OCHRONA DANYCH OSOBOWYCH W BIBLIOTEKACH. ASPEKTY PRAWNE, TECHNICZNE I ORGANIZACYJNE

Andrzej Koziara

Biblioteka Narodowa Życie codzienne przynosi bardzo dużo informacji o tym, że wiele organizacji komercyjnych, jak i tych, które nie prowadzą takiej działalności, poświęca bardzo mało uwagi zagadnieniom ochrony informacji oraz innych danych przez nie gromadzonych. Zjawisko to występuje z tym samym natężeniem w Polsce, Europie czy Stanach Zjednoczonych. Oczywiście w zależności od kraju, czy firmy, sposoby ataków w celu uzyskania nieuprawnionego dostępu do danych są różne, ale najczęściej bardzo skuteczne.

Jak wykazuje doświadczenie, dla intruzów z zewnątrz łakomym kąskiem są nie tylko dane osobowe, lecz również wszystkie informacje, za które mogą uzyskać odpowiednie wynagrodzenie. Pozyskane tą drogą informacje, z pozoru bardzo błahe, mogą utrudniać późniejsza, sprawną pracę firmy. Unormowania prawne służące ochronie danych osobowych powinny stać się inspiracją do podjęcia działań porządkujących zestaw procedur, opisujących czynności związane z zarządzaniem biblioteką. Pozwalają również na optymalizację procesów zachodzących w analizowanej instytucji, prowadząc do powiększenia efektów jej pracy przy zachowaniu niezmienionego poziomu kosztów.

Na wstępie należy również zaznaczyć, że podział zastosowany w tytule tego referatu jest całkowicie sztuczny. Wszystkie działania podejmowane w celu zwiększenia poziomu bezpieczeństwa systemów informatycznych mają swoje źródło w przepisać prawa (krajowego, regionalnego lub firmowego) natomiast realizowane są w sferze organizacyjnej i technicznej.

Dla osiągnięcia zamierzonych efektów, działania te muszą być w pełni skoordynowane z podejmowanymi przez jednostki nadrzędne oraz być źródłem działań podejmowanych przez nadzorowane przez nas jednostki.

Wszystkie czynności podejmowane przez jednostki, które zgłosiły swoje zbiory danych osobowych muszą być zgodne z zasadami określonymi w "Ustawie o ochronie danych osobowych" z dnia 29 sierpnia 1997 roku, z późniejszymi zmianami opublikowanej w postaci jednolitego tekstu w Dzienniku Ustaw 2002 r. Nr 101 poz. 926. Integralnymi składnikami tej ustawy są rozporządzenia wydawane przez Ministra Spraw Wewnętrznych i Administracji wynikające z art. 39a ustawy. W dniu 29 kwietnia 2004 Minister SWiA wydał dwa rozporządzenia obowiązujące od 1 maja 2004 (dnia wejścia Polski do Unii Europejskiej) regulujące szczegółowo:

- Dokumentację przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (opublikowane w Dz. U. z 2004 r. Nr 100, poz. 1024) - oznaczone w dalszym tekście jako rozporządzenie nr 1
- Wzór zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (opublikowane w Dz. U. z 2004 r. Nr 100, poz. 1025) - oznaczone w dalszym tekście jako rozporządzenie nr 2

W środowisku bibliotekarskim, a szczególnie bibliotek naukowych, konieczność podporządkowania się wymaganiom ustawy wzbudza do dnia dzisiejszego bardzo duże kontrowersje. W myśl jej zapisów z art. 43 ust. 1 administratorzy danych osobowych nie muszą rejestrować zbiorów danych przetwarzając je w związku z zatrudnieniem, świadczeniem usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się. Jeżeli zatem w bazie znajdują się tylko dane dotyczące studentów i pracowników własnej uczelni, zbiory takie nie podlegają rejestracji. Konieczność rejestracji wymusza okoliczność, że w bardzo niewielkim procencie czytelnikami są osoby z zewnątrz. Myślę, że kontrowersje są niesłuszne. Jak pokazują doświadczenia, określone tam wymagania inspirują zainteresowanie zarządzających sprawami bezpieczeństwa bibliotecznych systemów teleinformatycznych. Równocześnie skonkretyzowane i uporządkowane

wymagania dotyczące bezpieczeństwa systemów komputerowych, tworzą spójny system ochronny zapobiegający typowemu działaniu służb informatycznych, polegający na bezkrytycznym ograniczaniu funkcji dostępnych na stacjach roboczych.

