Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa.

Opracowanie omawia sposób przygotowania i zakresu dokumentacji opisującej politykę bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024)

Uwagi ogólne.

Zgodnie z § 3 i § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024), zwanego dalej rozporządzeniem, administrator danych obowiązany jest do opracowania w formie pisemnej i wdrożenia polityki bezpieczeństwa. Pojęcie „polityka bezpieczeństwa", użyte w rozporządzeniu należy rozumieć, jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej (tutaj danych osobowych) wewnątrz określonej organizacji [1]. Należy zaznaczyć, że zgodnie z art. 36 ust. 2 oraz art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.), zwanej dalej ustawą, polityka bezpieczeństwa, o której mowa w rozporządzeniu powinna odnosić się całościowo do problemu zabezpieczenia danych osobowych u administratora danych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych. Celem polityki bezpieczeństwa, jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych, o których mowa w § 36 ustawy. Polska Norma PN-ISO/IEC 17799 [3] określająca praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych, jako cel polityki bezpieczeństwa wskazuje „*zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji*". Zaznacza się, że dokument polityki bezpieczeństwa powinien deklarować zaangażowanie kierownictwa i wyznaczać podejście instytucji do zarządzania bezpieczeństwem informacji. Jako minimum w [3] wskazuje się, aby dokument określający politykę bezpieczeństwa zawierał:

a) *definicję bezpieczeństwa informacji, jego ogólne cele i zakres oraz znaczenie bezpieczeństwa jako mechanizmu umożliwiającego współużytkowanie informacji;*

b) oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji;

c) krótkie wyjaśnienie polityki bezpieczeństwa, zasad, standardów i wymagań zgodności mających szczególne znaczenie dla instytucji, np.:

1) zgodność z prawem i wymaganiami wynikającymi z umów;

2) wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa;

3) zapobieganie i wykrywanie wirusów oraz innego złośliwego oprogramowania;

4) zarządzanie ciągłością działania biznesowego;

5) konsekwencje naruszenia polityki bezpieczeństwa;

d) definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania przypadków naruszenia bezpieczeństwa;

e) odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dla poszczególnych systemów informatycznych lub zasad bezpieczeństwa, których użytkownicy powinni przestrzegać.

Wymienione wyżej, cytowane za [3], zalecenia w pełni można stosować do dokumentacji polityki bezpieczeństwa, o której mowa w § 4 rozporządzenia. Dokument określający politykę bezpieczeństwa nie powinien mieć charakteru zbyt abstrakcyjnego. Zasady postępowania określone w polityce bezpieczeństwa powinny zawierać uzasadnienie wyjaśniające przyjęte standardy i wymagania. Wyjaśnienia i uzasadnienia zalecanych metod sprawiają na ogół, że rzadziej dochodzi do ich naruszenia i nie przestrzegania [5].

Dokument, o którym mowa w § 4 rozporządzenia w zakresie przedmiotowym powinien koncentrować się na bezpieczeństwie przetwarzania danych osobowych, co wynika z art. 36 ustawy o ochronie danych osobowych[1]. Prawidłowe zarządzanie zasobami, w tym również zasobami informacyjnymi, zwłaszcza w aspekcie bezpieczeństwa informacji, wymaga właściwej identyfikacji tych zasobów [2] oraz określenia miejsca i sposobu ich przechowywania. Wybór zaś odpowiednich dla poszczególnych zasobów metod zarządzania ich ochroną i dystrybucją zależny jest od zastosowanych nośników informacji, rodzaju zastosowanych urządzeń, sprzętu komputerowego i oprogramowania. Stąd też w § 4 rozporządzenia ustawodawca wskazał, że polityka bezpieczeństwa powinna zawierać w szczególności:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym

[1] 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. Nr 100 poz. 1024), zwanego dalej rozporządzeniem, wydane zostało na podstawie delegacji ustawowej art. 39a ustawy o ochronie danych osobowych i jego zakres na podstawie art. 36 ust. 2 tejże ustawy ograniczony jest do przetwarzania danych osobowych.

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 przy przetwarzaniu danych.

