikowanych procedur w celu oceny stopnia i zakresu ich stosowania, poprzez użycie niżej wymienionych technik:

- porównanie określonych zbiorów danych z kryteriami ustalonymi przez audytorów (na podstawie przepisów prawa),
- sprawdzanie rzetelności informacji oraz jej porównanie z informacją zewnętrzną.

benchmarking (badania porównawcze lub analiza porównawcza) polega na porównywaniu procesów i praktyk stosowanych przez podmioty podobne oraz uważane za najlepsze w analizowanej dziedzinie.

Ponadto uzyskano wyjaśnienia i informacje od Kierownika Referatu Informatyki Starostwa Powiatowego w Policach Administratora Bezpieczeństwa Informacji oraz pracowników merytorycznych odpowiedzialnych za obszar objęty niniejszym zadaniem audytowym.

2. KRYTERIA OCENY STANU FAKTYCZNEGO ORAZ KLASYFIKACJA WYNIKÓW DLA POSZCZEGÓLNYCH KRYTERIÓW.

- Polskie normy regulujące zagadnienia w obszarze objętym zadaniem.
- zasady przetwarzania danych osobowych za kryterium przyjęto regulacje art. 23 do 31 a ustawy o ochronie danych osobowych.
- zabezpieczenie danych osobowych art.36 do 39 a ustawy o ochronie danych osobowych.
- rejestracja zbioru danych osobowych przyjęto art.40 do 46 a ustawy o ochronie danych osobowych.
- Bezpieczeństwo zasobów ludzkich (w tym w szczególności role i zakresy odpowiedzialności pracowników, odpowiedzialność kierownictwa).

3. USTALENIE STANU FAKTYCZNEGO ORAZ JEGO OCENA W ZAKRESIE WYZNACZONYCH KRYTERIÓW

Przedmiot zadania audytowego niejako determinuje jego charakter. Z uwagi na fakt, że zadanie audytowe dotyczy zagadnień bezpieczeństwa informacji w tym również ochrony danych osobowych oraz zagadnień o charakterze formalno-prawnym za właściwe uznano następujące działania.

Ustalenie stanu faktycznego odbyło się poprzez m.in. zapoznanie się z dokumentacją znajdującą się w Starostwie Powiatowym w Policach. W tym przypadku była to dokumentacja, która obejmowała zarówno instrukcje (regulaminy) jak również pisma praktycznie związane z wykonywaniem ustawowych obowiązków w powyższym zakresie w tym również obejmującą ochronę danych osobowych (np. upoważnienia do przetwarzania danych osobowych, karty upoważnień, listy kontrolne, kwestionariusze), dokumentację związaną z rejestracją zbiorów danych osobowych (np. karty zgłoszenia zbiorów danych osobowych), inne dokumenty wynikające z

instrukcji. Nadto w ramach ustalania stanu faktycznego dokonano wizytacji pomieszczeń, w których archiwizowane są dane osobowe zarówno w wersji elektronicznej (pokój informatyków, pokój ABI, serwerownia).

Zostały również zgodnie zadaniem audytowym przygotowane odpowiednie kwestionariusze kontrolne oraz zestawy pytań weryfikujących podejmowane działania faktyczne pod względem zgodności z instrukcją dotyczącą ochrony danych osobowych.

Przeprowadzono też rozmowy z Administratorem Bezpieczeństwa Informacji, pracownikami Referatu Informatyki szczegółowo precyzując faktyczny sposób realizacji poszczególnych zapisów Instrukcji dotyczącej ochrony danych osobowych.

Nadto w doniesieniu do obszaru audytu dotyczącego zgłoszenia danych do zbioru danych osobowych dokonano weryfikacji zgłoszeń poprzez sprawdzenie zarchiwizowanych zbiorów zgłoszeń . W ten sposób dokonane zgłoszenia poddano weryfikacji w oparciu o praktycznie wypracowany zestaw zbioru danych osobowych.

W oparciu o tak wielopłaszczyznowo zebrany materiał faktyczny dokonano oceny stanu faktycznego w oparciu o kryteria przewidziane w ustawie o ochronie danych osobowych, aktach wykonawczych, regulacjach zawartych w polskich normach na bieżąco przywoływanych w sprawozdaniu.

Ocena dotyczyła w pierwszym etapie prawidłowości w dobrze regulacji i mechanizmów funkcjonowania systemu ochrony danych osobowych, a w drugim etapie zgodności działań faktycznych w ramach realizacji obowiązków z zakresu ochrony danych osobowych z przyjętymi rozwiązaniami organizacyjnymi.

W oparciu o wskazane powyżej kryteria będące jednocześnie regulacjami prawnymi dokonano przedmiotowej oceny.

3.1. Zasady przetwarzania danych osobowych.

Zgodnie z art. 26 ustawy o ochronie danych osobowych administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

1) przetwarzane zgodnie z prawem,

2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem ust. 2,

3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje:

1) w celach badań naukowych, dydaktycznych, historycznych lub statystycznych,

2) z zachowaniem przepisów art. 23 i 25.

Przetwarzanie zgodne z prawem

W przypadku niniejszego kryterium stwierdzić należy, iż zgodność z prawem dotyczy przestrzegania zarówno przepisów prawa materialnego, jak i przepisów dotyczących postępowania. Legalność odnosi się do zgodności przetwarzania danych nie tylko z przepisami rangi ustawowej, ale także z normami zawartymi w aktach wykonawczych. Natomiast nie jest objęte omawianą zasadą przetwarzanie naruszające postanowienia umowne.

Omawiane kryterium zabrania m.in. (poza wyjątkowymi przewidzianymi prawem sytuacjami) zbierania danych w sposób ukryty, przez podsłuch, potajemną obserwację, w warunkach naruszenia tajemnicy korespondencji, tajemnicy informacji niejawnych lub zawodowej.

Ustawa polska poprzestaje na kryterium "zgodności z prawem" i nie wprowadza - tak jak dyrektywa 95/46/WE - obok tego "uzupełniającego" warunku "uczciwego", "w dobrej wierze" (*fairly, licitement, nach Treu und Glauben*) przetwarzania danych.[1]

[1] Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Komentarz do art.26 ustawy o ochronie danych osobowych, Lex/el.

W wyroku z dnia 4 marca 2002 r., II SA 3144/01, M. Praw. 2002, nr 8, s. 340, Naczelny Sąd Administracyjny podkreślił, że "żadne względy natury organizacyjno-finansowej nie powinny być traktowane jako podstawy do sprzecznego z prawem przetwarzania danych osobowych przez banki".

W oparciu o niniejsze kryterium stwardzić należy, iż w dużym stopniu jest ono spełnione, gdyż dane w audytowanej jednostce są przetwarzane zgodnie z prawem i dla celów związanych z wykonywaniem zadań przez powiat.

Dokonano więc weryfikacji wewnętrznych regulacji (w tym przypadku Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych oraz Polityki bezpieczeństwa).

§ 3 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 wskazuje, że na dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej "instrukcją".
Dokumentację taką prowadzi się w formie pisemnej i wdrażana jest przez administratora danych.