Pierwszym etapem przygotowania i wdrożenia firmowego systemu bezpieczeństwa jest opracowanie "polityki bezpieczeństwa". Obowiązek ten wynika artykułów nr 3 i 4 rozporządzenia nr 1. W polityce bezpieczeństwa zostają określone reguły i praktyczne zasady normujące sposób zarządzania, ochrony i rozpowszechniania informacji tworzonej w bibliotece. W zależności od technologii stosowanej w naszej instytucji informacje te mogą być gromadzone i przetwarzane w sposób tradycyjny (kartoteka) lub w systemach komputerowych. Zalecenia dotyczące tworzenia "polityki bezpieczeństwa" mówią, że powinna ona być: zatwierdzona przez dyrekcję biblioteki, oficjalnie opublikowana i dostępna na stale dla pracowników. Ważne jest również to, że powinna ona deklarować pełne zaangażowanie kierownictwa w jej realizację. Minimalne wymagania wobec polityki bezpieczeństwa są określone w Polskiej Normie nr PN-ISO 17799 z 2003 r. "Technika Informatyczna .....". Praktyczne zasady zarządzania bezpieczeństwem informacji". W praktyce powinna ona zawierać przynajmniej:

1. Definicję bezpieczeństwa informacji, jej ogólne cele i zakres.
2. Znaczenie bezpieczeństwa jako mechanizmu umożliwiającego współużytkowanie informacji.
3. Oświadczenie o intencjach kierownictwa, zatwierdzające cele i zasady bezpieczeństwa informacji.
4. Krótkie omówienie zasad, standardów i wymagań wymienionych w polityce bezpieczeństwa, a mających szczególne znaczenie dla instytucji. Przykładowo:
    - Zgodność z prawem i wymaganiami wynikającymi z umów międzynarodowych lub firmowych:
    - Wymagania dotyczące kształcenia pracowników w zakresie przestrzegania zasad bezpieczeństwa (BARDZO WAŻNE);
    - Zapobieganie i wykrywanie wirusów oraz innego złośliwego oprogramowania zaburzającego pracę serwerów i stacji roboczych;
    - Zarządzanie ciągłością działania użytkowego instytucji;
    - Konsekwencje naruszenia polityki bezpieczeństwa.
5. Definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji W szczególności powinny zostać omówione zasady zgłaszania przypadków naruszenia bezpieczeństwa zasobów informacyjnych.
6. Odsyłacze do innej szczegółowej dokumentacji uzupełniającej politykę bezpieczeństwa tj.: szczegółowych polityk bezpieczeństwa pojedynczych systemów komputerowych, procedur postępowania przygotowanych dla całej instytucji lub systemów komputerowych lub innych zasad bezpieczeństwa, które powinni przestrzegać pracownicy.

Ważne jest również by sam dokument określający politykę bezpieczeństwa był napisany jasnym i konkretnym językiem o niskim poziomie abstrakcyjności, a przez to zrozumiałym dla wszystkich pracowników. Zasady postępowania omówione w polityce bezpieczeństwa powinny zawierać szczegółowe uzasadnienie omawiające przyjęte standardy i wymagania bezpieczeństwa. Jeżeli w naszej bibliotece przetwarzane są zarejestrowane zbiory danych osobowych, zgodnie z ustawą powinniśmy przygotować oddzielną polityką bezpieczeństwa dotyczącego tego zakresu. Polityka taka powinna w całości wynikać z ogólnej polityki bezpieczeństwa biblioteki.