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

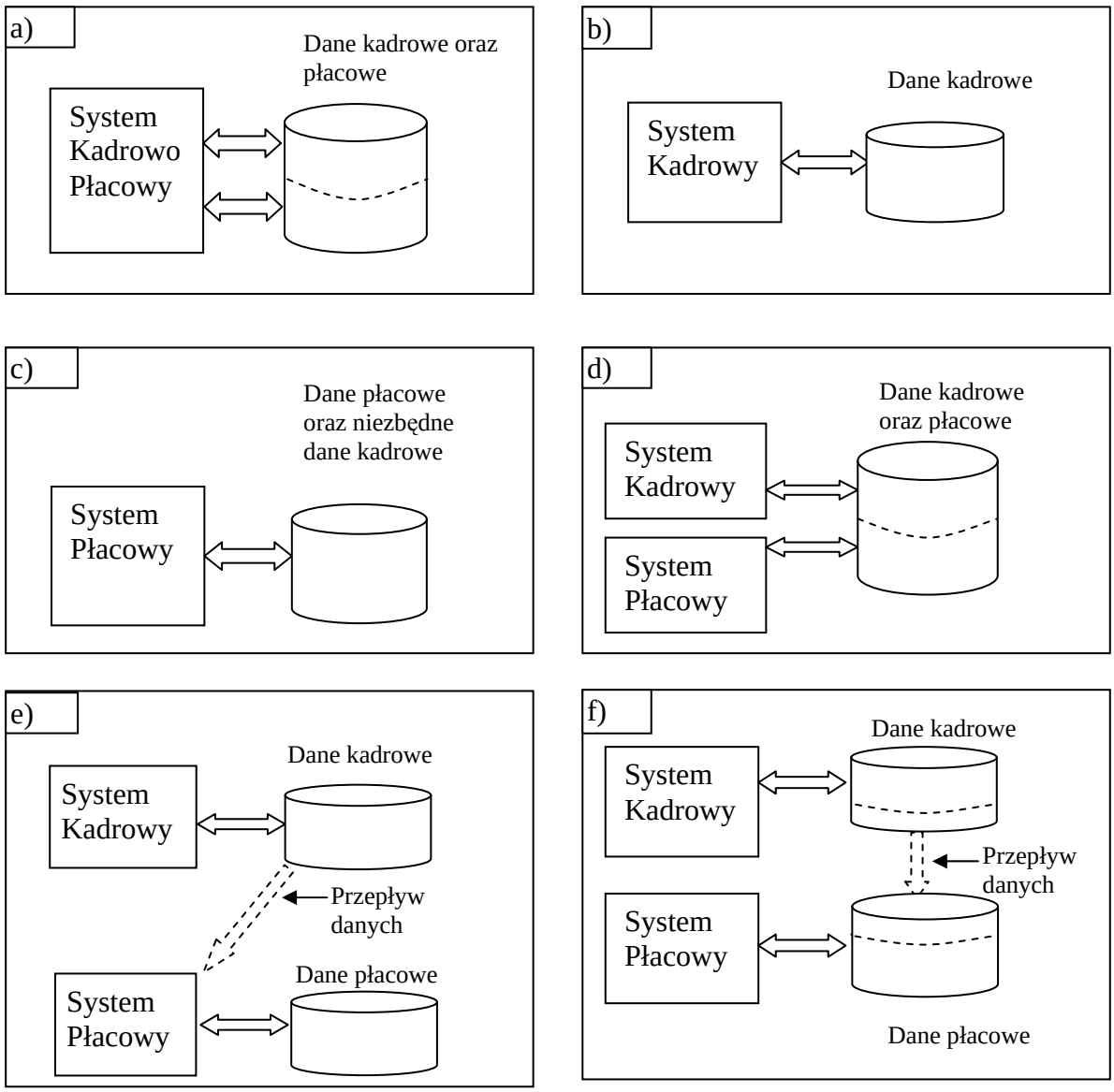
Określając obszar przetwarzania danych osobowych należy pamiętać, iż zgodnie z ustawą o ochronie danych osobowych, przetwarzaniem danych osobowych nazywamy jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. W związku z powyższym, określanie obszaru pomieszczeń, w którym przetwarzane są dane osobowe, powinno obejmować zarówno miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacja papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco). Zgodnie z treścią §4 punkt 1, wskazanie miejsca przetwarzania danych osobowych powinno być określone poprzez określenie budynków, pomieszczeń lub części pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Do obszaru przetwarzania danych należy zaliczyć również pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, uszkodzone komputery i inne urządzenia z nośnikami zawierającymi dane osobowe). Do obszaru przetwarzania danych osobowych administrator danych powinien zaliczyć również miejsce w sejfie bankowym, archiwum, itp. jeśli wykorzystywane są one np. do przechowywania elektronicznych nośników informacji zawierających kopie zapasowe danych przetwarzanych w systemie informatycznym, czy też do składowania innych nośników danych, np. dokumentów źródłowych.

