GIODO

Generalny Inspektor
Ochrony Danych Osobowych

ABC

bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych

WYDAWNICTWO SEJMOWE
Warszawa 2007

BIURO GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH

ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl
tel. (022) 860 70 81
fax (022) 860 70 86

Opracował Andrzej Kaczmarek
Dyrektor Departamentu Informatyki

Redaktor Andrzej Rudnicki

ISBN 978-83-7059-846-4

KANCELARIA SEJMU

Wydawnictwo Sejmowe
Wydanie pierwsze
Warszawa, listopad 2007

SPIS TREŚCI

WPROWADZENIE

Zgodnie z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2002 r. nr 101 poz. 926, z późn. zm.; dalej jako: ustawa), administrator danych osobowych zobowiązany jest do zapewnienia ochrony przetwarzanych danych osobowych *przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem*. Jakość zapewnianej ochrony powinna być odpowiednia do zagrożeń oraz kategorii danych nią objętych. Ponadto zgodnie z art. 38 ustawy *administrator danych zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane*.

Ten ostatni wymóg, pomimo że umieszczony został w rozdziale 5 ustawy dotyczącym zabezpieczenia przetwarzanych danych, odnosi się nie tylko do kwestii bezpieczeństwa, ale również – odpowiednich funkcjonalności przyjętego systemu przetwarzania. Funkcjonalności te wynikają z kolei nie tylko z potrzeby zapewnienia bezpieczeństwa danych, ale również z konieczności zapewnienia określonych właściwości oraz warunków umożliwiających administratorowi realizację zobowiązań wobec podmiotów danych wynikających z art. 32 i 33 ustawy i § 7 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; dalej jako: rozporządzenie). Wymagane w przywołanych przepisach obowiązki sprowadzają się m.in. do zapewnienia i udostępniania – na żądanie osoby, której dane są przetwarzane – informacji o:

1) dacie, od kiedy przetwarza się w zbiorze jej dane osobowe, oraz treści tych danych,
2) źródle, z którego pochodzą dane jej dotyczące, chyba że administrator jest obowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej,
3) sposobie i zakresie udostępniania jej danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
4) sposobie, w jaki zebrano dane.

Ogólnie przez pojęcie zapewnienia ochrony przetwarzanym danym należy rozumieć działanie mające na celu zabezpieczenie przed czymś złym, niekorzystnym, niebezpiecznym. W odniesieniu do danych osobowych będą to działania mające na celu zapewnienie, aby były one pozyskiwane i przetwarzane zgodnie z przepisami prawa. Oznacza to miedzy innymi, że powinny być one wykorzystywane tylko w określonym celu, zabezpieczone przed nieuprawnionymi zmianami, ujawnieniem nieupoważnionym osobom, zniszczeniem, utratą lub uszkodzeniem.

Czynności podejmowane w ramach tych działań oraz zastosowane środki techniczne i organizacyjne będą zależne od środowiska, w jakim dane są przetwarzane.

W niniejszym opracowaniu zostały omówione zagadnienia związane z zapewnieniem ochrony danych przetwarzanych przy użyciu systemów informatycznych. Pojęcie „ochrony danych" należy w tym przypadku utożsamiać z pojęciem „bezpieczeństwa informacji", stosowanym w literaturze z zakresu bezpieczeństwa teleinformatycznego. Według normy PN-ISO/IEC-17799:2005[1] przez bezpieczeństwo informacji należy rozumieć zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności. Wymienione właściwości, wg definicji zawartych w PN-I-13335-1[2], polegają odpowiednio na:

[1] *PN-SIO/IEC-17799:2005 Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, 2007.*

[2] *PN-I-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999.*

Poufność	– zapewnieniu, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
Integralność	– zapewnieniu, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
Dostępność	– zapewnieniu bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
Rozliczalność	– zapewnieniu, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
Autentyczność	– zapewnieniu, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
Niezaprzeczalność	– braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
Niezawodność	– zapewnieniu spójności oraz zamierzonych zachowań i skutków.

Należy zwrócić uwagę, że zapewnienie a następnie wykazanie określonych właściwości wymaga często zastosowania określonych środków i jednoczesnego spełnienia wielu warunków. Zapewnienie np. niezaprzeczalności podpisu elektronicznego (wykazanie, że dany dokument elektroniczny podpisała określona osoba) wymaga udowodnienia, że dany dokument nie został zmieniony (integralność), a złożony podpis należy do danej osoby (uwierzytelnienie).

Gdy do przetwarzania danych osobowych wykorzystuje się systemy informatyczne, zadania dotyczące zapewnienia określonych właściwości przenoszone są na odpowiednie wymagania dotyczące właściwości tych systemów. Dodatkowy problem, jaki wówczas powstaje, polega na zapewnieniu skuteczności i ciągłości zachowywania przez systemy informatyczne wymaganych właściwości. Właściwości te mogą być utracone na skutek błędów popełnionych przez administratora systemu lub celowych działań osób nieupoważnionych do ingerowania w dany system informatyczny. W konsekwencji, oprócz działań mających na celu

ochronę przetwarzanych danych, należy zapewnić również ochronę systemu informatycznego, którego użyto do ich przetwarzania. Stąd też w przepisach wykonawczych do ustawy, wydanych na podstawie delegacji zawartej w art. 39a, określone zostały wymagania dotyczące nie tylko polityki bezpieczeństwa, ale również systemu informatycznego oraz sposobu zarządzania nim.

1. POLITYKA BEZPIECZEŃSTWA

1.1. Uwagi ogólne

Zgodnie z § 3 i § 4 rozporządzenia 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 dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz określonej organizacji[3]. Należy zaznaczyć, że zgodnie z art. 36 ust. 2 oraz art. 39a ustawy, 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. Jej celem jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.

Polska Norma PN-ISO/IEC 17799:2005[4], określająca praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych, jako cel polityki bezpieczeństwa wskazuje „*zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji*". Należy przy tym podkreślić, że dokument polityki bezpieczeństwa powinien deklarować zaangażowanie kierownictwa i wyznaczać

[3] *PN-I-02000: Zabezpieczenia w systemach informatycznych – Terminologia, PKN, 1998.*

[4] *PN-SIO/IEC-17799:2005 Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, 2007.*

podejście instytucji do zarządzania bezpieczeństwem informacji. Jako minimum w powyższej normie wskazuje się, aby dokument określający politykę bezpieczeństwa zawierał:

a) mechanizm umożliwiający współużytkowanie informacji (patrz Wprowadzenie);
b) oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji w odniesieniu do strategii i wymagań biznesowych;
c) strukturę wyznaczania celów stosowania zabezpieczeń, w tym strukturę szacowania i zarządzania ryzykiem;
d) krótkie wyjaśnienie polityki bezpieczeństwa, zasad, norm i wymagań zgodności mających szczególne znaczenie dla organizacji, zawierające:
  1) zgodność z prawem, regulacjami wewnętrznymi i wymaganiami wynikającymi z umów;
  2) wymagania dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa;
  3) zarządzanie ciągłością działania biznesowego;
  4) konsekwencje naruszenia polityki bezpieczeństwa;
e) definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania incydentów związanych z bezpieczeństwem informacji;
f) odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dotyczących poszczególnych systemów informatycznych lub zalecanych do przestrzegania przez użytkowników zasad bezpieczeństwa.

Powyższe zalecenia w pełni można stosować do dokumentacji polityki bezpieczeństwa, o której mowa w § 4 rozporządzenia. Dokument określający politykę bezpieczeństwa nie może mieć zbyt abstrakcyjnego charakteru. Zasady postępowania w niej wskazane powinny zawierać uzasadnienie wyjaśniające przyjęte standardy i wymagania. Jeżeli ma to miejsce, to rzadziej dochodzi do ich naruszenia[5].

Dokument, o którym mowa w § 4 rozporządzenia, w zakresie przedmiotowym powinien koncentrować się na bezpieczeństwie przetwarza-

[5] Tomasz Pełech, *Stosowanie zabezpieczeń danych w systemach korporacyjnych: dobra wola czy prawny obowiązek?*, „Gazeta IT" nr 18, listopad 2003 r.

nia danych osobowych, co wynika z art. 36 ustawy. Prawidłowe zarządzanie zasobami, w tym również informacyjnymi, zwłaszcza w aspekcie bezpieczeństwa informacji, wymaga właściwej identyfikacji tych zasobów[6] 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 urządzeń, sprzętu komputerowego i oprogramowania. Stąd też w § 4 rozporządzenia wskazano, że polityka bezpieczeństwa powinna zawierać w szczególności następujące punkty:

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 przy przetwarzaniu danych.*

1.2. 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, 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 te miejsca, w których wykonuje się operacje na nich (wpisuje, modyfikuje, kopiuje), jak również te, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową bądź komputerowymi nośnikami 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 rozporządzenia miejsce przetwarzania danych osobowych powinno być określone poprzez wskazanie budynków, pomieszczeń lub części pomieszczeń, w których przetwarza się dane osobowe. Do obszaru przetwarzania danych należy zaliczyć również pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, niesprawne komputery i inne urządzenia z nośnikami zawierającymi dane osobowe). Do obszaru przetwarzania danych osobowych ich administrator 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.