Przywołane Rozporządzenie w § 4 wskazuje, że polityka bezpieczeństwa powinna zawierać w szczególności:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

4) sposób przepływu danych pomiędzy poszczególnymi systemami;

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Starosta Policki wydal w dniu 10 września 2010 r. Zarządzenie Wewnętrzne nr 16/2010 w sprawie polityki bezpieczeństwa w Starostwie Powiatowym w Policach.

Tak więc na tym etapie analiz będąc w obszarze porównań zgodności wewnętrznych aktów obowiązujących w starostwie z obowiązującym prawem dokonano weryfikacji treści Polityki bezpieczeństwa przyjętej w Starostwie Powiatowym w Policach.

Polityka bezpieczeństwa	
Wymogi Rozporządzenia	Zapisy wewnętrzne jednostki
1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;	Załącznik Nr 1 do Polityki Bezpieczeństwa Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Załącznik Nr 2 do Polityki Bezpieczeństwa Wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	Załącznik Nr 3 do Polityki Bezpieczeństwa Struktury zbiorów danych osobowych.
4) sposób przepływu danych pomiędzy poszczególnymi systemami;	Rozdział VII Sposób przepływu danych pomiędzy poszczególnymi systemami

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.	rozdział IX strategia zabezpieczeń danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych)

W oparciu o przeprowadzaną analizę porównawczą stwierdzić należy, że wprowadzona w Starostwie Powiatowym w Policach polityka bezpieczeństwa reguluje wszystkie obszary wskazane w regulacjach prawnych.

Z kolei § 5 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 wskazuje, że Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania:
   a) elektronicznych nośników informacji zawierających dane osobowe,
   b) kopii zapasowych, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

W kolejnym etapie procesu audytu poddano weryfikacji zgodność zapisów instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w starostwie Powiatowym w Policach.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych	
Wymogi Rozporządzenia	Zapisy wewnętrzne jednostki
procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;	Rozdział I Instrukcji
stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;	Rozdział II Instrukcji
procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;	Rozdział III Instrukcji
procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;	Rozdział IV Instrukcji
sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych, o których mowa w pkt 4,	Rozdział V Instrukcji
sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;	Rozdział VI Instrukcji
sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;	Rozdział VII Instrukcji
procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych	Rozdział VIII Instrukcji

Również w odniesieniu do Instrukcji zarządzania systemem informatycznym w wyniku dokonanej analizy stwierdzić należy zgodność zapisów z obowiązującym regulacjami.

W trakcie czynności audytowych audytor posłużył się również narzędziem ankiety z pytaniami pozwalającej na ustalenie stanu faktycznego.

W ramach tych działań ustalono co następuje.

1.W odniesieniu do funkcjonowania hot-spotu dla mieszkańców.

Hot-spot działa tylko na terenie budynku Starostwa Powiatowego przy ul. Tanowskiej 8.Jest to sieć Wi-Fi umożliwiająca korzystanie z Internetu - oddzielona fizycznie od sieci LAN. Sieć Wi-Fi tworzona jest przy pomocy urządzenia Aruba 200. Urządzenie zlokalizowane jest w serwerowni w piwnicy. Na każdym piętrze zlokalizowane są tzw. access pointy umożliwiające podłączenie się do sieci wifi. Sieć jest szyfrowana, dostęp do sieci następuje po podaniu klucza WPA/PSK, loginu oraz hasła. Dane dostępowe udostępnia osobom zainteresowanym Referat Informatyki. Sieć w większości przypadków wykorzystywana jest przez dziennikarzy obecnych na sesji rady powiatu.

2. Pomieszczenie tzw. serwerowni tj. wyposażenie, zabezpieczenia pomieszczeń i sieciowe, lokalizacja.

Serwerownia zlokalizowana jest w piwnicy (poziom -1) budynku Starostwa Powiatowego przy ul. Tanowskiej 8.Drzwi wzmocnione, 2 zamki, alarm, kraty w oknach, klimatyzacja x2, gaśnica. W przedmiotowym pomieszczeniu znajdują się następujące urządzenia:

1 serwer aplikacji,

1 serwer poczty elektronicznej,

2 serwery klasy blade - na 1 aplikacja SEOD, na 2-gim baza danych SEOD

szafa krosownicza sieci LAN

2 modemy internetowe.

1 Urządzenie typu UTM Fortigate 200B (router, firewall, antywirus, blokowanie stron www)

4 switche sieci LAN

1 centrala telefoniczna

Wszystkie urządzenia podpięte są do UPS-ów (4 szt.)

Sieć komputerowa w Starostwie Powiatowym składa się ze 130 jednostek.

3. Sposób instalacji systemu Finansowo-Księgowego

System FK zainstalowany jest na serwerze znajdującym się w serwerowni. Pracownicy mają dostęp do systemu poprzez aplikację kliencką zainstalowaną

na swojej stacji roboczej. Instalację aplikacji klienckiej w razie potrzeby wykonuje Starszy Informatyk. Dostęp do danych następuje po podaniu loginu i hasła (zmiana co 30 dni). Kopie wykonywane codziennie na inny dysk w macierzy dyskowej serwera oraz na taśmę magnetyczną typu streamer.

4.Opis Elektronicznego Obiegu Dokumentów

System Elektronicznego Obiegu Dokumentów (SEOD) w Starostwie wykorzystywany jest jako POMOCNICZY obieg dokumentów. Główny obieg dokumentów pozostaje papierowy.

1. Pismo od petenta trafia do Kancelarii Ogólnej.
2. Zakładanie tzw. Kontaktu - wprowadzanie danych nadawcy pisma + czego dotyczy sprawa.
3. Skanowanie dokumentu wpływającego i dodawanie do Kontaktu.
4. Pracownik Kancelarii dekretuje pismo na konkretnego naczelnika wydziału lub kierownika biura.
5. Naczelnik lub kierownik dekretuje Kontakt na swojego pracownika, który zajmie się sprawą.
6. Po zakończeniu sprawy pracownik zmienia status sprawy na Zakończony.

Taka sama procedura obowiązuje w lokalizacji na ul. Kresowej (WGN i WGKiK).

W systemie nie ma całego przebiegu realizacji sprawy. Jest tylko rozpoczęcie i zakończenie. Nie ma pełnej dokumentacji sprawy.

Jak się zauważa w literaturze, wymóg zapewnienia merytorycznej poprawności danych osobowych przez administratora wiąże się z obowiązkiem uwzględniania przez niego m.in. następujących okoliczności:

a) znaczenia ewentualnej niedokładności danych z perspektywy osoby, której one dotyczą;

b) oceny wiarygodności źródła pozyskiwania danych;

c) konieczności wypracowania trybu weryfikowania prawdziwości danych w odniesieniu do poszczególnych ich kategorii oraz zasad postępowania w przypadku stwierdzenia nieprawdziwości danych; chodzi tu m.in. o powiadomienie o błędnej informacji osób trzecich, którym dane przekazano (por. S. Singleton, *Data Protection. The New Law*, Bristol 1998, s. 19).

Ustawa wyraźnie wymaga, aby zbierane dane były **adekwatne do celów, w jakich są przetwarzane - zasada adekwatności (relewantności) danych.** Rodzajem i treścią dane nie powinny wykraczać poza potrzeby wynikające z celu ich zbierania. Omawiany wymóg sprzeciwia się też zbieraniu zarówno wszelkich danych dla tego celu nieistotnych, niemających znaczenia, jak i danych o "większym - niż uzasadniony z tego względu - stopniu szczegółowości".[2]

W oparciu o przeprowadzone czynności stwierdzić należy, że niniejszy warunek jest spełniony.