W przypadku, gdy dane osobowe przetwarzane są w systemie informatycznym, do którego dostęp poprzez sieć telekomunikacyjną posiada wiele podmiotów, wówczas w polityce

bezpieczeństwa informacje o tych podmiotach (nazwa podmiotu, siedziba, pomieszczenia, w których przetwarzane są dane), powinny być również wymienione jako obszar przetwarzania danych. Wymóg powyższy nie dotyczy sytuacji udostępniania danych osobowych użytkownikom, którzy dostęp do systemu uzyskują tylko z prawem wglądu w swoje własne dane po wprowadzeniu właściwego identyfikatora i hasła (np. systemów stosowanych w uczelniach wyższych do udostępniania studentom informacji o uzyskanych ocenach) oraz systemów, do których dostęp z założenia jest dostępem publicznym np. książka telefoniczna udostępniana w Internecie. W wyżej wymienionych sytuacjach wystarczające jest wskazanie budynków i pomieszczeń, w których dane są przetwarzane przez administratorów systemu informatycznego oraz budynki i pomieszczenia, w których dostęp do danych uzyskują osoby posiadające szerszy zakres uprawnień, niż tylko wgląd do swoich własnych danych lub danych udostępnianych publicznie.

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Ważnym elementem identyfikacji przetwarzanych zasobów informacyjnych jest wskazanie nazw zbiorów danych oraz systemów informatycznych używanych do ich przetwarzania. Stąd też oprócz wskazania obszaru przetwarzania danych, polityka bezpieczeństwa powinna identyfikować zbiory danych osobowych oraz systemy informatyczne używane do ich przetwarzania. W przypadku, gdy system zbudowany jest z wielu modułów programowych i moduły te mogą pracować niezależnie np. mogą być instalowane na różnych stacjach komputerowych, wówczas wskazanie systemu powinno być wykonane z dokładnością do poszczególnych jego modułów. Należy zauważyć również, iż jeden program może przetwarzać dane zawarte w jednym zbiorze jak i wielu zbiorach danych osobowych. Sytuacja może być również odwrotna, kiedy to wiele różnych programów przetwarza dane, stanowiące jeden zbiór danych osobowych. Programy te to najczęściej moduły zintegrowanego systemu. Każdy taki moduł dedykowany jest do wykonywania określonych, wydzielonych funkcjonalnie zadań. Przykładem, może być system kadrowy oraz system płacowy, które często występują jako jeden zintegrowany system kadrowo - płacowy. Systemy informatyczne mogą przetwarzać dane osobowe stanowiące jeden wspólny zbiór danych, jak też wiele odrębnych zbiorów danych osobowych. Mogą być zintegrowane tworząc jeden system, z jednym lub wieloma zbiorami danych. Przykłady możliwych w tym zakresie konfiguracje przedstawiono na Rys. 1



Rys. 1. Różne modele współpracy systemów informatycznych ze zbiorami danych; a, b, c) - jeden zbiór danych przetwarzany przez jeden system; d) - dwa oddzielne systemy (moduły programowe) przetwarzają dane zawarte w jednym zbiorze; e, f) - dwa oddzielne systemy (moduły programowe) przetwarzają dane zawarte w dwóch zbiorach pomiędzy którymi występuje przepływ danych.

Stąd też, w części polityki bezpieczeństwa identyfikującej zbiory danych osobowych oraz stosowane do ich przetwarzania programy powinny być zamieszczone nazwy zbiorów danych osobowych oraz nazwy używanych do ich przetwarzania programów komputerowych. Wykaz ten powinien zawierać informacje w zakresie precyzyjnej lokalizacji miejsca (budynek, pomieszczenie, nazwa komputera lub innego urządzenia np. macierzy dyskowej, biblioteki optycznej itp.), w których znajdują się zbiory danych osobowych przetwarzane na bieżąco oraz nazwy i lokalizacje programów (modułów programowych) używanych do ich przetwarzania.