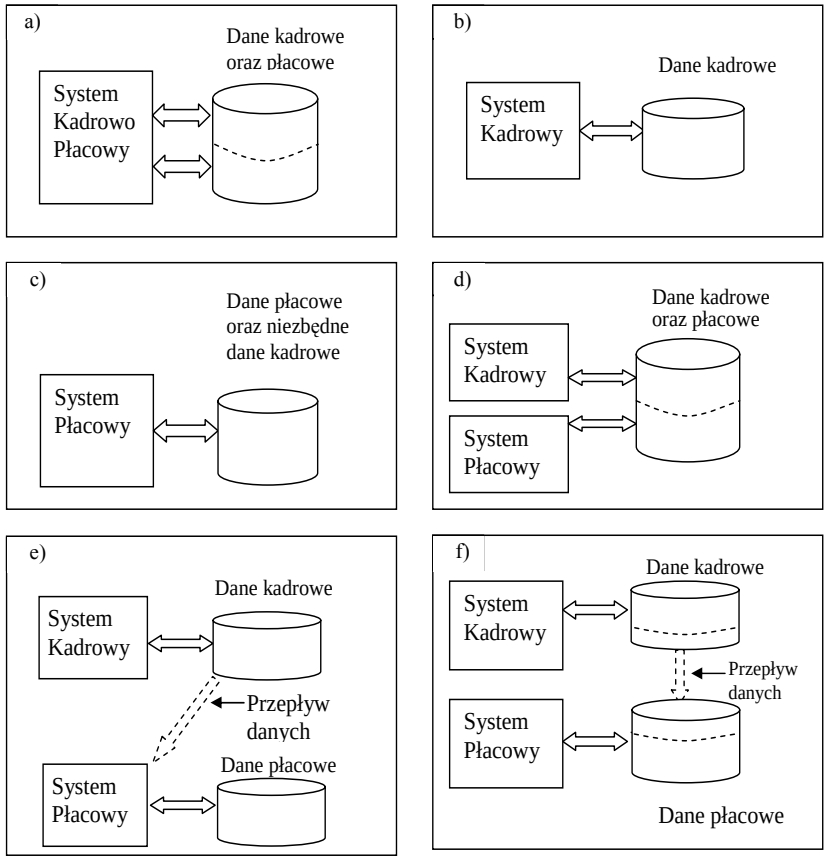
Jeżeli dane osobowe przetwarzane są w systemie informatycznym, do którego dostęp poprzez sieć telekomunikacyjną posiada wiele podmiotów, to w polityce bezpieczeństwa informacje o tych podmiotach (jego nazwa, siedziba, pomieszczenia, w których przetwarzane są dane) powinny być również wymienione jako 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), a także systemów, do których dostęp z założenia ma charakter publiczny (np. książka telefoniczna zamieszczona w Internecie). W wyżej wymienionych sytuacjach wystarczające jest wskazanie zarówno tych budynków i pomieszczeń, gdzie dane są przetwarzane przez administratorów systemu informatycznego, jak i tych, w których dostęp do danych uzyskują osoby posiadające szerszy zakres uprawnień niż tylko wgląd do swoich własnych danych lub danych udostępnianych publicznie.

[6] *PN-I-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999.*

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

Ważnym elementem identyfikacji 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. Gdy system zbudowany jest z wielu modułów programowych i mogą one 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 zarówno w jednym, jak i wielu zbiorach. Sytuacja może być również odwrotna, kiedy to wiele różnych programów przetwarza dane stanowiące jeden zbiór. Programami tymi są najczęściej moduły zintegrowanego systemu. Każdy taki moduł przeznaczony jest do wykonywania określonych, wydzielonych funkcjonalnie zadań. Przykładem mogą być systemy kadrowy oraz płacowy, które często występują jako jeden zintegrowany system kadrowo-płacowy. Programy informatyczne mogą być zintegrowane tworząc jeden system, z jednym lub wieloma zbiorami danych (przykłady możliwych w tym zakresie konfiguracji przedstawia rys. 1).

Z powyższego wynika, że 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 precyzujące lokalizację miejsca (budynek, pomieszczenie, nazwa komputera lub innego urządzenia, np. macierzy dyskowej, biblioteki optycznej), w którym znajdują się zbiory danych osobowych przetwarzane na bieżąco oraz nazwy i lokalizacje programów (modułów programowych) używanych do ich przetwarzania.



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

1.4. 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 jego struktury i zakres informacji w nim gromadzonych. Opisy poszczególnych pól informacyjnych w strukturze zbioru danych powinny jednoznacznie wskazywać, jakie kategorie danych są w nich przechowywane. Opis pola danych, 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 wypadku wyrażenia zgody lub literę „N" w razie jej braku. Brak stosownego opisu może spowodować inne niż zakładano sposoby zapisu oraz interpretacji określonej informacji.

Przykładowo, jeśli w zbiorze przetwarzane są informacje o danych adresowych klienta, zamówieniach klientów oraz sprzedawanych towarach (w zakresie przedstawionym w tabeli 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].

Tabela 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 przetwarzanych o kliencie danych (oznaczony wyżej jako „Zakres 1"), jak łatwo zauważyć, powstał na skutek relacji, jaka istnieje pomiędzy obiektami „dane adresowe klienta" i „zamówienia klienta". Relacja ta (rys. 2) 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 znajdują się w tym

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

samym zbiorze danych, nie poszerzają zakresu danych o kliencie, oznaczonym jako „Zakres 1”.

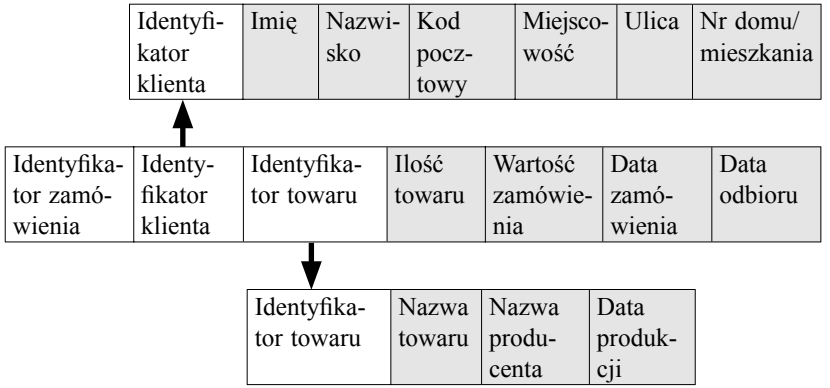
Jeżeli chodzi o relacyjne bazy danych, to praktycznie każdą informację można zapisać poprzez utworzenie odpowiedniej relacji. Dla struktury przedstawionej w tabeli 1 informacje o nazwie zamawianego towaru w zamówieniach klientów można zapisać alternatywnie w postaci relacji, co pokazuje tabela 2, a także rys. 3.

Tabela 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 opisami poszczególnych obiektów w istotny sposób wpływają na rzeczywisty zakres przetwarzanych informacji o wskazanym obiekcie.

Skróty i oznaczenia poszczególnych kategorii danych oraz indeksy i klucze wprowadzane ze względów technicznych 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. Zatem, 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. Przy opisie 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. Są to obiekty zapisane w bazie danych, tak jak inne dane. Mogą być nimi procedury i funkcje, które mogą być później używane przez aplikacje służące do przetwarzania danych. Pro-

cedury, które uruchamiane są przy zajściu określonego zdarzenia nazywane są wyzwalaczami (ang. *Trigger*)[7].

Wymóg wskazania powiązań pomiędzy polami informacyjnymi w strukturze zbiorów danych, określony w § 4 pkt 3 rozporządzenia, należy rozumieć jako wymóg wskazania wszystkich tych danych znajdujących się w strukturze zbioru, które poprzez występujące relacje można skojarzyć z określoną osobą. Przykładowo, ze struktury zbioru pokazanej w tabeli 1 wynika, iż do danych, które można skojarzyć z osobą o podanym imieniu i nazwisku, należą nie tylko dane zawarte w stosownej części tej tabeli, ale również dane znajdujące się w obiekcie o nazwie „zamówienia klienta". Połączenie to, zgodnie z definicją danych osobowych, powoduje poszerzenie zakresu 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 tabelach 1, 2), w postaci graficznej pokazującej istniejące powiązania pomiędzy obiektami (rys. 1, 2), jak również w formie opisu tekstowego, który dla przypadku wskazanego w tabeli 1 może być następujący:

W zbiorze danych przetwarzane są dane osobowe klientów w zakresie:

1) *danych adresowych klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu), oraz*
2) *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 przedstawiona w tekście poprzez wskazanie w punkcie 2, 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 1).

[7] Tomasz Pełech, *Stosowanie zabezpieczeń danych w systemach korporacyjnych: dobra wola czy prawny obowiązek?*, „Gazeta IT" nr 18, listopad 2003 r.