3.3. Zabezpieczenie danych osobowych.

W świetle obecnie obowiązującego prawa zgodnie z treścią art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych minister właściwy do spraw administracji publicznej w porozumieniu z ministrem właściwym do spraw informatyzacji określi, w drodze rozporządzenia, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2, oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.
Niniejszy przepis stanowi delegację ustawową do wydania rozporządzenia.

[2] Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Komentarz do art.26 ustawy o ochronie danych osobowych, Lex/el., op.cit.

Czynnościom audytorskim sprawdzającym poddano zapisy wewnętrznych obowiązujących w urzędzie instrukcji. Na podstawie powyższego poczyniono następujące spostrzeżenia.

§5 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Policach wskazuje, że do obsługi i użytkowania systemu informatycznego dopuszcza się osoby pisemnie upoważnione. Realizacja tego obowiązku następuje poprzez wypełnienie procedury przewidzianej w Rozdziale I Instrukcji.

Odpowiednio więc został określony wzór wniosku o zatrudnienie nowego pracownika (załącznik nr 1).

§ 1 Instrukcji przewiduje również wzór wniosku o udzielenie uprawnień do przetwarzania danych osobowych dla stażysty, praktykanta i wolontariusza.(załącznik nr 2).

Załącznik nr 4 do Instrukcji zawiera wzór decyzji/ upoważnienia do przetwarzania danych osobowych co stanowi wypełnienie dyspozycji art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), po zapoznaniu się z opinią Administratora Bezpieczeństwa Informacji.

Przedmiotowa decyzja zawiera wskazanie zbioru danych osobowych, których upoważnienie będzie dotyczyć nadto zapisy Administratora Bezpieczeństwa Informacji dotyczące wykonania określonych czynności w tym przede wszystkim przewidzianych w § 8 ust. 1 – 8 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Starostwie Powiatowym w Policach oraz zapisy Administratora Bezpieczeństwa Informacji dotyczące realizacji udzielonego upoważnienia.

§ 15 Instrukcji wskazuje, że ABI i główny Specjalista w Wydziale Administracji i Organizacji Starostwa prowadzący sprawy kadrowe prowadzą system elektroniczny ewidencji osób upoważnionych przy przetwarzaniu danych osobowych. Przywołany powyżej przepis zawiera również wskazanie elementów niniejszej ewidencji. Wzór ewidencji jest określony w załączniku nr 8 do Instrukcji.

W toku czynności audytowych dokonano analizy wypełnienia przedmiotowego obowiązku. Obecnie niniejsza procedura nie jest jeszcze wdrożona. Zarówno poszczególne osoby nie posiadają upoważnień do przetwarzania danych osobowych oraz nie ma tym samym ewidencji przedmiotowych upoważnień.

Zgodnie z zapisem § 19 Instrukcji hasło powinno składać się z unikatowego zestawu ośmiu znaków. Taki zapis Instrukcji jest reminescencją przyjętego założenia w §3 Polityki bezpieczeństwa audytowanej jednostki tj.: *„W starostwie z uwagi na fakt, że urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączone są z siecią publiczną, stosuje się wysoki poziom bezpieczeństwa teleinformatycznego."* Należy przywołane powyżej zapisy regulacji wewnętrznych uznać za zasadne z uwagi na zapisy pkt. VIII załącznika do 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, gdzie już w odniesieniu do środków bezpieczeństwa na poziomie podwyższonym przewiduje się środki bezpieczeństwa na poziomie podwyższonym.

Środki bezpieczeństwa na poziomie podwyższonym

W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

Środki bezpieczeństwa na poziomie wysokim

1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. W przypadku zastosowania logicznych zabezpieczeń, o których mowa w ust. 1, obejmują one:

a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

Administrator danych stosuje na poziomie wysokim środki bezpieczeństwa, określone w części A i B załącznika, o ile zasady zawarte w części C nie stanowią inaczej.

Jednocześnie stwierdzić należy, że w wyniku oceny prawidłowości procedury rozpoczęcia, zawieszenia i zakończenia pracy użytkowników końcowych poddano sprawdzeniu realizację zobowiązań zawartych w Instrukcji zarządzania.

Zgodnie z zapisem § 26 ust. 4 Instrukcji Administrator Systemu jest obowiązany do takiego skonfigurowania systemu aby wygaszacz ekranu włączał się po 5 minutach od przerwania pracy, a wznowienie wyświetlania nastąpiło dopiero po wprowadzeniu odpowiedniego hasła.

Dostępy do komputerów są chronione hasłami (6-8 znakowymi). Poustawiane są wygaszacze.

Wejścia do serwerowni są opisane w § 6 strefy bezpieczeństwa. Wejście do serwerowni mają tylko informatycy. Sprzątanie tych pomieszczeń jest możliwe tylko w obecności osób upoważnionych do wejścia.

Zgodnie z zapisem § 28 system informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania
z przetwarzanych informacji.

Uprawnienia, o których mowa w ust.1 , mogą w szczególności obejmować:

1. prawo do odczytu danych,
2. prawo do odczytu wartości statystycznych dla określonej populacji danych.
3. Prawo do modyfikacji istniejących danych,
4. Prawo do usuwania danych,

5. Prawo do przekazywania (przesyłania) danych.

Jeśli aplikacje mają mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji są stosowane. Jednak pracownicy mający do niej dostęp mają pełną kontrolę.

Kolejnym krokiem w czynnościach audytowych było sprawdzenie w oparciu o przyjętą próbę procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania.

Zgodnie § 39 Instrukcji Administrator Systemu jest odpowiedzialny za wykonywanie ustaleń ABI, w zakresie:

1) grafiku tworzenia kopii zapasowych, z uwzględnieniem wymagań w zakresie częstotliwości ich tworzenia,

2) procesu tworzenia kopii zapasowych,

3) procesu weryfikacji poprawności utworzenia kopii zapasowych,

4) okresowego – z częstotliwości uzależnioną od czasu przechowywania kopii – testowania

możliwości odtworzenia danych z kopii zapasowych.

5) zabezpieczenia dostaw nośników wykorzystywanych do tworzenia kopii zapasowych.

6) koordynacji procesu odtwarzania danych w razie wystąpienia awarii.

Natomiast na podstawie § 45 Instrukcji:

1. ASI jest odpowiedzialny za prowadzenie ewidencji nośników użytych do przechowywania kopii zapasowych

2. Zapisy w ewidencji, o której mowa w ust.1, uwzględniają numery ewidencyjne nośników.

są one zapisywane w postaci:

D1/S/T/D2

gdzie:

D1 – dzień utworzenia kopii,

S – oznaczenie systemu, z którego dane zostały zapisane na kopii zapasowej lub zakresu danych,

T - typ kopii zapasowej (pełny, przyrostowy, różnicowy),

D2 - dzień utworzenia kolejnej kopii.

W ramach czynności audytowych ustalono, że osoba pełniąca funkcję ASI nie prowadziła przedmiotowej ewidencji.