3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Zgodnie z § 4 pkt 3 rozporządzenia, dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze. Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać jakie kategorie danych są w nich przechowywane. Opis pola danych, w przypadkach, gdy możliwa jest niejednoznaczna interpretacja jego zawartości, powinien wskazywać nie tylko kategorię danych, ale również format jej zapisu i/lub określone w danym kontekście znaczenie. Za niewystarczający należy uznać np. opis jednoznakowego pola w postaci „Zgoda na przetwarzanie danych osobowych dla celów marketingowych", jeśli nie dodamy, że w pole to należy wpisywać literę „T" w przypadku wyrażenia zgody lub literę „N" w przypadku nie wyrażenia zgody. Brak stosownego opisu może spowodować inne niż zakładano sposoby zapisu oraz interpretacji określonej informacji.

W odniesieniu do opisu struktury zbioru, w przypadku zbiorów danych przetwarzanych w systemie informatycznym, należy zauważyć, iż jest on niezbędny dla ustalenia bądź też weryfikacji zakresu danych. Zakres ten, w przypadku relacyjnych baz danych, nie wynika bezpośrednio z zakresu danych przypisanych poszczególnym obiektom zapisanym w zbiorze. Jest on zależny od relacji ustalonych pomiędzy poszczególnymi obiektami. Przykładowo, jeśli w zbiorze przetwarzane są informacje o danych adresowych klienta, zamówieniach klientów oraz sprzedawanych towarach w zakresie przedstawionym w tablicy 1, to z relacji ustanowionych za pośrednictwem pola o nazwie identyfikatora klienta pomiędzy obiektami: „*dane adresowe klienta*" i „*zamówienia klienta*" wynika, że w zbiorze tym przetwarzane są informacje o klientach w następującym zakresie:

<***Zakres 1***>: [imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), nazwa towaru, ilość towaru, wartość zamówienia, data zamówienia, data odbioru],

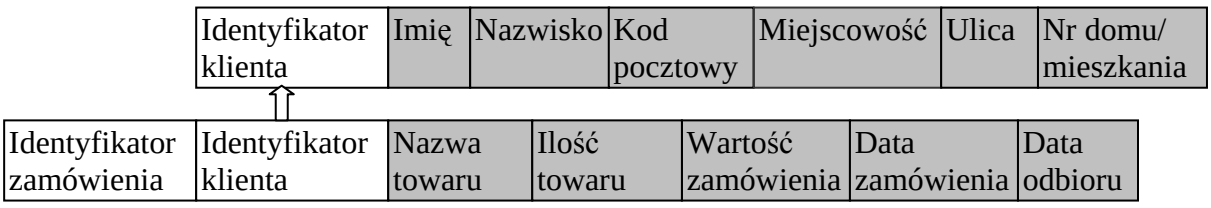
oraz informacje o towarach w zakresie:

<***Zakres 2***>: [identyfikator towaru, nazwa towaru, nazwa producenta, data produkcji].

Tablica 1. Struktura zbioru zawierającego informacje o klientach, zamówieniach i produktach.

dane adresowe klienta:	[**identyfikator klienta**, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania)]
zamówienia klienta:	[identyfikator zamówienia, **identyfikator klienta**, nazwa towaru, ilość towaru, wartość zamówienia, data zamówienia, data odbioru]
sprzedawane towary:	[identyfikator towaru, nazwa towaru, nazwa producenta, data produkcji]

Zakres danych przetwarzanych o kliencie oznaczony wyżej jako „*Zakres 1*”, jak łatwo zauważyć, powstał na skutek relacji, jaka istnieje pomiędzy obiektami „*dane adresowe klienta*” i „*zamówienia klienta*”. Relacja ta spowodowała, że zakres danych, zawarty w obiekcie „*dane adresowe klienta*”, powiększony został o dane zawarte w obiektach „*zamówienia klienta*”. Warto tutaj zauważyć, że w obiekcie oznaczonym „*zamówienia klienta*”, zamawiany towar wskazany został bezpośrednio poprzez określenie jego nazwy, a nie relacji z obiektem, w którym opisane są wszystkie dane na jego temat. Zapis taki spowodował, że dane o sprzedawanych towarach zapisane w obiektach oznaczonych „*sprzedawane towary*”, pomimo, że fizycznie zapisane są w tym samym zbiorze danych, nie poszerzają zakresu danych o kliencie oznaczony jako „*Zakres 1*”.