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

1.5. Sposób przepływu danych pomiędzy poszczególnymi systemami (§ 4 pkt 4 rozporządzenia)

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 (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 opisie sposobu 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). Taki przepływ występuje np. często pomiędzy systemami kadrowym i płacowym (rys. 1 pkt f) oraz pomiędzy systemami kadrowym i płacowym a systemem płatnik służącym do rozliczeń pracowników z ZUS. Dla identyfikacji procesów przetwarzania danych osobowych szczególne znaczenie ma specyfikacja ich przepływu w systemach z rozproszonymi bazami danych. Chodzi tu o sytuację, w której poszczególne podzbiory zlokalizowane są w różnych miejscach oddalonych od siebie terytorialnie i mogą zawierać, w zależności od lokalizacji, różne informacje (tzw. niejednorodne oraz federacyjne bazy danych)[8]. Dla systemów korporacyjnych o zasięgu międzynarodowym, informacja o przepływie danych pomiędzy oddziałami korporacji znajdującymi się w państwach nienależących do Europejskiego Obszaru Gospodarczego musi być traktowana jako prze-

[8] *Podstawy bezpieczeństwa systemów teleinformatycznych*, red. Andrzej Białas, Gliwice 2002; Paul Beynon-Davies, *Systemy baz danych*, Warszawa 1998.

pływ danych do państwa trzeciego[9] z wynikającymi z tego tytułu konsekwencjami[10]. W polityce bezpieczeństwa w punkcie określającym sposób przepływu danych pomiędzy systemami nie jest wymagane szczegółowe omawianie rozwiązań technologicznych. Najistotniejsze jest wskazanie zakresu przesyłanych danych, podmiotu lub kategorii podmiotów, do których są one przekazywane oraz ogólnych informacji na temat sposobów ich przesyłania (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 porównać do opisu relacji pomiędzy poszczególnymi polami informacyjnymi w strukturach zbiorów danych, co przedstawiono w punkcie 1.3. Przy przepływie danych pomiędzy systemami informatycznymi relacje, jakie powstają pomiędzy danymi przetwarzanymi w zbiorach poszczególnych systemów, nie wynikają z ich struktury. W razie 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 co do klasyfikacji poszczególnych systemów informatycznych z punktu widzenia kategorii przetwarzanych danych osobowych. Klasyfikacja ta powinna w szczególności wykazać, czy w danym systemie informatycznym są przetwarzane dane osobowe podlegające szczególnej ochronie, o których mowa w art. 27 ustawy, czy też nie. Informacje te uzupełnione o dane dotyczące środowiska pracy poszczególnych systemów oraz ich ewentualne połączenie z siecią publiczną powinny dać odpowiedź w kwestii wyboru odpowiedniego poziomu bezpieczeństwa, o czym mowa w § 6 rozporządzenia. Inaczej mówiąc, podsumowaniem wykazów i opisów, o których mowa w punktach 1, 2 i 3 polityki bezpieczeństwa powinno być wskazanie

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

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

w punkcie 4 wymaganych dla poszczególnych systemów informatycznych poziomów bezpieczeństwa.

1.6. 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, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności. Środki te powinny zapewnić zachowanie ww. właściwości dla wszelkich działań związanych z przetwarzaniem danych osobowych. Należy pamiętać, iż środki te powinny być określone po uprzednim przeprowadzeniu wnikliwej analizy zagrożeń i ryzyka związanych z przetwarzaniem danych osobowych. Analiza ta powinna obejmować cały proces przetwarzania danych osobowych i uwzględniać podatność stosowanych systemów informatycznych na określone zagrożenia. Przez „podatność systemu" należy rozumieć słabość w systemie, która może umożliwić zaistnienie zagrożenia, np. włamania do systemu i utraty poufności danych. Podatność taka może np. polegać na braku mechanizmu kontroli dostępu do danych, co może spowodować zagrożenie przetwarzania danych, przez nieupoważnione osoby. Analizując środowisko przetwarzania danych, należy ocenić ryzyko zaistnienia określonych zagrożeń. Ryzykiem tym może być prawdopodobieństwo wykorzystania określonej podatności systemu na istniejące w danym środowisku zagrożenia. Dlatego zastosowane środki techniczne i organizacyjne powinny być adekwatne do zagrożeń wynikających ze sposobu przetwarzania danych i środowiska, w jakim ten proces ma miejsce, a także do 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. 36–39 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 zabezpieczenia będą stosowane. Sygnalizacja istniejącego zagrożenia pozwala podjąć odpowiednie działania zapobiegawcze. Ważna jest często sama świadomość istnienia określonych zagrożeń, wynikających np. z przetwarzania danych w systemie informatycznym podłączonym do sieci Internet czy też 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. W takich sytuacjach prawidłowe opracowanie polityki bezpieczeństwa przetwarzania danych osobowych 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 dotyczące zarządzania i planowania bezpieczeństwa systemów informatycznych, opisane zostały m.in. w Polskich Normach[11].

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 (powinny być one zidentyfikowane po wykonaniu zadań wymienionych w punktach 2, 3 i 4 polityki bezpieczeństwa) niezbędne jest zapewnienie środków bezpieczeństwa spełniających co najmniej minimalne wymagania określone w załączniku do rozporządzenia.

[11] *PN-SIO/IEC-17799:2005 Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, 2007; PN-I-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999.*

Opis środków, o których mowa w § 4 pkt 5 rozporządzenia, powinien obejmować zarówno środki techniczne, jak i organizacyjne. Przykładowo w odniesieniu do stosowanych mechanizmów uwierzytelniania powinny być wskazane i opisane zarówno zagadnienia dotyczące uwierzytelnienia użytkowników w systemach informatycznych, jak i odnoszące się do uwierzytelnienia przy wejściu (wyjściu) do określonych pomieszczeń, a także sposób rejestracji wejść (wyjść) itp. W wypadku stosowania narzędzi specjalistycznych (np. zapór ogniowych – chroniących system informatyczny przed atakami z zewnątrz; systemów wykrywania intruzów – ang. *Intrusion Detection System* – IDS), należy wskazać w polityce bezpieczeństwa, czy 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 tego dotyczące powinny być objęte stosowną ochroną przed dostępem do nich osób nieupoważnionych.

1.7. Zapewnienie dokumentacji i ciągłości doskonalenia zabezpieczeń

W celu należytego wykonania ww. zadań art. 36 ust. 2 ustawy zobowiązuje administratorów danych do prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zastosowane w celu zapewnienia ich ochrony. Z kolei ust. 3 obliguje administratora do wyznaczenia administratora bezpieczeństwa informacji, nadzorującego przestrzeganie przyjętych zasad i monitorującego skuteczność działania zastosowanych środków ochrony. Jest to konieczne ze względu na złożoność problemu stosowania zabezpieczeń, na którą składają się czynniki stawiające broniącego na pozycji gorszej od atakującego[12]. Do czynników tych należą: asymetria, zależność od otoczenia oraz ciągłość działania. Asymetria działań mających na celu zabez-

[12] http://wazniak.mimuw.edu.pl – informacje publikowane w ramach projektu *Opracowanie programów nauczania na odległość na kierunku studiów wyższych – Informatyka* sfinansowanego ze środków Europejskiego Funduszu Społecznego z programu *Sektorowy Program Operacyjny Rozwój Zasobów Ludzkich 2004–2006*.

pieczenie systemu polega na tym, że: aby skutecznie zabezpieczyć system należy usunąć wszystkie słabości, podczas gdy wystarczy znaleźć jedną, aby skutecznie zaatakować.

Zależność od otoczenia – to z kolei wpływ całego otoczenia systemu, środowiska informatycznego, w jakim dany system przetwarzania danych funkcjonuje, na jego bezpieczeństwo. Inne zagrożenia wystąpią np. w sieci lokalnej określonej organizacji, niemającej styku z siecią publiczną, a inne, gdy dany system funkcjonuje w środowisku sieci Internet.

Ciągłość działania to z kolei wymóg permanentnego monitorowania i aktualizacji zastosowanych środków bezpieczeństwa. Jakakolwiek zmiana struktury systemu czy też dodanie nowych usług każdorazowo wymaga jego weryfikacji pod względem zagrożeń i ryzyka, na jakie przetwarzane dane mogą być narażone i tym samym – weryfikacji zastosowanych środków bezpieczeństwa.

2. PODSTAWOWE WYMAGANIA DOTYCZĄCE FUNKCJONALNOŚCI SYSTEMU INFORMATYCZNEGO

W odniesieniu do systemów informatycznych ustawa wprowadziła szereg przepisów dotyczących zarówno ich bezpieczeństwa, jak i funkcjonalności. Celem tych regulacji jest zapewnienie, aby systemy informatyczne, używane do przetwarzania danych osobowych, posiadały takie funkcje i mechanizmy, które będą wspomagały administratora w wywiązywaniu się z nałożonych na niego obowiązków. Wymagania te można podzielić najogólniej na dwie grupy. Pierwsza – to wymagania mające na celu zapewnienie ścisłej kontroli nad przetwarzanymi danymi. Natomiast druga – to wymagania wynikające z uprawnień osób, których dane są przetwarzane.