W ramach przeprowadzonego procesu audytu kolejnym czynnościom audytowym poddane zostały zagadnienia dotyczące sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych. **Uwzględniono szczególnie zapisy § 47 pkt. 9 Instrukcji dotyczące prowadzenia ewidencji nośników.**

Zgodnie z przywołanym zapisem ASI prowadzi ewidencję nośników przenośnych używanych do zapisu danych osobowych z uwzględnieniem:

1) numeru ewidencyjnego nośnika,

2) rodzaju informacji zapisanych na nośniku,

3) nazwiska lub identyfikatora osoby, na której wniosek zapisano nośnik,

4) nazwiska lub identyfikatora osoby, która pierwotnie zapisała dane na nośniku,

5) daty pierwotnego zapisania danych na nośniku,

6) celu, w jakim dane te zostały zapisane,

7) nazwisk lub identyfikatorów osób, które odczytywały lub modyfikowały dane zapisane

na nośniku, oraz dat, kiedy operacje te miały miejsce,

8) miejsca przechowywania nośnika,

9) adnotacji o zniszczeniu nośnika lub zapisanych na nim danych.

W toku czynności audytowych ustalono, że na chwilę obecną taka ewidencja nie jest prowadzona.

Art. 36. Ust. 1 Ustawy o ochronie danych osobowych stanowi, że administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną,

przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Wymogi zabezpieczenia danych osobowych, o których mowa w art. 36-39 u.o.d.o. odnoszą się zarówno do danych przetwarzanych w sposób tradycyjny (manualny), jak i do danych przetwarzanych w systemach informatycznych.

W zakresie zbiorów przetwarzanych w sposób tradycyjny Generalny Inspektor Ochrony Danych Osobowych zwrócił uwagę na zabezpieczenie przed udostępnianiem osobom trzecim.

Ustawodawca nie podaje, jakie konkretnie środki mają być zastosowane przez administratora danych. Obowiązki administratora wynikają z postawionych mu zadań. Zadania te ujęte są bardzo szeroko i ogólnie: administrator ma - jak zaznaczono w komentowanym przepisie - zapewnić ochronę przetwarzanych danych osobowych. Tak ujęty obowiązek jest następnie uszczegółowiony w ten sposób, że wskazane zostały najistotniejsze zadania polegające na zabezpieczeniu danych przed ich:

a) udostępnieniem osobom nieupoważnionym,
b) zabraniem przez osobę nieuprawnioną,
c) uszkodzeniem,
d) zniszczeniem,
e) zmianą,
f) utratą,
g) przetwarzaniem z naruszeniem ustawy.

Zadania te powinny być zrealizowane przez zastosowanie odpowiednich, należy przez to rozumieć: skutecznych, środków technicznych i organizacyjnych.

Ustawodawca nie przesądza, jak wskazano już powyżej, jakie to mają być środki. Mogą być one różnego rodzaju, od rozwiązań architektoniczno-budowlanych przez systemy alarmowe i służby ochrony aż po środki technicznego i czysto informatycznego charakteru (karty chipowe, kody dostępu, systemy kodujące i przeciwdziałające hakerstwu). Administrator powinien dzięki nim wyeliminować wystąpienie opisanych wyżej szkodliwych zdarzeń, a gdy to niemożliwe - maksymalnie ograniczyć ryzyko ich pojawienia się.

Skuteczność zastosowanych środków powinna podlegać badaniom. Przy stosowaniu zabezpieczeń powinno się też uwzględniać zmieniające się warunki oraz postęp techniczny (informatyczny), co powodować może konieczność zmiany czy modernizowania wprowadzonych wcześniej przez administratora systemów ochrony.

System informatyczny jest zabezpieczony przed udostępnieniem osobom nieupoważnionym poprzez zabezpieczenie komputerów końcowych użytkowników indywidualnymi hasłami dostępu. System posiada również aktualne zabezpieczenie antywirusowe.[3] Nośniki informacji charakteryzują się określoną trwałością. Kopie dokonywane są codziennie i zapisywane na elektronicznych nośnikach informacji. Stosowane jest również wykrywanie i usuwanie wirusów komputerowych, które to czynności kontroluje administrator bezpieczeństwa informacji.

W przypadku zainfekowania wirusem system automatycznie koduje zdarzenia wg. swojego dziennika. Na nośnikach wskazywany jest dzień tygodnia, a po wykonanym back-upie system generuje informację o wykonaniu.

Sposób zabezpieczenia poszczególnych pomieszczeń został określony w załączniku nr 1 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

---

[3] 1. System informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizmy ochrony antywirusowej, o ile:
1) system operacyjny wykorzystywany do przetwarzania danych osobowych lub aplikacje biorące udział w ich przetwarzaniu są narażone na występowanie wirusów,
2) istnieje możliwość wprowadzenia do systemu informatycznego wirusów z zewnątrz – za pośrednictwem sieci informatycznej lub nośników przenośnych.
2. System informatyczny w Starostwie chroniony jest przed działaniem wirusów komputerowych aktualnym oprogramowaniem antywirusowym aktualizowanym na bieżąco.
3. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych przez ASI.
4. Oprogramowanie, o którym mowa w ust. 3, sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.
5. Niezależnie od nadzoru, o którym mowa w ust. 4, ASI nie rzadziej niż raz na tydzień przeprowadza pełną kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach, jak również w serwerach i stacjach roboczych.
6. Użytkownik jest obowiązany zawiadomić ASI o pojawiających się komunikatach lub objawach, wskazujących na wystąpienie zagrożenia wywołanego wirusami komputerowymi.
7. W celu przeciwdziałania wirusom i atakom zainfekowanych plików system informatyczny będzie skanowany przez ASI co 24 godziny pod kątem obecności w systemie wirusów i innych zagrożeń.
8. Dostęp do Internetu możliwy jest wyłącznie na tych stacjach roboczych i komputerach przenośnych, które są specjalnie chronione urządzeniem sprzętowym z wbudowanym programem Firewall.

W toku czynności audytowych ustalono, że w odniesieniu do serwerowni zastosowano następujące zabezpieczenia- szafa pancerna, czujka systemu alarmowego.

System obiegu znajduje się na dwóch serwerach. Beck-upy są wykonywane codziennie z systemu FK i kadrowo-płacowego. Zapisy są wykonywane na taśmy z systemu fk i kadrowo-płacowego. Z bestii oraz kadrowo-płacowe beck-upy są wykonywane na dysk i na taśmy.

W trakcie czynności audytowych dokonano wizji pomieszczeń tj. serwerowni, pokoju informatyków, pomieszczeń specjalisty ds. audytu. Stwierdzono brak monitoringu wizualnego. Stosowana jest ochrona fizyczna.

Zgodnie z zapisami art. 36 ustawy o ochronie danych osobowych administrator danych:

- prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.
- wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba, że sam wykonuje te czynności.

Na podstawie przeprowadzonych czynności audytorskich stwierdzić należy, że administrator zastosował właściwe środki techniczne i organizacyjne zapewniające ochronę danych osobowych. Pomieszczenia, w których przechowywane są dane osobowe są odpowiednio zabezpieczane w zależności od stopnia ważności danych tj.: szafa zamykana na klucz, czujka systemu alarmowego, identyfikator + hasło, szafa pancerna.