Dla prawidłowej realizacji polityki bezpieczeństwa niezbędne jest dokonanie inwentaryzacji zasobów, które będą podlegać jej działaniu. W związku z powyższym w art. 4 rozporządzeniu

w sposób szczegółowy wymieniono wszystkie składniki, które powinny zostać poddane zewidencjonowaniu. Są to:

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.

Ad.1

Ustawa definiuje szczegółowo, istotę określenia "miejsce przetwarzania danych osobowych". W uproszczeniu możemy powiedzieć, że są to wszystkie pomieszczenia gdzie je wprowadzamy, modyfikujemy, udostępniamy czy je przechowujemy. Należy pamiętać o wszystkich pomieszczeniach, gdzie mogą się one znaleźć, a w szczególności o szafach zawierających papierowe archiwa z danymi osobowymi. Także miejscach gdzie przechowujemy wycofany z eksploatacji lub uszkodzony sprzęt komputerowy oraz miejscach, gdzie przechowujemy dobre lub uszkodzone elektroniczne nośniki danych, na których były przechowywane bazy danych osobowych (wymontowane dyski twarde, dyskietki od napędów ZIP, taśmy od streamerów, płyty optyczne CD i DVD). Jeżeli dane osobowe są przetwarzane równocześnie przez kilka bibliotek, polityki bezpieczeństwa muszą być przygotowane oddzielnie dla każdej z nich. Równocześnie w polityce jednostki wiodącej powinny zostać wymienione wszystkie miejsca, gdzie są przetwarzane dane składowane we wspólnej bazie. W wykazie miejsc, gdzie przetwarzane są dane osobowe, powinny się również znaleźć lokalizacje serwerów zawierających bazy danych osobowych osób korzystających z możliwości zamawiania zbiorów poprzez OPAC.

Ad. 2

Podstawową sprawą przy identyfikacji przetwarzanych zbiorów informacji jest określenie nazw zbiorów oraz programów używanych do ich przetwarzania. W polityce bezpieczeństwa należy szczegółowo opisać strukturę oprogramowania używanego do przetwarzania zbioru danych osobowych, z uwzględnieniem sposobu jego instalowania. W przypadku oprogramowania składającego się z wielu modułów, należy określić szczegółowo granice ich oddziaływania.

Ad. 3

W polityce bezpieczeństwa należy szczegółowo zdefiniować zawartość poszczególnych pól w rekordach gromadzonych danych. W szczególności należy zwrócić uwagę na te pola, które ze względu na swoją naturę (np. "uwagi o czytelniku") nie mają ściśle określonej zawartości. Dla takich pól, polityka powinna ściśle określać zakres informacji, które mogą zostać do niego wprowadzone. Należy również ustalić sposób weryfikacji raz wprowadzonych danych, oraz sposób archiwowania poprawianej informacji.

Ad. 4

Współczesne technologie informatyczne umożliwiają niemalże swobodne przekazywania danych pomiędzy różnymi systemami informatycznymi. Polityka bezpieczeństwa musi ściśle zdefiniować akceptowane przez nas kanały ich dystrybucji. Powinien zostać zdefiniowany maksymalny zakres dystrybuowanych danych oraz cel ich przekazywania. W przypadku bibliotek mogą to być wykazy nierzetelnych czytelników, przekazywanych wzajemnie przez biblioteki rejestrujące wypożyczenia książek w sposób rozproszony w różnych systemach komputerowych System powinien umożliwiać

rejestrowanie w sposób trwały zakresu przekazanych danych. Równocześnie należy określić zestaw danych, który może podlegać automatycznej aktualizacji. W przypadku sieci bibliotek uczelni wyższych, mogą to być adresy korespondencyjne używane w chwili wysyłania upomnień. Dane te mogą być automatycznie aktualizowane z systemu kadrowego dla upomnień pracowniczych oraz dziekanatowego dla upomnień wysyłanych do studentów.