2.1. Minimalne wymagania wynikające z potrzeb zapewnienia bezpieczeństwa

W tej grupie wymagań funkcjonalnych wymienione są warunki, jakim powinny odpowiadać systemy informatyczne, aby zapewnić przetwarzanym danym bezpieczeństwo przed ich nieuprawnionym ujawnieniem, zmianami lub zniszczeniem. Wymagania te wynikają wprost z obowiązku zabezpieczenia danych (art. 36 ustawy) i zachowania nad nimi kontroli (art. 37 i 38 ustawy). Konkretne środki, jakie należy zastosować, będą zależne od infrastruktury technicznej i wielkości używanego systemu informatycznego. Minimalne wymogi, jakie powinny być spełnione, określone zostały w załączniku do rozporządzenia. Uzależnione są one od ryzyka i zagrożeń, na jakie narażone są przetwarzane dane.

2.1.1. Minimalne wymagania funkcjonalne dotyczące kontroli dostępu do danych

Minimalne wymagania dotyczące funkcjonalności używanego do przetwarzania danych systemu informatycznego określone zostały w części A ww. załącznika w punkcie II, który brzmi: *W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.*

Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;

b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

Z przepisu tego wynika, że – poza wyjątkiem, kiedy dane przetwarzane są przy użyciu jednego komputera, przez jedną osobę – system informatyczny wykorzystywany do przetwarzania danych musi być wyposażony w mechanizmy kontroli dostępu. Ustawodawca przy nakładaniu tego obowiązku wyszedł z założenia, że gdy dostęp do danych posiada wyłącznie jedna osoba, w celu zapewnienia informacji o tym, kto wprowadził dane do tego systemu wystarczy zabezpieczyć cały system przed dostępem innych osób. W praktyce oznacza to, że system taki

może być zainstalowany wyłącznie na jednej stacji komputerowej, do której dostęp jest ograniczony tylko dla jednej osoby.

We wszystkich pozostałych sytuacjach dostęp do systemu informatycznego zabezpieczony powinien być za pomocą mechanizmów uwierzytelnienia, gdzie każdemu użytkownikowi przypisuje się jednoznaczny identyfikator oraz dane służące uwierzytelnieniu. W celu uzyskania dostępu do tak zabezpieczonego systemu użytkownik musi wprowadzić swój identyfikator i przypisane mu dane uwierzytelniające. Kontrolę dostępu uzyskuje się w tym wypadku poprzez przypisanie w systemie danemu użytkownikowi odpowiednich uprawnień, a także poprzez zapewnienie, że dane służące uwierzytelnieniu zna tylko użytkownik, którego one dotyczą. Dostęp do określonych informacji czy też funkcji służących wykonywaniu określonych operacji na danych powinien być przyznawany zgodnie z nadanymi dla konkretnego użytkownika uprawnieniami. Ponadto, wykonywane przez niego operacje (w razie ich rejestrowania) powinny być opatrywane jego identyfikatorem. W szczególności, gdy przedmiotem wykonywanych operacji jest wprowadzenie danych osobowych, w bazie systemu wraz z wprowadzonymi danymi powinien być odnotowany identyfikator użytkownika, który wprowadzał te dane i data ich wprowadzenia.

2.1.2. Minimalne wymagania dotyczące systemu uwierzytelnienia

W rozporządzeniu nie określa się metod uwierzytelnienia, jakie powinny być stosowane. Może to być jedna z trzech znanych, wymienionych poniżej metod lub dowolna ich kombinacja.

Najbardziej znane metody uwierzytelnienia

Metoda wykorzystująca znany tylko danemu użytkownikowi sekret, nazywana również metodą typu **co wiem**. Jest najczęściej stosowana. Uwierzytelnienie użytkownika polega w niej na wprowadzeniu identyfikatora i znanego tylko temu użytkownikowi hasła.

Metoda wykorzystująca posiadanie przedmiotu o określonych własnościach, nazywana również metodą typu **co posiadam**. Polega ona na weryfikacji cech dostarczonego przez uwierzytelniającą się osobę przedmiotu, np. karty magnetycznej, karty mikroprocesorowej tokenu, itp.

Metody wykorzystujące dane biometryczne charakterystyczne dla danego użytkownika, zwane metodami typu **kim jestem**. Uwierzytelnienie wykonywane jest w nich poprzez porównanie danych biometrycznych przypisanych w systemie użytkownikowi o danym identyfikatorze z danymi biometrycznymi charakteryzującymi uwierzytelniającą się osobę.

W razie wykorzystywania metody uwierzytelniania, bazującej na identyfikatorze użytkownika i haśle, wymagane jest, aby długość hasła składała się co najmniej z 6 znaków, gdy wymaganym poziomem bezpieczeństwa jest poziom podstawowy, i 8 znaków, jeśli mamy do czynienia z podwyższonym lub wysokim poziomem bezpieczeństwa. Ten ostatni wymóg zapisany jest w części B ww. załącznika, w punkcie VIII, który brzmi następująco: *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.*

2.2. Minimalne wymagania funkcjonalne wynikające z obowiązku informacyjnego

Wymagania dotyczące obowiązku informacyjnego określają zakres danych, jakie powinny być rejestrowane w systemie informatycznym. Ich posiadanie przez administratora danych jest niezbędne dla wykonania obowiązku informacyjnego określonego w art. 32 ust. 1 pkty 3–5 ustawy. Stanowią one, że: *każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:*

[...]

3) *uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych,*
4) *uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej,*
5) *uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane.*

Sposób wykonania tego obowiązku sprecyzowany został w § 7 ust. 1 rozporządzenia, którego treść jest następująca: *Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten zapewnia odnotowanie:*

1) *daty pierwszego wprowadzenia danych do systemu;*
2) *identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;*
3) *źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;*
4) *informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;*
5) *sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.*

Łatwo zauważyć, że obligatoryjność odnotowywania daty wprowadzenia danych oraz identyfikatora użytkownika wynika, nie tylko z obowiązku informacyjnego, ale również z określonego w art. 38 ustawy, obowiązku zachowania kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone. Stąd też w przepisach rozporządzenia postawiono dodatkowe warunki dotyczące sposobu ich odnotowywania, mające zapewnić, aby dane nie mogły być modyfikowane przez użytkownika w sposób nieuprawniony. Warunki te określa § 7 ust. 2 rozporządzenia, stanowiąc, że *odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.*

2.3. Niestandardowe sposoby realizacji minimalnych wymagań funkcjonalnych

Standardowo, jeżeli system informatyczny, służący do przetwarzania danych osobowych, jest budowany z uwzględnieniem wymagań funkcjonalnych określonych w § 7 ust. 1 rozporządzenia, to wszystkie wymagane funkcjonalności powinny zostać wbudowane jako integralna

jego całość. W praktyce jednak bardzo często spotykane są rozwiązania cząstkowe, w których do przetwarzania danych używa się wielu różnych systemów dostosowanych do realizacji wąskiego zakresu zadań, instalowanych często na wydzielonych stanowiskach komputerowych. Systemy takie nie zawsze posiadają wszystkie wymagane funkcjonalności, o których mowa w § 7 ust. 1 rozporządzenia. Dotyczy to zwłaszcza funkcjonalności umożliwiającej odnotowywanie informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione oraz dacie i zakresie tego udostępnienia. Wyjściem ratunkowym dla administratora danych w takiej sytuacji jest rozwiązanie organizacyjne wskazane w § 7 ust. 4 rozporządzenia, które mówi, że *w przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.*

3. POZIOMY BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

Obowiązek stosowania przez administratorów danych odpowiednich zabezpieczeń systemu informatycznego zapisany został w art. 36–39a ustawy. W art. 36 ust. 1 wymaga się, aby administrator danych zastosował środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności, aby zabezpieczył *dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.*

W § 6 rozporządzenia wprowadzony został podział wymaganych zabezpieczeń na 3 następujące poziomy: podstawowy, podwyższony i wysoki.

Zabezpieczenia na poziomie co najmniej podstawowym należy stosować, gdy:

1) *w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 27 ustawy, oraz*

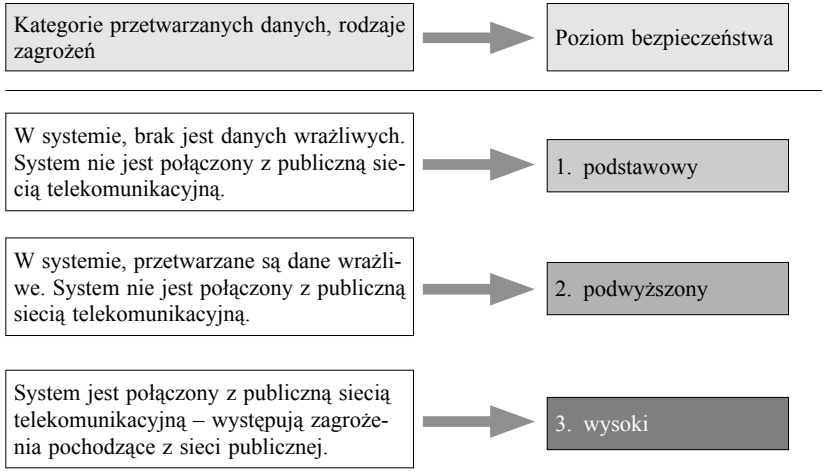
2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

Zabezpieczenia na poziomie co najmniej podwyższonym należy stosować, gdy:

1) w systemie informatycznym przetwarzane są dane osobowe, o których mowa w art. 27 ustawy, oraz

2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

Gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, należy stosować zabezpieczenia na poziomie wysokim. Powyższe zależności zostały przedstawione na rys. 4.