Zgodnie z Art. 37 ustawy o ochronie danych osobowych do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Procedura nadawania uprawnień była już przedmiotem szczegółowych czynności audytorskich w punkcie dotyczącym zabezpieczenia danych osobowych oraz zasad przetwarzania danych osobowych.

Art. 38 ustawy o ochronie danych osobowych stanowi, że administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Zgodnie z Art. 39 ustawy o ochronie danych osobowych administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

1) imię i nazwisko osoby upoważnionej,

2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,

3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

2. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Zapis powyższy odzwierciedla regulację mi.in. § 15 Instrukcji.

W oparciu o przeprowadzone powyżej czynności audytorskie stwierdzić należy, że niniejszy obowiązek nie został dochowany.

Natomiast nowela z dnia 22 stycznia 2004 r. rozciągnęła zakres stosowania tego przepisu także na przetwarzanie danych w zbiorach tradycyjnych (np. kartotekach). Przepis ten ustanawia obowiązki służące w pierwszym rzędzie sprawowaniu kontroli w zakresie wprowadzania i "wyprowadzania" (przekazywania) danych osobowych do i ze zbioru.

I tak, na administratorze danych ciąży obowiązek zapewnienia kontroli nad tym:

- jakie dane osobowe,
- kiedy,
- przez kogo

zostały wprowadzone do zbioru oraz

- jakie dane osobowe,
- kiedy,
- komu

zostały ze zbioru przekazane, niezależnie od tego, w jaki sposób nastąpiło przekazanie danych (zrezygnowano tu ze szczególnego podkreślenia tego obowiązku w przypadku przekazywania danych za pomocą urządzeń teletransmisji).

Jak ma być sprawowana powyższa kontrola - ustawa nie rozstrzyga. Dobór służących jej środków pozostawiony został administratorowi danych. Podlegają one jednak kontroli Generalnego Inspektora, jego zastępcy i upoważnionych przez Generalnego Inspektora inspektorów.

Omawiana kontrola ma nie tyle służyć celom ewidencyjno-dokumentacyjnym, co przede wszystkim zapobiegać przypadkom naruszenia przepisów o ochronie danych osobowych i umożliwiać, w razie dokonania naruszenia, wskazanie osoby odpowiedzialnej.

Wydaje się jednak, iż dopełnienie przewidzianego komentowanym przepisem obowiązku w przypadku przetwarzania danych w sposób tradycyjny może w praktyce pociągać za sobą znaczne utrudnienie działalności administratorów danych.

W odniesieniu do przetwarzania danych w systemach informatycznych analizowany obowiązek znajduje swoją konkretyzację w wymogach w zakresie odnotowania gromadzenia i udostępniania danych osobowych, jakie przewidziane zostały w rozporządzeniu wykonawczym do ustawy.

Na podstawie Art. 39a. ustawy minister właściwy do spraw administracji publicznej w porozumieniu z ministrem właściwym do spraw informatyzacji określi, w drodze rozporządzenia, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2, oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.

Komentowany przepis został dodany do ustawy na mocy noweli z dnia 22 stycznia 2004 r. Delegacja zawarta w tym przepisie zastąpiła upoważnienie ustawowe wyrażone wcześniej w art. 45 pkt 1, który został uchylony.

W wykonaniu delegacji ustawowej Minister Spraw Wewnętrznych i Administracji wydał rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia

i systemy informatyczne służące do przetwarzania danych osobowych. Zastąpiło ono obowiązujące do dnia 30 kwietnia 2004 r. rozporządzenie w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.[4]

Analiza realizacji zapisów 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 przez audytowaną jednostkę.

Uznano za właściwe dokonanie również analizy przyjętych rozwiązań w Starostwie Powiatowym w Policach przez pryzmat wskazanych w rozporządzeniu środków bezpieczeństwa.
Kryteria przewidziane w niniejszym obszarze dotyczyły następujących obszarów:

1) sposobu prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
2) podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
3) wymagań w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych.

Na podstawie ww. kryteriów szczegółowo sprecyzowanych w załączniku do rozporządzenia dokonano następujących ustaleń.

Stwierdzić należy, że obszar, o którym mowa w § 4 pkt 1 rozporządzenia tyczący zabezpieczenia przed dostępem osób nieuprawnionych na czas

[4] Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Komentarz do art.39 (a) ustawy o ochronie danych osobowych, Lex/el., op.cit.

nieobecności w nim osób upoważnionych do przetwarzania danych osobowych jest spełniony.

Przebywanie osób nienprawnionych w obszarze, o którym mowa w § 4 pkt 1 rozporządzenia, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

Również w odniesieniu do niniejszego zapisu stwierdzić należy, że w praktycznym wykonywaniu obowiązków przez audytowaną jednostkę niniejszy warunek jest spełniony. Realizacja tego obowiązku została stwierdzona poprzez wizytacje pomieszczeń w toku czynności audytorskich oraz szczegółowe pytania (stwierdzono m.in. zamykanie pokoi, przebywanie osób trzecich w pomieszczeniach zawierających dane osobowe tylko w obecności osób upoważnionych do przetwarzania danych osobowych). System informatyczny służący do przetwarzania danych osobowych zabezpieczony jest, w szczególności przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

Jednocześnie stwierdzono, że w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych. Dostęp do systemu odbywa się poprzez hasło i login i zapewniona jest niepowtarzalność haseł.

Jednocześnie w wyniku przeprowadzonych czynności stwierdzono wypełnienie przez starostwo następujących dyspozycji wynikających z przywołanego rozporządzenia t.j.:

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.

2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.

3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

4. Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;

b) usuwa się niezwłocznie po ustaniu ich użyteczności.

Jednocześnie stwierdzono, że administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.

3.4. Rejestracja zbiorów danych osobowych

Zgodnie z art. 40 ustawy o ochronie danych osobowych administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

W trakcie czynności audytowych ustalono zbiory danych osobowych, jakie zostały zgłoszone do rejestru.

Powiat Policki zgłosił do rejestru następujące zbiory:

1. Rejestr wydanych decyzji o pozwolenie na budowę.
2. Ewidencja gruntów i budynków
3. Rejestr zgłoszonych robót budowlanych
4. Rejestr zgłoszeń zakończonych budów.
5. Rejestr zaświadczeń o samodzielności lokali.
6. Rejestr zgłoszonych rozbiórek i remontów budynków i obiektów budowlanych
7. Rejestr umów
8. Użytkownicy nieruchomości skarbu państwa
9. Rejestr użytkowników wieczystych
10. Rejestracja pojazdów
11. Ewidencja posiadaczy prawa jazdy
12. Wykaz posiadaczy kart rowerowych i motorowerowych.
13. Wykaz posiadaczy świadectw kwalifikacyjnych.

14. Ewidencja radnych powiatu.
15. Rejestr sprzętu pływającego.
16. Rejestr wydanych kart wędkarskich i łowieckich.
17. Rejestr wniosków i wydanych licencji na wykonywanie krajowego drogowego transportu rzeczy i osób.

Jednocześnie należy wskazać, że audytowana jednostka dokonała weryfikacji posiadanych danych osobowych. Zostały one skatalogowane w Załączniku nr 1 do Polityki bezpieczeństwa określonym jako wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe. Podsumowując wyodrębniono 79 takich zbiorów.