Ad. 5

Element bardzo ważny i ulegający najczęstszym zmianom. Opisuje on wszystkie działania podejmowane przez służby informatyczne dla zapewnienia poufności gromadzonych danych. Określa on również zakres niezbędnych działań podjętych wobec pracowników, definiując ich rolę w zakresie przestrzegania przyjętych zasad. Z reguły w polityce określa się podstawowe normy postępowania. Ze względu na gwałtowny rozwój systemów operacyjnych stacji roboczych oraz systemów operacyjnych i bazodanowych instalowanych na serwerach, szczegółowe rozwiązania powinny zostać określone w załącznikach do polityki. Załączniki te powinny być aktualizowane przy każdej stosowanej technologii. O każdej takiej zmianie powinni zostać w sposób jawny powiadomieni wszyscy pracownicy, których taka zmiana dotyczy. Dla zapewnienia stabilności ochrony systemów, główna polityka bezpieczeństwa firmy powinna być zmieniana w ostateczności, gdy już nie ma możliwości załatwienia tej sprawy poprzez odpowiednie załączniki. Szczegółowy zakres elementów związanych z bezpieczeństwem zostanie omówiony w dalszej części opracowania.

Na podstawie założeń zdefiniowanych w polityce bezpieczeństwa administrator danych osobowych (kierownik jednostki - dyrektor biblioteki) zobowiązany jest do przygotowania instrukcji określającej sposób zarządzania systemami informatycznymi, służącej do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji. Instrukcja taka powinna zostać zatwierdzona przez administratora danych osobowych do stosowania, a zawarte w niej zapisy przekazane do realizacji przez pracowników.

W instrukcji powinny zostać zawarte ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane. Opisujemy również zastosowane rozwiązania techniczne, procedury eksploatacji i zasady użytkowania zastosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Jeżeli w bibliotece do przetwarzania danych osobowych wykorzystujemy kilka systemów informatycznych, instrukcja taka może dotyczyć wszystkich systemów lub należy dla każdego z nich opracować ją oddzielnie.

W minimalnej postaci, instrukcja taka musi obejmować elementy określone w art. 5 rozporządzenia:

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:
    - Elektronicznych nośników informacji zawierających dane osobowe;
    - Kopii zapasowych, o których mowa w pkt 4;
6. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania umożliwiającego nieuprawniony dostęp do systemu informatycznego

7. Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia tj. informacji o odbiorcach gromadzonych przez nas danych osobowych
8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Dla zapewniania ochrony przetwarzanych danych osobowych instrukcja powinna określać zasady postępowania w każdym z wymienionych powyżej działów.

Ad. 1
Należy tutaj zdefiniować zasady przyznawania użytkownikowi identyfikatora w systemie informatycznym, jak również zasady nadawania lub modyfikacji uprawnień użytkownika do zasobów systemu informatycznego. Powinny one obejmować operacje związane z nadawaniem użytkownikom uprawnień począwszy od utworzenia użytkownikowi konta, poprzez przydzielanie i modyfikację jego uprawnień, aż do momentu usunięcia konta z systemu informatycznego. Jesteśmy tutaj zobowiązani do określenia w sposób jednoznaczny zasad postępowania z hasłami użytkowników oraz administratorów systemów informatycznych. Definiujemy również zasady administrowania systemem informatycznym w przypadkach awaryjnych, np. nieobecności odpowiedniego administratora.

Ad. 2
Należy tutaj określić tryb przydzielania haseł. Trzeba opisać, czy hasła mają być przekazywane użytkownikom w formie ustnej, czy pisemnej oraz opisać stopień jego złożoności. W zależności od sposobu przyłączenia do sieci określono minimalną długość haseł, zakres używanych znaków (małe i duże litery, cyfry i znaki specjalne), minimalną częstotliwość jego zmiany oraz ilość zapamiętywanych przez system haseł. Należy również określić osoby upoważnione do zmiany haseł na żądanie użytkowników (osobowe lub funkcjonalne). Niedopuszczalne jest przekazywanie nazw użytkowników oraz haseł poprzez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej. W zależności od zastosowanego systemu możemy wymusić przy pierwszym logowaniu konieczność zmiany hasła. Rozporządzenie szczegółowo określa zasady tworzenia haseł i tak: hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni i składać się co najmniej z 6 znaków, jeżeli w systemie nie są przetwarzane dane, o których mowa w art. 27 ustawy lub 8 znaków, jeżeli takie dane są przetwarzane. Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej. Należy również opisać sposób przechowywania haseł administratorów i ewidencji awaryjnego ich używania.