Rys. 4. Zależności pomiędzy zakresem przetwarzanych danych i zagrożeniem, na jakie są narażone, a wymaganym poziomem bezpieczeństwa

3.1. Poziom podstawowy

Podstawowy poziom bezpieczeństwa wymaga zastosowania określonych środków organizacyjnych oraz technicznych. Wykaz minimalnych środków bezpieczeństwa, jakie na tym poziomie, zgodnie z załącznikiem do rozporządzenia, powinny być zastosowane przedstawiono w tabeli 3.

Tabela 3. Wykaz minimalnych środków bezpieczeństwa wymaganych do osiągnięcia podstawowego poziomu bezpieczeństwa

Lp.	Opis wymaganych rozwiązań technicznych lub organizacyjnych
I.	*1. Obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.* *2. Przebywanie osób nieuprawnionych 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.*
II.	*1. W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.* *2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:* *a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;* *b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.*
III.	*System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:* *1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;* *2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.*
IV.	*1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony 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.*
V.	*Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.*

Lp.	Opis wymaganych rozwiązań technicznych lub organizacyjnych
VI.	*Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:* *1) likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;* *2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;* *3) naprawy pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.*
VII.	*Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.*

3.2. Poziom podwyższony

Gdy zakres przetwarzanych danych obejmuje dane wymienione w art. 27 ustawy i system nie jest narażony na zagrożenia z sieci publicznej, co praktycznie oznacza, że nie jest do niej podłączony, wówczas trzeba wprowadzić podwyższony poziom bezpieczeństwa. Aby to nastąpiło, należy zastosować wszystkie środki, wymagane dla osiągnięcia poziomu podstawowego oraz dodatkowo środki wymienione w tabeli 4.

Tabela 4. Wykaz dodatkowych w stosunku do poziomu podstawowego minimalnych środków bezpieczeństwa wymaganych do osiągnięcia podwyższonego poziomu bezpieczeństwa

Lp.	Opis wymaganych rozwiązań technicznych lub organizacyjnych
VIII.	*W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i w(ielkie litery oraz cyfry lub znaki specjalne.*
IX.	*Urządzenia i nośniki zawierające dane osobowe, o których mowa w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przekazywane poza obszar, o którym mowa w § 4 pkt 1 rozporządzenia, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.*
X.	*Instrukcję zarządzania systemem informatycznym, o której mowa w § 5 rozporządzenia, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika.*

3.3. Poziom wysoki

Wysoki poziom bezpieczeństwa systemu informatycznego jest wymagany wszędzie tam, gdzie systemy używane do przetwarzania danych połączone zostały z siecią wykorzystywaną do świadczenia usług publicznych. Jego zastosowanie jest wówczas niezbędne z uwagi na dodatkowe zagrożenia, jakie mogą pochodzić z tej sieci. Mogą to być próby „włamania" się do naszego systemu przez osoby nieuprawnione lub próby zniszczenia danych. Skutkiem przeprowadzonego ataku może być również zablokowanie możliwości korzystania z systemu poprzez przeciążenie komputera, na którym dany system został zainstalowany. Stąd też, oprócz środków wskazanych w punktach 3.1 i 3.2 zestawionych w tabelach 3 i 4, niezbędne jest zastosowanie środków wymienionych w tabeli 5.

Tabela 5. Wykaz dodatkowych w stosunku do poziomu podstawowego i podwyższonego minimalnych środków bezpieczeństwa wymaganych do osiągnięcia wysokiego poziomu bezpieczeństwa

Lp.	Opis wymaganych rozwiązań technicznych lub organizacyjnych
XII.	*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.*
XIII.	*Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.*

4. INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Jednym z wymogów nałożonych na administratorów danych, zgodnie z § 3 ust. 1 rozporządzenia, jest opracowanie instrukcji, określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zwanej dalej instrukcją.

Powinna być ona zatwierdzona przez administratora danych i przyjęta do stosowania, jako obowiązujący dokument. Zawarte w niej procedury i wytyczne powinny być przekazane osobom odpowiedzialnym w jednostce za ich realizację stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności. Np. zasady i procedury nadawania uprawnień do przetwarzania danych osobowych czy też sposób prowadzenia ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych powinny być przekazane osobom zarządzającym organizacją przetwarzania danych; sposób rozpoczęcia i zakończenia pracy, sposób użytkowania systemu czy też zasady zmiany haseł – wszystkim osobom będącym jego użytkownikami; zasady ochrony antywirusowej, a także procedury wykonywania kopii zapasowych – osobom zajmującym się techniczną eksploatacją i utrzymaniem ciągłości pracy systemu.

W treści instrukcji powinny być zawarte ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które są przy ich użyciu przetwarzane, zastosowane rozwiązania techniczne, jak również procedury eksploatacji i zasady użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych. Gdy administrator do przetwarzania danych wykorzystuje nie jeden, lecz kilka systemów informatycznych, wówczas stosownie do podobieństwa zastosowanych rozwiązań powinien opracować jedną, ogólną instrukcję zarządzania lub oddzielne instrukcje dla każdego z użytkowanych systemów. Zatem inny będzie zakres opracowanych zagadnień w małych podmiotach, w których dane osobowe przetwarzane są przy pomocy jednego lub kilku komputerów, a inny w dużych, w których funkcjonują rozbudowane lokalne sieci komputerowe z dużą ilością serwerów i stacji roboczych przetwarzających dane przy użyciu wielu systemów informatycznych.

W instrukcji powinny być wskazane systemy informatyczne, ich lokalizacje i stosowane metody dostępu (bezpośrednio z komputera, na którym system jest zainstalowany, w lokalnej sieci komputerowej czy też poprzez sieć telekomunikacyjną, np. łącze dzierżawione, Internet). Instrukcja ma obejmować zagadnienia dotyczące bezpieczeństwa informacji, a w szczególności elementy wymienione w § 5 rozporządzenia, na które składają się:

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 rozporządzenia,*
8) *procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.*

W celu zapewnienia ochrony przetwarzanym danym, w odniesieniu do każdego z wymienionych wyżej punktów, w treści instrukcji powinny być wskazane odpowiednie dla stosowanych systemów informatycznych zasady postępowania. Poniżej przedstawiono ogólne wskazówki w tym zakresie.

4.1. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności (§ 5 pkt 1 rozporządzenia)

W punkcie tym powinny zostać opisane zasady przyznawania użytkownikowi systemu informatycznego identyfikatora, jak również zasady nadawania lub modyfikacji uprawnień dostępu użytkownika do zasobów systemu informatycznego. Zasady te powinny obejmować operacje związane z nadawaniem użytkownikom uprawnień do pracy w systemie informatycznym począwszy od utworzenia użytkownikowi konta, poprzez przydzielanie i modyfikację jego uprawnień, aż do momentu usunięcia konta z systemu informatycznego. Procedura określająca zasady rejestracji użytkowników powinna w sposób jednoznaczny określać zasady postępowania z hasłami użytkowników uprzywilejowanych (tzn. użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych), jak również zasady administrowania systemem informatycznym w przypadkach awaryjnych, np. nieobecności administratora.

W instrukcji należy wskazać osoby odpowiedzialne za realizację procedury określającej zasady przyznawania uprawnień do korzystania z systemów informatycznych oraz za realizację związanych z tym czynności technicznych takich, jak rejestrowanie i wyrejestrowywanie użytkowników, którym uprawnienia te zostały nadane.

4.2. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem (§ 5 pkt 2 rozporządzenia)

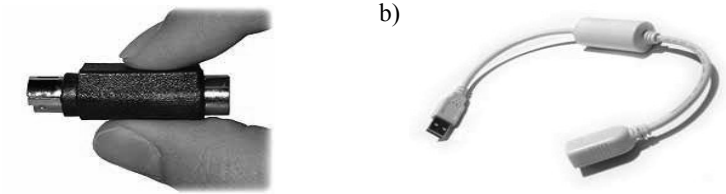
W punkcie tym powinien zostać opisany tryb przydzielania haseł, tj. wskazanie, czy hasła użytkowników przekazywane mają być w formie ustnej czy pisemnej oraz wskazanie zaleceń dotyczących stopnia ich złożoności. Powinny zostać również wskazane, funkcjonalnie lub personalnie, osoby odpowiedzialne za przydział haseł. Zaleca się, aby unikać przekazywania haseł przez osoby trzecie lub za pośrednictwem niechronionych wiadomości poczty elektronicznej. Użytkownik

po otrzymaniu hasła powinien być zobowiązany do niezwłocznej jego zmiany, chyba że system nie umożliwia wykonania takiej operacji. W zależności od stosowanych rozwiązań należy podać dodatkowe informacje dotyczące haseł (np. wymogi dotyczące ich powtarzalności czy też zestawu tworzących je znaków). Powinna być również zawarta informacja o wymaganej częstotliwości i metodzie zmiany hasła – np. czy zmiana hasła wymuszana jest po określonym czasie przez system informatyczny, czy też użytkownik sam musi o tym pamiętać. Przy określaniu częstotliwości zmiany haseł należy pamiętać, iż hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni i składać się co najmniej z 6 lub 8 znaków – w zależności od tego, czy w systemie są przetwarzane dane wrażliwe, o których mowa w art. 27 ustawy (załącznik do rozporządzenia pkt IV ppk 2 w zw. z pkt VII).