Z przeprowadzonej analizy zbiorów zgłoszonych do rejestru przez audytowaną jednostkę wynika, że w 1999 roku zostało zgloszone ww. zbiory i w zasadzie od tego czasu administrator nie zgłaszał innych zbiorów.

Tymczasem zgodnie z art. 40 ustawy administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

Nadto zgodnie z art. 41 ust. 2 ustawy administrator danych jest obowiązany zgłaszać Generalnemu Inspektorowi każdą zmianę informacji, o której mowa w ust. 1, w terminie 30 dni od dnia dokonania zmiany w zbiorze danych, z zastrzeżeniem ust. 3. Z obowiązku rejestracyjnego wyłączone zostały określone, taksatywnie wymienione kategorie zbiorów danych osobowych (art. 43 ust. 1 u.o.d.o.). Są to zbiory danych:

1) zawierających informacje niejawne;
1a) które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności;
2) przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym;
2a) przetwarzanych przez Generalnego Inspektora Informacji Finansowej;
2b) przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym;

3) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego;
4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się;
5) dotyczących osób korzystających z usług administratora świadczonych w sferze medycznej, obsługi notarialnej, adwokackiej lub radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta;
6) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego;
7) dotyczących osób pozbawionych wolności na podstawie ustawy w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności;
8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej;
9) powszechnie dostępnych;
10) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego;
11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

W kontekście analizy realizacji przez jednostkę niniejszego obszaru zwrócić należy również uwagę na regulacje dotyczące momentu rozpoczęcia przetwarzania danych osobowych. Zgodnie z art. 46 ust. 1 ustawy administrator danych może, z zastrzeżeniem ust. 2, rozpocząć ich przetwarzanie w zbiorze danych po zgłoszeniu tego zbioru Generalnemu Inspektorowi, chyba że ustawa zwalnia go z tego obowiązku.

Obowiązek przetwarzania danych w odniesieniu do tzw. danych sensytywnych ustawodawca ukształtował inaczej tj. przewidział możliwości ich przetwarzania w zbiorze danych po zarejestrowaniu zbioru.

Przedmiotowa regulacja określa więc ramy możliwości legalnego przetwarzania danych osobowych.

Zgodnie z nowym brzmieniem komentowanego przepisu warunkiem legalności przetwarzania danych sensytywnych w zbiorze (danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym) jest **zarejestrowanie** zbioru danych. Oznacza to, iż administrator może przetwarzać dane sensytywne w zbiorze dopiero z chwilą dokonania rejestracji zbioru przez Generalnego Inspektora. Konsekwencją zmiany stanu prawnego jest nałożenie na Generalnego Inspektora obowiązku niezwłocznego wydania administratorowi zaświadczenia o zarejestrowaniu takiego zbioru danych.

W odniesieniu do innego rodzaju danych można powiedzieć, że przepis określa moment (czas), od którego **można rozpocząć przetwarzanie danych osobowych** w zbiorze. Ustawa przyjęła ogólną zasadę, iż jest nim już samo zgłoszenie (data zgłoszenia) zbioru do rejestracji. Od zasady tej istnieją wyjątki dotyczące:

1) zbiorów zwolnionych z obowiązku rejestracji,
2) zbiorów istniejących już w chwili wejścia w życie komentowanej ustawy,
3) zbiorów zawierających dane sensytywne.

W przypadku zbiorów zwolnionych z obowiązku rejestracji (na podstawie art. 43 ust. 1 u.o.d.o.) można przyjąć, iż rozpoczęcie przetwarzania danych osobowych związane jest ze spełnieniem ogólnych warunków i zasad, jakie w tej mierze przewidziane są przepisami. W tym przypadku chodzi o spełnienie przesłanek decydujących o legalności takich działań, w tym też wymogów w zakresie

zabezpieczenia danych osobowych - rozdział 5 u.o.d.o. (co potwierdza postanowienie art. 31 ust. 3).[5]

Jednocześnie podczas czynności audytorskich dokonano wizji pomieszczeń, w których przechowywane są serwery danych. Audytor stwierdził, że serwerownia zlokalizowana jest w piwnicach budynku Starostwa Powiatowego w Policach. Nadto bezpośrednio przed wizytą audytora doszło do incydentu zalania pomieszczeń, w których jest zlokalizowany ww. sprzęt. Z pomocą w obiektywizacji zasad przyjść może niewątpliwie 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 (Dz.U.2012.526) odwołujące się w § 20 ust. 3 do takich norm jak PN-ISO/IEC 27001 dotyczącej systemu zarzadzania bezpieczeństwem informacji czy PN-ISO/IEC 27005 dotyczące zarządzania ryzykiem.

§ 20 ust. 3 ww. Rozporządzenia stwierdza, że wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem.

Odwołując się do ustalonego podczas czynności audytowych stanu faktycznego posiłkowo można się odwołać do Załącznika A do Polskiej Normy PN-ISO/IEC 27001, a w szczególności z zakresu Bezpieczeństwa fizycznego i środowiskowego, gdzie w punkcie A.9.1.4. wskazana jest ochrona przed zagrożeniami zewnętrznymi i środowiskowymi, i gdzie jako zabezpieczenie wskazuje się, iż „należy opracować i stosować ochronę fizyczną przed zniszczeniami powstałymi na skutek pożaru, zalania, trzęsienia ziemi, wybuchu.....".

Mając również na uwadze konstrukcję budynku Starostwa Powiatowego w Policach tj. faktu, iż budynki piwnic znajdują się poniżej poziomu gruntu zasadna jest rekomendacja o przeniesieniu pomieszczeń serwerowni na wyższy poziom ww.

[5] Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz, Komentarz do art.46 ustawy o ochronie danych osobowych, Lex/el., op.cit.

budynku lub zastosowania odpowiedniego podwyższenia posadowienia sprzętu celem zabezpieczenia zalaniem.

Rekomendowana zmiana jest szczególnie istotna z uwagi na wysokie ryzyko powtórzenia incydentu w przyszłości biorąc pod uwagę ukształtowanie terenu oraz przyjęte rozwiązania konstrukcyjne budynku Starostwa.

Uzasadnieniem dla niniejszego rozwiązania jest również rekomendacja zawarta w punkcie A.9.2.1. przywołanego już Załącznika A, gdzie jest mowa o lokalizacji i ochronie sprzętu. Jako zabezpieczenie wskazuje się, że sprzęt należy rozlokować lub chronić w taki sposób aby redukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz możliwości nieautoryzowanego dostępu.

Łączenie funkcji ABI i Kierownika Referatu Informatyki Starostwa Powiatowego w Policach

Podczas czynności audytowych stwierdzono również, iż osoba pełniąca obowiązki Kierownika Referatu Informatyki pełni jednocześnie funkcje Administratora Bezpieczeństwa Informacji. Ustalono również, iż zakres obowiązków ABI określony w Polityce Bezpieczeństwa nie ma odzwierciedlenia w zakresie czynności podpisanym i znajdującym się w aktach osobowych osoby wykonującej te czynności.

Należy jednocześnie wskazać, iż w toku czynności audytowych na bieżąco są wprowadzane zalecenia i obecnie przygotowane zostały projekty zakresów czynności dla ABI i ASI.

Zgodnie z art. 36 ust. 3 u.o.d.o. administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.