Ad. 3
Należy tutaj wyspecyfikować kolejne czynności wykonywane podczas uruchamiania systemu informatycznego przetwarzającego dane osobowe. Szczegółowo należy opisać czynności i zasady postępowania użytkowników podczas przeprowadzania procesu uwierzytelniania się (logowania się do systemu). Instrukcja powinna określać sposoby postępowania w celu zachowanie poufności haseł oraz uniemożliwiać nieuprawnione przetwarzanie danych. Należy również określić metody postępowania w sytuacji tymczasowego zawieszenia pracy na skutek opuszczenia stanowiska pracy lub w okolicznościach, kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba. Instrukcja powinna określać sposoby informowania użytkowników o ich powinnościach w chwili zaprzestania pracy, poprzez opisanie sposobów wylogowywania się z systemu oraz wyłączania stacji roboczej. Procedury przeznaczone dla użytkowników systemów przetwarzających dane osobowe w sposób jednoznaczny muszą określać sposób postępowania w sytuacji podejrzenia naruszenia bezpieczeństwa systemu np. w przypadku braku możliwości zalogowania się użytkownika na jego konto, zauważenia zmiany zawartości danych lub innych wskazujących na ingerencję w przetwarzane dane lub sprzęt.

Ad. 4
Należy tutaj opisać sposób i częstotliwość tworzenia kopii zapasowych danych przetwarzanych w systemie oraz kopii samego oprogramowania używanego do ich przetwarzania. Określamy rodzaj

danych które będziemy zabezpieczać, na jakim nośniku, oraz przy pomocy jakich narzędzi programowych i sprzętu będzie to wykonywane. W procedurze określamy dokładny harmonogram wykonywania kopii zapasowych dla poszczególnych zbiorów danych wraz ze wskazaniem odpowiedniej metody sporządzania kopii (kopia przyrostowa, kopia całościowa). Jeżeli procedura wykonywania kopii jest bardzo skomplikowana, możemy skonstruować ją jako zestaw odwołujący się poszczególnych systemów. W takim przypadku szczegółowe procedury są załączone do instrukcji zarządzania. W procedurach opisujących wykonywanie kopii zapasowych określamy maksymalny czas używania poszczególnych nośników, sposób ich rotacji oraz sposoby ich likwidacji. Procedura likwidacji nośników zawierających dane osobowe powinna uwzględniać wymogi zawarte w załączniku do rozporządzenia, nakazujące by wszystkie urządzenia (dyski twarde lub inne nośniki elektroniczne) zawierające dane osobowe, przeznaczone do wymiany gwarancyjnej lub likwidacji, pozbawiać zapisu tych danych, a gdy nie jest to możliwe, uszkadzać w sposób uniemożliwiający ich odczytanie.

Ad. 5.
Należy tutaj opisać sposób i czas przechowywania nośników informacji używanych do wykonywania kopii zapasowych (taśmy magnetyczne, płyty optyczne CD i DVD oraz dyskietki FDD i ZIP). Określeniu podlegają również pomieszczenia, przeznaczone do przechowywania nośników informacji, jak również sposoby fizycznego i logicznego zabezpieczenia przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem(szafy metalowe, ogniotrwałe, deponowanie na zewnątrz).Przy opracowywaniu zaleceń uwzględniamy wymogi załącznika do rozporządzenia (pkt. 4 ppkt 4a). W czasie przygotowania instrukcji należy pamiętać, że kopie awaryjne należy usuwać bezzwłocznie po ustaniu ich użyteczności. Jeżeli podejmujemy decyzję o przechowywaniu kopii zapasowych na zewnątrz, należy szczegółowo określić procedury bezpiecznego ich deponowania uwzględniające również czas transportu