Hasła w systemie informatycznym powinny być przechowywane w postaci zaszyfrowanej. Należy wskazać sposób przechowywania haseł użytkowników posiadających uprawnienia administratorów systemów informatycznych oraz sposób odnotowywania ich awaryjnego użycia. Dodatkowo w razie zastosowania innych, niż identyfikator i hasło, metod weryfikacji tożsamości użytkownika (np. kart mikroprocesorowych czy też metod biometrycznych), w instrukcji powinny być zawarte wytyczne dotyczące ich stosowania. Przykładowo dla kart mikroprocesorowych należy wskazać sposób ich personalizacji, zaś dla metod biometrycznych – sposób pobierania danych biometrycznych w procesie rejestrowania użytkownika w systemie oraz sposób ich przechowywania.

Ponadto w tej części instrukcji należy poinformować użytkownika o możliwych zagrożeniach i konsekwencjach związanych z tzw. utratą tożsamości elektronicznej (tj. utratą danych służących uwierzytelnieniu, co może skutkować pozyskaniem tych danych przez osoby nieuprawnione), a przede wszystkim – o konieczności przestrzegania obowiązku ochrony miejsca przetwarzania danych przed dostępem osób nieupoważnionych. To zagrożenie może wystąpić, np. przy podłożeniu oprogramowania, które – jeśli użytkownik je zainstaluje – spowoduje przejęcie przez osobę nieuprawnioną danych służących uwierzytelnieniu (identyfikatora i hasła) lub podłączenie w tym celu w sposób niezauważony odpowiednich urządzeń nazywanych keyloggerami (rys. 5).

a) b)



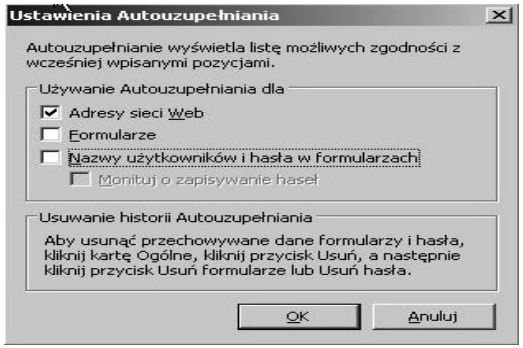
c)

Rys. 5. Urządzenia nazywane keyloggerami, służące do rejestracji wszelkich operacji wykonywanych przy użyciu klawiatury: a) keylogger w postaci „przejściówki" włączanej do gniazda, w które włącza się klawiaturę; b) keylogger w postaci przedłużacza do klawiatury; c) keylogger wbudowany w klawiaturę

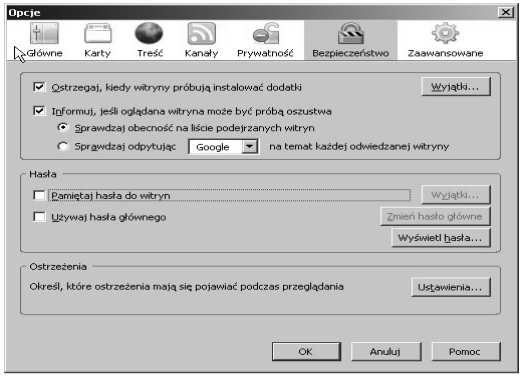
Pokazane na rys. 5 urządzenia mogą być wykorzystane do zebrania wszystkich danych wprowadzanych do systemu za pomocą klawiatury.

W razie korzystania z systemów podłączonych do sieci publicznej, należy szczegółowo opisać sposób korzystania z używanych przeglądarek internetowych. W szczególności trzeba określić zasady dotyczące miejsca przechowywania haseł do aplikacji internetowych, z których użytkownicy będą korzystać. Dobrą praktyką jest wówczas zalecenie zablokowania możliwości zapamiętywania haseł na stacji komputerowej, co dla przeglądarki Internet Explorer oraz Mozilla Firefox pokazano na rys. 6.

a)



b)



Rys. 6. Ustawienie przeglądarki – a) Internet Explorer oraz b) Mozilla Firefox – w taki sposób, aby komputer nie zapamiętywał haseł w formularzach logowania do aplikacji internetowych

4.3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu (§ 5 pkt 3 rozporządzenia)

W punkcie tym powinny być wskazane kolejne czynności, jakie należy wykonać w celu uruchomienia systemu informatycznego, a w szczególności zasady postępowania użytkowników podczas przeprowadzania procesu uwierzytelniania się (logowania się do systemu). Przestrzeganie określonych w instrukcji zasad powinno zapewniać zachowanie poufno-

ści haseł oraz uniemożliwiać nieuprawnione przetwarzanie danych. Należy również określić metody postępowania w sytuacji tymczasowego zaprzestania pracy na skutek opuszczenia stanowiska pracy lub w okolicznościach, kiedy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba. Użytkownik powinien być poinstruowany o konieczności wykonania operacji wyrejestrowania się z systemu informatycznego przed wyłączeniem stacji komputerowej oraz o czynnościach, jakie w tym celu powinien wykonać. Procedury przeznaczone dla użytkowników systemu powinny wskazywać sposób postępowania w sytuacji podejrzenia naruszenia bezpieczeństwa systemu, np. w razie braku możliwości zalogowania się użytkownika na jego konto czy też w sytuacji stwierdzenia fizycznej ingerencji w przetwarzane dane bądź użytkowane narzędzia programowe lub sprzętowe.

4.4. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania (§ 5 pkt 4 rozporządzenia)

W punkcie tym należy wskazać metody i częstotliwość tworzenia kopii zapasowych danych oraz kopii zapasowych systemu informatycznego używanego do ich przetwarzania. Należy określić, dla jakich danych wykonywane będą kopie zapasowe, typ nośników, na których będą one wykonywane oraz narzędzia programowe i urządzenia, które mają być do tego celu wykorzystywane. W procedurze powinien być określony harmonogram wykonywania kopii zapasowych dla poszczególnych zbiorów danych wraz ze wskazaniem odpowiedniej metody sporządzania kopii (kopia przyrostowa, kopia całościowa). Fragment instrukcji dotyczący wykonywania kopii zapasowych, gdy procedury ich wykonywania są złożone, może się odwoływać do procedur szczegółowych przypisanych poszczególnym zbiorom danych czy też systemom informatycznym. Procedury takie powinny być wówczas załączone do instrukcji zarządzania. W procedurach określających zakres i sposób wykonywania kopii zapasowych powinny być wskazane okresy rotacji oraz całkowity czas użytkowania poszczególnych nośników danych. Powinny być określone procedury likwidacji nośników zawierających kopie zapasowe danych po ich wycofaniu na skutek utraty przydatności

lub uszkodzenia. Procedura likwidacji nośników zawierających dane osobowe powinna uwzględniać wymogi zawarte w pkt VI ppkt 1 załącznika do rozporządzenia. Nakazują one, aby urządzenia, dyski lub inne informatyczne nośniki, przeznaczone do likwidacji, pozbawiać zapisu danych, a gdy nie jest to możliwe – uszkadzać w sposób uniemożliwiający ich odczytanie.

4.5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych, o których mowa w § 5 pkt 4 rozporządzenia (§ 5 pkt 5 rozporządzenia)

W tym punkcie instrukcji należy określić sposób i czas przechowywania wszelkiego rodzaju nośników informacji (dyskietki, płyty CD, taśmy magnetyczne), tj. wskazać pomieszczenia, przeznaczone do ich przechowywania, jak również sposób ich zabezpieczenia przed nieuprawnionym przejęciem, odczytem, skopiowaniem lub zniszczeniem.

Przy opracowywaniu zaleceń dotyczących sposobu i czasu przechowywania nośników informacji należy uwzględnić wymogi rozporządzenia w tym zakresie. Kopie zapasowe należy przechowywać w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem (pkt IV ppkt 4a załącznika do rozporządzenia), a kopie awaryjne należy bezzwłocznie usuwać po ustaniu ich użyteczności (pkt IV ppkt 4b załącznika do rozporządzenia).

W celu bezpiecznego przekazywania nośników informacji podmiotom zewnętrznym należy określić procedury i metody, dzięki którym informacje te będą chronione przed dostępem osób nieuprawnionych podczas ich transportu/przekazywania.