Rys. 2. Zakres danych osobowych (pola oznaczone szarym tłem) przetwarzanych w zbiorze zawierającym informacje o danych adresowych klienta, zamówieniach oraz sprzedawanych towarach.

W przypadku relacyjnych baz danych praktycznie każdą informację można zapisać poprzez utworzenie odpowiedniej relacji. Dla struktury przedstawionej w tablicy 1, informacje o nazwie zamawianego towaru w zamówieniach klientów można zapisać alternatywnie w postaci relacji, co pokazano w tablicy 2.

Tablica 2. Struktura zbioru zawierającego informacje o klientach, zamówieniach i towarach z informacją o zamówionym towarze zapisaną w postaci relacji.

dane adresowe klienta:	[**identyfikator klienta**, imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania)]
zamówienia klienta:	[identyfikator zamówienia, **identyfikator klienta**, ***identyfikator towaru***, ilość towaru, wartość zamówienia, data zamówienia, data odbioru]
sprzedawane towary:	[***identyfikator towaru***, nazwa towaru, nazwa producenta, data produkcji]

Przedstawiona powyżej, na pozór niewielka, zmiana w strukturze opisu obiektów w zbiorze danych powoduje, że na skutek wprowadzonej dodatkowo relacji pomiędzy zamówieniami klientów i sprzedawanymi produktami, zakres przetwarzanych informacji o klientach i wykonywanych przez nich zakupach powiększa się do zakresu:

<**Zakres 3**>: [imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/ mieszkania), nazwa towaru, nazwa producenta, data produkcji, ilość towaru, wartość zamówienia, data zamówienia, data odbioru].

Rys. 3. Zakres danych osobowych (pola oznaczone szarym tłem) przetwarzanych w zbiorze zawierającym informacje o danych adresowych klienta, zamówieniach oraz sprzedawanych towarach.

Analizując powyższy przykład można zauważyć, że istniejące w strukturze zbioru danych relacje, pomiędzy opisem poszczególnych obiektów, w istotny sposób wpływają na rzeczywisty zakres przetwarzanych informacji o wskazanym obiekcie.

Skróty i oznaczenia poszczególnych kategorii danych oraz wprowadzane ze względów technicznych indeksy i klucze, w celu podwyższenia efektywności przetwarzania, sprawiają

często, że techniczny opis struktury zbioru danych, a zwłaszcza postać, w jakiej ta struktura jest zapisana w systemie informatycznym, nie zawsze są wystarczająco przejrzyste.

Stąd też, stosując się do § 4 pkt 3 rozporządzenia, należy w polityce bezpieczeństwa wskazać poszczególne grupy informacji oraz istniejące między nimi relacje identyfikując w ten sposób pełny zakres danych osobowych, jakie przetwarzane są w określonym zbiorze. Opisując struktury zbiorów danych nie jest konieczne przedstawianie pełnej dokumentacji struktury bazy danych z wyszczególnieniem oryginalnych nazw poszczególnych pól informacyjnych, stosowanych kluczy, czy też definicji wbudowanych obiektów funkcyjnych takich jak: procedury, funkcje, pakiety, i wyzwalacze[2] [4].

Wymóg wskazania powiązań pomiędzy polami informacyjnymi w strukturze zbiorów danych, określony w § 4 pkt 3 rozporządzenia, należy rozumieć jako wymóg wskazania wszystkich tych danych, występujących w strukturze zbioru, które poprzez występujące relacje można skojarzyć z określoną osobą. Tak, np. ze struktury zbioru pokazanej w tablicy 1, wynika, iż do danych, które można skojarzyć z osobą o podanym imieniu i nazwisku, należą nie tylko dane zawarte w tym obiekcie, ale również dane zawarte w obiekcie o nazwie „zamówienia klienta". Połączenie to, zgodnie z definicją danych osobowych, powoduje poszerzenie zakresu tych danych osobowych klienta, o dane zawarte w obiekcie „zamówienia klienta".