Cytowany przepis wskazuje jednocześnie na zasadnicze zadanie administratora bezpieczeństwa informacji tj. nadzorowanie przestrzegania zasad określonych w ust.1 art. 36. tj. ochrona danych osobowych, zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub

zniszczeniem.

Jak wskazuje się w doktrynie z nadzorczej funkcji ABI wynika, że pojęcie "nadzór" oznacza kontrolę połączoną z możliwością wiążącego oddziaływania, władczej ingerencji. To z kolei implikuje fakt, że administrator bezpieczeństwa informacji powinien więc mieć zapewnioną możliwość reagowania w sytuacjach zagrożenia czy też naruszenia zasad ochrony danych osobowych.

Wskazuje się również na różne możliwości zatrudniania ABI tj. na podstawie umów o pracę czy umów zlecenia. Z uwagi na nadzorczy charakter działań ABI wskazuje się, że pożądane jest jednak nie łączeniu funkcji związanych z obsługą systemu informatycznego z funkcją ABI.

W praktyce funkcja ABI jest niekiedy łączona ze sprawowaniem innych funkcji np. pełnomocnika ds. informacji niejawnych. Choć formalnie nie ma przeszkód do przyjmowania takiego rozwiązania, jednak niekiedy może prowadzić to do sytuacji, w której ABI będzie musiał nadzorować własne działania. ***Szczególnie wyraźnie widoczne jest to w sytuacji, gdy administratorem bezpieczeństwa informacji jest administrator systemu informatycznego.*** *Z tego względu lepszym rozwiązaniem jest wyznaczanie ABI spośród pracowników, którzy nie są zatrudnieni przy przetwarzaniu danych. W literaturze postuluje się, aby przyznać ABI pozycję niezależną od pionu służb informatycznych i podległość np. bezpośrednio dyrektorowi a nie kierownikowi działu informatyki (A. Drozd, Ustawa o ochronie danych..., s. 253).*

4. Wskazanie słabości kontroli zarządczej oraz analiza ich przyczyn.

W oparciu o ustalenia poczynione na podstawie podjętych działań i zastsowanych technik przeprowadzania zadania, jak również na podstawie przyjętych kryteriów oceny stanu faktycznego oraz klasyfikacji wyników dla poszczególnych kryteriów oraz ustaleń stau faktycznego w zakresie wyznaczonych kryteriów wskazać można na nastęujace słabości kontroli zarządczej w zakresie niniejszego zadania audytowego.

1. Przede wszystkim w obszarze objętym niniejszym zadaniem w zakresie bezpieczeństwa fizycznego i środowiskowego należy wskazać na konieczność zabezpieczenia zasobu sprzętowego znajdującego się w serwerowni. W opinii audytora najlepszym rozwiązaniem byłaby zmiana pomieszczenia z obecnego piwnicznego na wyższy poziom kondygnacji budynku Starostwa. W przypadku, gdyby takie rozwiązanie okazało się zbyt kosztowne proponowane jest umieszczenie serwerów oraz pozostałego sprzętu na podwyższeniu uniemożliwiającym zalanie.
2. Należy uaktualnić listę zgłoszonych do GIODO zbiorów danych osobowych. W zasadzie w ramach wewnętrznych struktur funkcjonowania audytowanej jednostki dokonano weryfikacji przedmiotowych zbiorów w przywołanym już powyżej załączniku nr do Polityki Bezpieczeństwa. Jednak w ślad za tymi działaniami nie dokonano zgłoszeń nowych zbiorów oraz aktualizacji dotychczas zgłoszonych.
3. W opinii audytora należy również rozdzielić obecną wewnętrzną regulację dotyczącą wykonywania przez tą samą osobę funkcji Administratora Bezpieczeństwa Informacji i Kierownika Referatu Informatyki Starostwa Powiatowego. Nadto w opinii audytora z uwagi na audytowany w niniejszym zadaniu obszar należy również dokonać zmian w zakresie podległości służbowej osoby zatrudnionej na stanowisku informatyka w Wydziale Geodezji tak aby osoba ta podlegała pod kierownika Referatu Informatyki. Przyjęcie takiego rozwiązania zapewni centralizację usług informatycznych ich standaryzację, usprawni przepływ informacji, a przede wszystkim zapewni lepszą realizację zadań w zakresie ochrony danych osobowych oraz bezpieczeństwa informacji.
4. Regulacje dot. Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych. W trakcie czynności audytowych stwierdzono, że zarówno Polityka jak i Instrukcja regulują wszystkie obszary wskazane dla tych aktów w obowiązujących regulacjach prawnych (por. str. 14 i 15 sprawozdania).

Jednak dokonana analiza potwierdziła, że w obszarze objętym audytem czynności te nie są faktycznie realizowane (por. punkt następny).

5. W nawiązaniu do punktu powyższego stwierdzić należy, że praktycznie nie są realizowane zapisy § 45 Instrukcji Zarządzania Systemem Informatycznym, gdzie ASI jest odpowiedzialny za prowadzenie ewidencji nośników użytych do przechowywania kopii zapasowych. Tym samym nie jest również realizowany zapis § 47 pkt. 9 Instrukcji również tyczący prowadzenie ewidencji nośników oraz szczegółowych danych określonych w instrukcji dotyczących ewidencji (por. str. 24 sprawozdania).Zgodnie z przywołanym zapisem ASI prowadzi ewidencję nośników przenośnych używanych do zapisu danych osobowych. Brak realizacji przedmiotowych zapisów generuje bardzo duże ryzyko braku kontroli przez ABI, ASI oraz ADO nad zgormadzonymi w nośnikach danymi osobowymi, ich lokalizacją oraz zabezpieczeniem przed nieuprawnionym użyciem, dostępem czy też przetwarzaniem.
6. Brak realizacji obowiązków zakreślonych ustawą o ochronie danych osobowych w zakresie dopuszczenia do przetwarzania danych osobowych jednie osób upoważnionych (por. str. 20 i n. sprawozdania) generuje szereg ryzyk. Pomimo szczegółowo określonych zasad, procedur i załączników dotyczących procedury nadawania uprawnień do przetwarzania danych w zasadzie żaden z tych zapisów Instrukcji nie jest obecnie w audytowanej jednostce realizowany (np. § 1,5,15 Instrukcji). Rekomenduje się więc wdrożenie w audytowanej jednostce Rozdziału I Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych co tym samym umożliwi realizację obowiązków wynikających z art. 37 i n. u.o.d.o.
7. Stwierdzony w toku czynności audytowych brak zakresów czynności ABI i ASI „rozmywa" odpowiedzialność i ostatecznie wprowadza chaos organizacyjny w obszarze objętym audytem. Za słuszne należy uznać co już powyżej w sprawozdaniu zostało ujęte podjęcie w audytowanej jednostce działań polegające na stworzeniu zakresów czynności dla ww. osób. Pomocna w tym zakresie jest również regulacja PN-ISO/EC 27001:2007, gdzie

w załączniku A w pkt. A.10.1.3 w odniesieniu do rozdzielania obowiązków wskazano, że należy rozdzielać obowiązki i zakresy odpowiedzialności w celu ograniczenia możliwości nieuprawnionej lub nieumyślnej modyfikacji lub niewłaściwego użycia aktywów organizacji. Z kolei pkt. A.8.2.1 przywołanej normy w zakresie odpowiedzialności kierownictwa wskazuje, że „kierownictwo powinno wymagać od pracowników, wykonawców oraz użytkowników reprezentujących stronę trzecią stosowania zasad bezpieczeństwa zgodnie z wprowadzonymi w organizacji politykami i procedurami.