4.6. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia (§ 5 pkt 6 rozporządzenia)

W opisie zabezpieczeń systemu informatycznego przed działalnością oprogramowania należy określić obszary systemu informatycznego narażone na ingerencję wirusów komputerowych oraz wszelkiego rodzaju inne szkodliwe oprogramowanie. Trzeba wskazać możliwe źródła przedostania się szkodliwego oprogramowania do systemu oraz działania, jakie należy podejmować, aby minimalizować możliwość jego zainstalowania się. Niezależnie od wskazania w instrukcji tzw. profilaktycznych czynności należy przedstawić zastosowane narzędzia programowe, których zadaniem jest przeciwdziałanie skutkom szkodliwego działania takiego oprogramowania. Jeśli zostało zainstalowane oprogramowanie antywirusowe należy je wskazać. Ponadto trzeba określić metody i częstotliwość aktualizacji definicji wirusów oraz osoby odpowiedzialne za zarządzanie tym oprogramowaniem. Konieczne jest przedstawienie procedur postępowania użytkowników na okoliczność zidentyfikowania określonego typu zagrożeń. Użytkownik powinien być poinformowany o wskazówkach postępowania, gdyby oprogramowanie zabezpieczające wskazywało zaistnienie zagrożenia. Zdarza się, że zamiast oprogramowania antywirusowego stosowane są inne metody ochrony przed szkodliwym oprogramowaniem. Należy je również wyraźnie opisać. Mogą do nich należeć, np. fizyczne odłączenie urządzeń umożliwiających odczyt danych z wymiennych nośników informatycznych poszczególnych stacji komputerowych (np. odłączenie stacji CD, stacji dyskietek itp.), a także wyznaczenie wydzielonego stanowiska w sieci komputerowej do wymiany danych za pomocą nośników zewnętrznych.

4.7. Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia (§ 5 pkt 7 rozporządzenia)

Zgodnie z § 7 ust. 1 pkt 4 rozporządzenia dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system ten powinien zapewnić odnotowanie informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych. Wynika stąd, że system informatyczny wykorzystywany do przetwarzania danych osobowych powinien posiadać funkcjonalności umożliwiające odnotowanie wspomnianych wyżej informacji. Sposób oraz forma odnotowania, jak wynika z § 5 pkt 7 rozporządzenia, powinna zostać określona w instrukcji. Należy jednak zauważyć, iż nie jest wystarczające odnotowanie w formie papierowej informacji, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia, gdyż byłoby to niezgodne z przedstawioną w ustawie definicją systemu informatycznego.

Należy również podkreślić, że w razie przetwarzania danych osobowych nie tylko w jednym systemie informatycznym wymagania, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu. Wynika stąd, że odnotowanie informacji o udostępnieniach możliwe jest w jednym systemie tylko wtedy, gdy zbiór danych przetwarzany w dwóch lub więcej systemach dotyczy dokładnie tych samych osób. Przykładem takiej sytuacji jest korzystanie przez wiele aplikacji z tej samej bazy danych. Niedopuszczalne jest natomiast odnotowanie wskazanej informacji wyłącznie w jednym systemie, gdy grupy osób, których dane przetwarzane są w poszczególnych systemach nie są dokładnie tożsame. Gdy zbiór osób, których dane przetwarzane są w jednym systemie, różni się od zbioru osób, których dane przetwarzane są w drugim systemie i nie zachodzi relacja zawierania się pomiędzy tymi zbiorami, wówczas konieczne jest odnotowanie informacji o udostępnieniach odrębnie w każdym systemie obsługującym te zbiory lub ewentualnie w systemie przeznaczonym specjalnie do odnotowania tych informacji.

4.8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych (§ 5 pkt 8 rozporządzenia)

W punkcie tym należy określić cel, zakres, częstotliwość oraz procedury wykonywania przeglądów i konserwacji systemu informatycznego oraz podmioty i osoby do tego uprawnione. Procedury wykonywania czynności konserwacyjnych systemu, gdy zleca się je osobom nieposiadającym upoważnień do przetwarzania danych (np. specjalistom z firm zewnętrznych), powinny określać sposób nadzoru nad nimi przez administratora danych. W razie przekazywania do naprawy nośników informatycznych zawierających dane osobowe należy wcześniej wskazać sposób usuwania danych osobowych z tych nośników. W procedurach dotyczących naprawy sprzętu komputerowego należy uwzględnić wymóg, określony w punkcie VI ppkt 3 załącznika do rozporządzenia, który nakazuje, aby urządzenia, dyski lub inne elektroniczne nośniki informacji – zawierające dane osobowe, przeznaczone do naprawy – pozbawiać wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie bądź też naprawiać je pod nadzorem osoby upoważnionej przez administratora danych.

5. PYTANIA I ODPOWIEDZI

Zgodnie z ustawą nie trzeba rejestrować zbiorów danych osobowych, które służą tylko do przetwarzania danych w celu wystawienia faktury. Czy zwolnienie to zwalnia również administratora danych z obowiązku zabezpieczenia danych w tym zbiorze?

Wymogi dotyczące zabezpieczenia zbiorów danych osobowych, o których mowa w art. 36 ustawy, odnoszą się do wszystkich zbiorów, w których przetwarzane są dane osobowe. Obowiązek zabezpieczenia danych nie jest uzależniony od celu przetwarzania, rodzaju podmiotu będącego administratorem, jak również przywilejów, do których m.in. należy zwolnienie administratorów danych z obowiązku rejestracji określonego typu zbiorów.

Zwolnienie z obowiązku zgłoszenia zbioru danych osobowych do rejestracji, które dotyczy zbiorów wskazanych w art. 43 ust. 1 ustawy nie implikuje zwolnienia z innych obowiązków, w tym również z zabezpieczenia danych, o którym mowa w art. 36 ustawy.

Jeśli w bazie danych mam takie dane klienta, jak imię, nazwisko i adres, i użytkownik A po zalogowaniu się zobaczy jego dane (np. Jan Nowak), to czy do rejestru zdarzeń („logów") systemu należy wpisać informację w postaci: użytkownik A o godzinie 11:11:12 dnia 23 lipca 2006 r. widział dane klienta: Jan Nowak?

Obowiązek odnotowywania informacji o tym: komu, kiedy, jakie dane i w jakim celu zostały udostępnione, zgodnie z § 7 ust. 1 pkt 4 rozporządzenia, dotyczy tylko odbiorców danych. Użytkownik systemu przeglądający dane klienta lub klientów, który zgodnie z art. 7 pkt 6 lit. b ustawy musi być osobą upoważnioną do przetwarzania danych, nie jest odbiorcą danych. Stąd też należy stwierdzić, że z ustawy nie wynika obowiązek odnotowywania faktu zapoznania się użytkownika systemu z danymi osób, które są w nim zarejestrowane. Nie oznacza to jednak, że obowiązku takiego, w celu prowadzenia ścisłej kontroli dostępu do danych, nie mogą nakładać inne, odrębne przepisy.

Jeżeli zbiór danych znajduje się na stanowisku komputerowym wydzielonym z sieci, a jedynie proces zbierania danych osobowych odbywa się metodą teletransmisji poprzez sieć Internet, to czy konieczne jest zastosowanie wysokiego poziomu bezpieczeństwa w stosunku do komputera (sieci komputerowej) używanej wyłącznie do zbierania danych? Czy w razie zbierania danych osobowych drogą mailową konieczne jest stosowanie wysokiego poziomu zabezpieczeń?

Zgodnie z § 6 ust. 4 rozporządzenia wysoki poziom zabezpieczeń należy stosować w stosunku do komputera bądź sieci, które połączone są z siecią publiczną. Fakt zbierania danych przy użyciu poczty elektronicznej, która nie jest pocztą wewnętrzną funkcjonującą tylko w obrębie lokalnej sieci komputerowej, świadczy o tym, że sieć ta oraz podłączone do niej komputery, w tym ten, na którym odbierana jest poczta

elektroniczna, połączone są z siecią publiczną. Komputer ten należy zatem zabezpieczyć na poziomie wysokim.

Należy również zaznaczyć, że ankiety osobowe, które mają być przesyłane pocztą elektroniczną, powinny być zabezpieczone przed ujawnieniem osobom nieuprawnionym – poprzez zastosowanie odpowiednich środków kryptograficznych.

Jeżeli dla zbioru danych stosuje się wysoki poziom zabezpieczeń i zbieranie ich od podmiotów zewnętrznych odbywa się metodą teletransmisji poprzez sieć Internet, to czy konieczne jest zabezpieczenie procesu przesyłania danych za pomocą połączenia szyfrowanego protokołem SSL? Czy wpływ na zastosowanie tego instrumentu ma fakt przetwarzania danych wrażliwych?