W § 4 pkt 3 rozporządzenia wyraźnie wskazano, że w polityce bezpieczeństwa ma być zawarty **opis struktury zbiorów** wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi. Opis ten może być przedstawiony w postaci formalnej (tak jak np. w tablicach 1, 2), w postaci graficznej pokazującej istniejące powiązania pomiędzy obiektami (rys. 1,2), jak również opisu tekstowego. Opis tekstowy, dla przypadku wskazanego w tablicy 1, może być następujący:

„*W zbiorze danych przetwarzane są dane osobowe klientów w zakresie:*

a) dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu), oraz

b) wszystkich składanych przez danego klienta zamówieniach (nazwa towaru, ilość towaru, wartość zamówienia, data zamówienia i data odbioru)."

W przytoczonym przykładzie opisu tekstowego, informacja o powiązaniach pomiędzy poszczególnymi polami informacyjnymi występującymi w strukturze zbioru, została

[2] Procedury, funkcje, pakiety, wyzwalacze – są to obiekty zapisane w bazie danych, tak jak inne dane. Obiektami tymi mogą być procedury i funkcje, które mogą być później używane przez aplikacje służąca do przetwarzania danych. Procedury, które uruchamiane są przy zajściu określonego zdarzenia nazywane są wyzwalaczami (ang. Trigger)

przedstawiona w tekście, poprzez wskazanie w punkcie b), że w strukturze zbioru są też informacje *o wszystkich składanych przez **danego** klienta zamówieniach* (powiązanie zamówienia z danymi klienta, które należy rozumieć jako dane adresowe wymienione w punkcie a).

Należy pamiętać, że opis struktury zbiorów, o którym mowa w § 4 pkt 3 rozporządzenia, powinien być przedstawiony w sposób czytelny i zrozumiały.

4. Sposób przepływu danych pomiędzy systemami.

W punkcie tym należy przedstawić sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach, do przetwarzania których systemy te są wykorzystywane. Przedstawiając przepływ danych można posłużyć się np. schematami, jak na rys. 1, które wskazują, z jakimi zbiorami danych system lub moduł systemu współpracuje, czy przepływ informacji pomiędzy zbiorem danych a systemem informatycznym jest jednokierunkowy np. informacje pobierane są tylko do odczytu, czy dwukierunkowy (do odczytu i do zapisu). W sposobie przepływu danych pomiędzy poszczególnymi systemami należy zamieścić również informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (przy wykorzystaniu zewnętrznych nośników danych) lub półautomatycznie – za pomocą teletransmisji (przy wykorzystaniu specjalnych funkcji eksportu/importu danych), wykonywanych w określonych odstępach czasu. Taki przepływ danych występuje np. często pomiędzy systemami Kadrowym i Płacowym (Rys. 1f) oraz pomiędzy systemami Kadrowym, Płacowym a systemem Płatnik służącym do rozliczeń pracowników z ZUS. Dla identyfikacji procesów przetwarzania danych osobowych szczególne znaczenie ma specyfikacja przepływu danych w systemach z rozproszonymi bazami danych. W rozproszonej bazie danych, dane zlokalizowane są w różnych miejscach oddalonych od siebie terytorialnie i mogą zawierać, w zależności od lokalizacji, różne zakresy danych (tzw. niejednorodne oraz federacyjne, rozproszone bazy danych) [5]. Dla systemów korporacyjnych o zasięgu międzynarodowym, informacja o przepływie danych pomiędzy oddziałami korporacji znajdującymi się w państwach nie należących do Europejskiego Obszaru Gospodarczego musi być traktowana jako przepływ danych do państwa trzeciego[3] z wynikającymi z tego tytułu konsekwencjami[4]. W polityce bezpieczeństwa, w punkcie określającym sposób przepływu danych pomiędzy systemami nie

[3] Przez państwo trzecie – rozumie się zgodnie z art. 7 pkt 7 ustawy o ochronie danych osobowych państwo nie należące do Europejskiego Obszaru Gospodarczego

[4] Wymogi związane z przekazywaniem danych osobowych do państwa trzeciego określone zostały w art. 18 ust. 1 pkt 4, 41 ust. 1 pkt 7, 47 oraz 48 ustawy o ochronie danych osobowych.

jest wymagane szczegółowe omawianie rozwiązań technologicznych. Najistotniejsze jest wskazanie zakresu przesyłanych danych, podmiotu lub kategorii podmiotów, do których dane są przekazywane oraz ogólnych informacji na temat sposobu przesyłania danych (Internet, poczta elektroniczna, inne rozwiązania), które mogą decydować o rodzaju narzędzi niezbędnych do zapewnienia ich bezpieczeństwa podczas teletransmisji.