8. Również z przyczyn powyżej wskazanych rekomenduje się scentralizowanie usług obsługi informatycznej starostwa i uwzględnienie w strukturze organizacyjnej podległości osoby na stanowisku informatyka w Wydziale Geodezji, Kartografii i Katastru Starostwa Kierownikowi Referatu Informatyki Starostwa Powiatowego w Policach.
9. Również celem wypełnienia dyspozycji art. 40 i 41 ustawy o o.d.o., jak zostało powyżej w sprawozdaniu wskazane należy dokonać aktualizacji zgłoszeń zbiorów danych osobowych (por.str.32 i n. sprawozdania). W zasadzie w trakcie przygotowania Polityki Bezpieczeństwa zostały określone zbiory danych osobowych przez poszczególne komórki organizacyjne Starostwa. Rekomenduje się w toku dalszych czynności weryfikacje niniejszych zbiorów oraz ich zgłoszenie Generalnemu Inspektorowi Danych Osobowych.

Przyczyny zaistniałych powyżej wymienionych sytuacji są różnorakie a poprzestając choćby na jednym przykładzie wynikają z trudności związanych z okolicznościami zewnętrznymi. Tak jest w sytuacji gdy Wydział Geodezji Starostwa znajduje się w innym budynku niż pozostałe referaty. Naturalną wówczas tendencją jest tworzenie się „swoistej autonomii" takiego wydziału. Taka tendencja jednak nie sprzyja efektywnemu kształtowaniu struktury organizacyjnej jednostki i wykonywania zadań z zakresu objętego audytem.

5.Skutki lub ryzyka wynikające ze wskazanych slabości kontroli zarządczej.

W zasadzie można odnieść się do skutków i ryzyk co do każdej z wymienionych słabości kontroli zarządczej. Po części działania takie zostały już poczynione w ramach czynności audytowych i określone w niniejszy sprawozdaniu.
Ta część sprawozdania pozwala na podsumowanie tych działań w obszarze objętym niniejszym zadaniem.

Jeżeli chodzi o określenie stwierdzonych zagrożeń to wskazać należy na następujące.

Ryzyko utraty danych w wyniku zniszczenia sprzętu w odniesieniu do analizowanej kwestii pomieszczenia w serwerowni oraz dotychczasowych incydentów. Polska Norma PN-ISO/EC 27001:2007 definiuje przedmiotowe zagrożenie przed zniszczeniem powstałym na skutek pożaru, zalania, trzęsienia ziemi, wybuchu i innych form naturalnych.

W odniesieniu do wszelkich kwestii dotyczących spraw organizacyjnych tj. zakresów czynności, upoważnień, relacji pomiędzy poszczególnymi referatami w obszarze objętym niniejszym audytem wskazać należy na zagrożenie braku praktycznego stosowania w zakresie objętym audytem dokumentu: Polityki Bezpieczeństwa i Instrukcji. (Polska Norma PN-ISO/EC 27001:2007 – A.5.1.1).
Tym samym brak regularnego przeglądu polityki bezpieczeństwa i jej adekwatności, przydatności i skuteczności. (Polska Norma PN-ISO/EC 27001:2007 – A.5.1.2).
Występuje również:

- brak zgodności roli i zakresów odpowiedzialności pracowników, wykonawców oraz użytkowników z polityką bezpieczeństwa (Polska Norma PN-ISO/EC 27001:2007 – A.8.1.1).
- brak rozdzielenia obowiązków i zakresów odpowiedzialności w celu ograniczenia możliwości nieuprawnionej lub nieumyślnej modyfikacji lub niewłaściwego użycia aktywów jednostki (Polska Norma PN-ISO/EC 27001:2007 – A.10.1.3).

6.Zalecenia w sprawie wyeliminowania słabości kontroli zarządczej.

W sposób szczegółowy rekomendacje co do poszczególnych słabości kontroli zarządczej zostały wykazywane na bieżąco w sprawozdaniu tak więc w niniejszym punkcie zawarte jest ich ogólne podsumowanie, które można ująć w następujących punktach.

- Wdrożenie w audytowanej jednostce Rozdziału I Instrukcji Zarządzania Systemem Informatycznym dotyczącym procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.
- Odpowiednie zmiany w lokalizacji sprzętu serwerowni (rekomendacje jak powyżej).
- Nadanie zakresów czynności dla Administratora Systemu Informatycznego oraz Administratora Bezpieczeństwa Informacji.
- Scentralizowanie obsługi informatycznej jednostki poprzez podporządkowanie osoby na stanowisku informatyka w Wydziale Geodezji, Kartografii i Katastru Starostwa Kierownikowi Referatu Informatyki Starostwa Powiatowego w Policach.
- Aktualizacja zgłoszonych i zgłoszenie nowych zbiorów danych osobowych Generalnemu Inspektorowi Danych Osobowych.

7. Opinia audytora wewnętrznego w sprawie adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze ryzyka objętym zadaniem zapewniającym.

W toku realizacji przedmiotowego zadania audytowego stwierdzono bardzo szybką reakcją kierownictwa na zgłaszane obszary potencjalnych ryzyk związanych z przetwarzaniem danych osobowych w Starostwie Powiatowym w Policach (np. sprecyzowanie zakresów czynności, podjęcie wstępnych czynności zmierzających do wdrożenia procedur).

Nadto należy wskazać na dysponowanie przez audytowaną jednostkę właściwym potencjałem sprzętowym i personalnym umożliwiającym realizację obowiązków

w zakresie ochrony i przetwarzania danych osobowych (zatrudnienie informatyków i ABI, modernizacja sieci informatycznej, stosowanie odpowiednich nośników informacji w zakresie archiwizacji).

Natomiast niezbędne jest jak to już zostało szczegółowo wskazane wprowadzenie zaleceń wskazanych powyżej.

Rozdział III

1.Wykaz adresatów sprawozdania

Starosta Powiatu Polickiego.

2. Liczba egzemplarzy sprawozdania

Sprawozdanie sporządzono w 1 egzemplarzu.

Michał Pruski
Audytor wewnętrzny

Bibliografia:

I. Pozycje zwarte

1. Fajgielski P. (2010) *Kontrola i Audyt przetwarzania danych osobowych*, Prescom sp. z o.o., Wrocław.
2. Jędruszczak, B. Nowakowski (2011) *System kontroli GIODO i ochrona informacji niejawnych. Praktyczne wskazówki ochrony i kontroli danych osobowych i informacji niejawnych*, Beck InfoBiznes., Warszawa.
3. Zarządzenie ryzykiem -ISO/IEC CD 27005:2007

II. Akty prawne

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.z 2002 nr 101 poz.926 j.t.).
2. 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.z 2004 nr 100 poz.1024).
3. Rozporządzenie Ministra Finansów z dnia 1 lutego 2010 r. w sprawie przeprowadzania i dokumentowania audytu wewnętrznego (Dz.U.z 2010 nr 21 poz.108).
4. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 nr 182 poz.1228).
5. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U.2011.159.948).
6. 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 (Dz.U.2012.526).