Ad. 6
Należy tutaj opisać obszary naszych systemów narażonych na ingerencję wirusów komputerowych oraz wszelkiego innego rodzaju oprogramowania mogącego mieć wpływ na bezpieczeństwo przetwarzanych danych osobowych. Należy określić wszelkie możliwe do zidentyfikowania źródła przedostania się szkodliwego oprogramowania oraz działania, jakie będą podejmowane by zminimalizować możliwość zainstalowania takiego oprogramowania na serwerach i stacjach roboczych. Instrukcja powinna zawierać specyfikację stosowanego oprogramowania przeciwdziałającego szkodliwemu działaniu oprogramowań "wrogich". Należy wyspecyfikować nazwy oprogramowań antywirusowych stosowanych w firmie oraz określić sposób i częstotliwość uaktualniania bazy wirusów. Użytkownik musi zostać przeszkolony w zakresie procedur postępowania w przypadku, gdy oprogramowanie zabezpieczające wskazuje zaistnienie zagrożenia. W punkcie tym należy również wyspecyfikować wszystkie inne sposoby zabezpieczające nasze serwery i stacje robocze przed nieuprawnionym pozyskiwaniem danych osobowych. Mogą do nich należeć np. fizyczne blokady urządzeń zapisujących dane na nośnikach wymiennych (streamery, stacje optyczne z funkcją zapisu czy stacje FDD i ZIP)

Ad. 7.
Jest to punkt, który będzie dotyczył niewielkiej liczby bibliotek. Z reguły dane osobowe są gromadzone na potrzeby własne. Jedynym wyjątkiem może być przekazywanie danych osobowych czytelników zalegających ze zwrotem książek instytucjom, które mogą mieć wpływ na przyspieszenie ich zwrotu. Przykładowo może być to wykaz studentów danej uczelni, którzy nie zwrócili książek do bibliotek pedagogicznych lub publicznych

Ad. 8.
Należy tutaj określić zakres, częstotliwość oraz procedury wykonywania przeglądów i konserwacji systemu informatycznego. Dotyczy to w równej mierze sprzętu, jak i oprogramowania Należy wskazać firmy i osoby fizyczne nie będące naszymi pracownikami, uprawnione do dokonywania przeglądów i konserwacji systemu. Procedury wykonywania czynności konserwacyjnych zlecane

osobom nie mającym uprawnień do przetwarzania danych (np. firmom zewnętrznych), winny określać sposób nadzorowania przez administratora danych wykonywanych prac.

Po przygotowaniu polityki bezpieczeństwa i instrukcji określającej sposób zarządzania systemami informatycznymi, prostym wydaje się wypełnienie "Zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych". Zawiera on informacje formalne podawane w częściach od A do D oraz część E opisującą konfigurację systemu przetwarzającego dane osobowe oraz wszystkie środki bezpieczeństwa podjęte przez instytucję w celu uniemożliwienia nieuprawnionego dostępy do danych.

Scharakteryzowane powyżej czynności oprócz wypełnienia warunków formalnych, są okazją do uporządkowania organizacyjnego naszej instytucji. Zapobiegają również stosowaniu rozwiązań nadmiarowych lub zbędnych i mogą stać się wstępem do prac zmierzających do uzyskania certyfikatu ISO 9000.

Zapraszam również do zapoznania się z aktualnymi rozwiązaniami stosowanym na terenie BUŚ. Dostęp do nich będzie możliwy po wyrażeniu takiego zapotrzebowania w sposób pisemny.

Literatura:

1. Ustawia z dnia 29 sierpnia 1997 roku o ochronie danych osobowych", z późniejszymi zmianami, tekst jednolity Dziennik Ustaw z 2002 r. Nr 101 poz. 926
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, Dziennik Ustaw z 2004 r. Nr 100, poz. 1024
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, Dziennik Ustaw z 2004 r. Nr 100, poz. 1025
4. Kevin Mitnick, Wiliam Simon , "Sztuka podstępu", wydanie polskie Wydawnictwo Helion 2003