Przepływ danych pomiędzy poszczególnymi systemami informatycznymi, z punktu widzenia analizy zakresu przetwarzanych danych, można z punktu widzenia uzyskiwanego wyniku porównać do opisu relacji pomiędzy poszczególnymi polami informacyjnymi w strukturach zbiorów danych, co przedstawiono w punkcie 3. W przypadku przepływu danych pomiędzy systemami informatycznymi relacje, jakie powstają pomiędzy danymi przetwarzanymi w zbiorach poszczególnych systemów, nie wynikają z ich struktury. W przypadku przepływu danych pomiędzy systemami, dane z poszczególnych zbiorów łączone są dynamicznie poprzez wykonanie określonych funkcji systemu lub odpowiednio zdefiniowanych procedur zewnętrznych.

Poprawne wykonanie zadań wymienionych w punktach 2 i 3 polityki bezpieczeństwa oraz przeprowadzona analiza przepływu danych powinna dać odpowiedź w zakresie klasyfikacji poszczególnych systemów informatycznych z punktu widzenia kategorii przetwarzanych danych osobowych. Klasyfikacja ta powinna w szczególności wskazywać, czy w danym systemie informatycznym są przetwarzane dane osobowe podlegające szczególnej ochronie, o których mowa w § 27 ustawy, czy też nie. Informacje te uzupełnione o dane dotyczące środowiska pracy poszczególnych systemów z punktu widzenia ich połączenia z publiczną siecią telekomunikacyjną powinny dać odpowiedź w zakresie wymaganych poziomów bezpieczeństwa, o których mowa w § 6 rozporządzenia. Stąd też podsumowaniem wykazów i opisów, o których mowa w punktach 2, 3 i 4 polityki bezpieczeństwa powinno być wskazanie w punkcie 4 wymaganych dla poszczególnych systemów informatycznych poziomów bezpieczeństwa.

5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych

W tej części polityki bezpieczeństwa należy określić środki techniczne i organizacyjne niezbędne dla zapewnienia przetwarzanym danym poufności i integralności. Środki te powinny zapewnić jednocześnie rozliczalność wszelkich działań powodujących przetwarzanie danych osobowych. Należy pamiętać, iż środki, o których mowa wyżej, powinny być określone po uprzednim przeprowadzeniu wnikliwej analizy zagrożeń i ryzyka związanych z

przetwarzaniem danych osobowych. Analiza zagrożeń i ryzyka powinna obejmować cały proces przetwarzania danych osobowych. Powinna uwzględniać podatność stosowanych systemów informatycznych na określone zagrożenia. Przy czym, podatność systemu należy tutaj rozumieć jako słabość w systemie, która może umożliwić zaistnienie zagrożenia np. włamania do systemu i utraty poufności danych. Podatnością taką jest np. brak mechanizmu kontroli dostępu do danych, który może spowodować zagrożenie przetwarzania danych przez nieupoważnione osoby. Analizując środowisko przetwarzania danych należy ocenić ryzyko zaistnienia określonych zagrożeń. Ryzyko to można określić jako prawdopodobieństwo wykorzystania określonej podatności systemu na istniejące w danym środowisku zagrożenia. Ważnym jest, aby zastosowane środki techniczne i organizacyjne niezbędne do zapewnienia poufności i integralności przetwarzanych danych były adekwatne do zagrożeń wynikających ze sposobu, jak również kategorii przetwarzanych danych osobowych. Środki te powinny zapewniać rozliczalność wszelkich działań (osób i systemów) podejmowanych w celu przetwarzania danych osobowych. Powinny one spełniać wymogi określone w art. 36 do 39 ustawy oraz być adekwatne do wymaganych poziomów bezpieczeństwa, o których mowa w § 6 rozporządzenia. W odniesieniu do rozliczalności działań podejmowanych przy przetwarzaniu danych osobowych zastosowane środki powinny w szczególności wspomagać kontrolę administratora nad tym, jakie dane osobowe i przez kogo zostały do zbioru wprowadzone (art. 38 ustawy).

Ryzykiem dla przetwarzania danych osobowych w systemie informatycznym podłączonym do sieci Internet jest np. możliwość przejęcia lub podglądu tych danych przez osoby nieupoważnione. Ryzyko to będzie tym większe im mniej skuteczne będą stosowane zabezpieczenia. Sygnalizacja istniejącego zagrożenia pozwala podjąć odpowiednie działania zapobiegawcze. Ważne jest często samo uświadomienie istnienia określonych zagrożeń np. wynikających z przetwarzania danych w systemie informatycznym podłączonym do sieci Internet czy też zagrożeń spowodowanych stosowaniem niesprawdzonych pod względem bezpieczeństwa technologii bezprzewodowej transmisji danych. Zidentyfikowane zagrożenia można minimalizować m.in. poprzez stosowanie systemów antywirusowych, mechanizmów szyfrowania, systemów izolacji i selekcji połączeń z siecią zewnętrzną (firewall), itp. Dla dużych systemów informatycznych (systemów połączonych z sieciami publicznymi, systemów z rozproszonymi bazami danych, itp.) wybór właściwych środków wymaga posiadania wiedzy specjalistycznej. Prawidłowe opracowanie polityki bezpieczeństwa przetwarzania danych osobowych w ww. zakresie jest procesem złożonym, wymagającym m.in. znajomości podstawowych pojęć i modeli używanych do opisywania sposobów zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele, o których mowa,

jak również zagadnienia w zakresie zarządzania i planowania bezpieczeństwa systemów informatycznych, opisane zostały m.in. w Polskich Normach [2,3].

Podczas określania środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i integralności przetwarzanych danych, jak również rozliczalności podejmowanych w tym celu działań, należy kierować się m.in. klasyfikacją poziomów bezpieczeństwa wprowadzoną w § 6 rozporządzenia. Dla każdego z wymienionych tam poziomów, które powinny być zidentyfikowane po wykonaniu zadań wymienionych w punktach 2, 3 i 4 polityki bezpieczeństwa, niezbędne jest zapewnienie co najmniej takich środków bezpieczeństwa, które spełniają minimalne wymagania określone w załączniku do rozporządzenia.

Opis środków, o których mowa w § 4 pkt 5 rozporządzenia, powinien obejmować zarówno środki techniczne jak i organizacyjne. W odniesieniu np. do stosowanych mechanizmów uwierzytelniania powinny być wskazane i opisane zarówno zagadnienia dotyczące uwierzytelnienia użytkowników w systemach informatycznych jak i zagadnienia dotyczące uwierzytelnienia przy wejściu (wyjściu) do określonych pomieszczeń, a także sposób rejestracji wejść/wyjść itp. W przypadku stosowania narzędzi specjalistycznych (zapory ogniowe chroniące system informatyczny przed atakami z zewnątrz, systemy wykrywania intruzów (ang. Intrusion Detection System – IDS, itp.), należy wskazać w polityce bezpieczeństwa, że środki takie są stosowane, w jakim zakresie i w odniesieniu do jakich zasobów. W polityce bezpieczeństwa – dokumencie udostępnianym do wiadomości wszystkim pracownikom - nie należy opisywać szczegółów dotyczących charakterystyki technicznej i konfiguracji stosowanych narzędzi. Dokumenty opisujące szczegóły w tym zakresie powinny być objęte ochroną przed dostępem do nich osób nieupoważnionych.

Literatura:

1. PN-I-02000: Zabezpieczenia w systemach informatycznych – Terminologia, PKN,1998
2. PN-I-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999
3. PN-ISO/IEC 17799 Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, 2003
4. Tomasz Pełech, Gazeta IT nr 6(25) 20 czerwiec 2004
5. Andrzej Białas, Eugeniusz Januła i inni; (red. Andrzej Białas) Podstawy bezpieczeństwa systemów teleinformatycznych; Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2002
6. Paul Beynon-Davies, Systemy baz danych, Wydawnictwo Naukowo-Techniczne, Warszawa 1998.

7. Lech Banachowski, Bazy Danych – Tworzenie aplikacji, Akademicka Oficyna Wydawnicza PLJ, Warszawa 1998.

Przygotował: A. Kaczmarek