Zgodnie z art. 36 ustawy administrator danych ma obowiązek zabezpieczenia danych m.in. przed ich nieuprawnionym ujawnieniem. W razie przesyłania danych metodą teletransmisji przy użyciu sieci publicznej zawsze istnieje możliwość przejęcia przesyłanych danych przez osobę nieuprawnioną. Istnieje również niebezpieczeństwo ich nieuprawnionej zmiany, uszkodzenia lub zniszczenia. Niezbędne jest zatem zastosowanie odpowiednich zabezpieczeń, które ochronią przesyłane dane. O tym, jakie środki należy zastosować, administrator danych powinien zdecydować samodzielnie. Może to być wymieniony w pytaniu protokół szyfrowania danych SSL, jak również inne środki ochrony kryptograficznej, np. szyfrowanie przy użyciu poczty elektronicznej i klucza publicznego odbiorcy.

Jestem odpowiedzialny za stworzenie dokumentów dotyczących ustawy w firmie liczącej około 1000 pracowników. Moje pytanie dotyczy dwóch punktów, które powinny być opisane w polityce bezpieczeństwa:

„Wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe" oraz

„Wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych".

Czy w ww. punktach należy umieścić spis wszystkich pracowników, komputerów i pokoi, w których są wprowadzane i modyfikowane dane osobowe, czy wystarczy tylko podać działy/piony, w których przetwarzane są dane?

Dokumentacja stanowiąca politykę bezpieczeństwa powinna zawierać w szczególności wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, jak również wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe należy rozumieć jako wyszczególnienie w sposób spójny i jednoznaczny miejsc, w których przetwarza się dane osobowe zarówno w zbiorach prowadzonych w postaci zwykłej (papierowej), jak i elektronicznej. Należy zauważyć, że miejscem, o którym mowa powyżej, może być zarówno obszar całego budynku lub budynków, obszar kilku wybranych pomieszczeń, jak i obszar stanowiący wydzieloną część danego pomieszczenia. Przykładowo, gdy upoważniony podmiot realizuje przetwarzanie danych osobowych we wszystkich pomieszczeniach budynku, wówczas zawartym w polityce bezpieczeństwa wykazem obszaru przetwarzania danych może być ogólna informacja, że miejscem przetwarzania danych osobowych są wszystkie pomieszczenia znajdujące się w budynku o danym adresie. Podobnie jest, gdy proces przetwarzania danych realizowany jest w pomieszczeniach zajmujących całe piętro budynku – w wykazie można wówczas opisać wszystkie pomieszczenia znajdujące się na danym piętrze budynku o wskazanym adresie. Wskazanie w sposób ogólny miejsca przetwarzania danych – rozumianego jako pomieszczenia stanowiące cały budynek, wybraną kondygnację budynku itp. – możliwe jest tylko wówczas, gdy we wszystkich pomieszczeniach tego obszaru podmiot przetwarza dane osobowe.

Wykaz zbiorów danych osobowych, wraz ze wskazaniem programów używanych do ich przetwarzania, powinien zawierać informacje o tym, jakie zbiory danych osobowych są przetwarzane przez podmiot oraz przy użyciu jakich systemów dane zawarte w tych zbiorach są przetwarzane.

Czy firma zajmująca się hostingiem stron internetowych (czyli dzierżawą miejsca na serwerze i świadczeniem usług dostępu do tych serwisów z Internetu) staje się podmiotem przetwarzającym dane w sytuacji, gdy hostowany serwis posiada w swej strukturze dane osobowe i mechanizmy je obsługujące?

Zgodnie z art. 31 ust. 1 ustawy powierzenie przetwarzania danych osobowych musi być dokonane w formie umowy, która określi m.in. jego zakres oraz zadania i obowiązki podmiotu, któremu przetwarzanie zostaje powierzone. Nie każda zatem umowa hostingu stron internetowych może być uznana za umowę powierzenia przetwarzania danych osobowych. Z sytuacją powierzenia przetwarzania danych osobowych będziemy mieli do czynienie tylko wtedy, gdy zawarta umowa spełniać będzie wymagania określone w art. 31 ustawy. Oznacza to, że musi być ona sporządzona w formie pisemnej i wskazywać cel oraz zakres przetwarzania. Jeżeli usługa hostingu sprowadza się wyłącznie do dzierżawy miejsca na serwerze, to w zakresie przetwarzania danych powinien się znaleźć co najmniej obowiązek odpowiedniego zabezpieczenia przetwarzanych danych przed nieupoważnionymi zmianami lub zniszczeniem. Ponadto, jeżeli powierzający przetwarzanie nie wykonuje kopii zapasowej przetwarzanego zbioru danych u siebie, to obowiązek ten musi być wykonywany przez podmiot hostujący, co również powinno być zawarte w umowie.

Jeżeli podmiot udostępniający system (serwer) nie posiada wiedzy co do rodzaju danych przetwarzanych w tym systemie i nie powierzono mu danych w myśl art. 31 ustawy, to podlega on postanowieniom art. 14 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną i jego odpowiedzialność za przetwarzane dane jest ograniczona zgodnie z art. 12–15 tej ustawy.

Czy administrator serwera, na którym w ramach świadczonych usług hostingowych przetwarzane są dane osobowe, staje się automatycznie administratorem tych danych?

Z art. 31 ust. 1 ustawy wynika, że administrator danych może powierzyć wykonywanie czynności obejmujących przetwarzanie danych, w tym przy użyciu systemu informatycznego, innemu podmiotowi. Może to mieć miejsce na podstawie zawartej na piśmie umowy. Podmiot, któremu powierzono przetwarzanie danych osobowych nie staje się ich administratorem, jest jednak obowiązany, przed rozpoczęciem przetwarzania, podjąć środki zabezpieczające, o których mowa w art. 36––39 ustawy, oraz spełnić wymagania, określone w rozporządzeniu do ustawy. W zakresie przestrzegania wskazanych powyżej przepisów podmiot ten ponosi taką samą odpowiedzialność jak administrator danych. Nie zwalnia to oczywiście tego ostatniego z obowiązku sprawowania nadzoru nad przestrzeganiem przepisów ustawy przez podmiot, któremu powierzył przetwarzanie danych. Art. 31 ust. 4 ustawy mówi wyraźnie, że *odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.*

Z przywołanych przepisów wynika, że zarówno podmiot powierzający przetwarzanie danych (administrator danych), jak i podmiot, któremu dane zostały powierzone, zobligowane są do przestrzegania przepisów dotyczących ochrony danych osobowych. Do administratora danych należy jednak wybór takiego rozwiązania informatycznego (systemu informatycznego), które spełnia wymogi zawarte w ustawie i aktach wykonawczych do niej. Wiąże się to z wyborem takiego dostawcy usług internetowych, który oferuje system informatyczny spełniający wymogi ustawy. Należy również zaznaczyć, że administrator danych zawierający umowę powierzenia przetwarzania danych osobowych z dostawcą usług internetowych ma wpływ na treść takiej umowy i jego obowiązkiem jest ujęcie w niej wszystkich aspektów dotyczących ochrony przetwarzanych danych. W umowie takiej podmiot, któremu zleca się przetwarzanie danych osobowych, powinien być poinformowany przede wszystkim o fakcie, że na jego serwerach będą przetwarzane dane osobowe i w związku z tym przyjmuje on na siebie odpowiedzialność wynikającą ze wskazanych powyżej przepisów.

Może jednak zaistnieć sytuacja, w której podmiot udostępniający system (serwer) nie posiada wiedzy co do rodzaju danych przetwarzanych w tym systemie (np. w przypadku konta shell'owego). Wówczas udostępniający zasoby systemu informatycznego podlega postanowieniom art. 14 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną i jego odpowiedzialność za przetwarzane dane jest ograniczona zgodnie z art. 12–15 tej ustawy.

Reasumując, należy stwierdzić, iż rozumowanie, jakoby administrator serwera, na którym świadczone są usługi hostingu automatycznie stawał się administratorem danych osobowych, jest nieprawidłowe. Gdy mamy do czynienia z powierzeniem przetwarzania danych, w rozumieniu art. 31 ustawy, co oznacza, że podmiot udostępniający infrastrukturę informatyczną posiada wiedzę co do charakteru przetwarzanych danych, wówczas podlega jej przepisom w zakresie art. 36–39, pomimo iż nie jest administratorem danych osobowych. Natomiast jeżeli podmiot udostępniający system nie posiada wiedzy co do charakteru przetwarzanych danych, to podlega przepisom art. 12–15 ustawy o świadczeniu usług drogą elektroniczną.

Jaka jest rola i odpowiedzialność hostingodawcy w sytuacji, kiedy w ramach jego usług hostingobiorca przetwarza we własnym celu zbiór danych osobowych? Czy pojecie systemu informatycznego, o którym mowa w rozporządzeniu, i wymagania, jakie powinien on spełniać, odnoszą się wówczas tylko do tej części systemu, którą wykorzystuje hostingobiorca?

Zgodnie z art. 7 pkt 2a ustawy pod pojęciem system informatyczny należy rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Należy zatem uznać, że dane osobowe, przetwarzane są zarówno w systemie informatycznym hostingobiorcy, jak i systemie informatycznym hostingodawcy. Proces teletransmisji danych zachodzący pomiędzy tymi systemami realizowany jest z wykorzystaniem teleinformatycznej infrastruktury tworzącej publiczną sieć Internet. Przez system informatyczny hostingodawcy należy rozumieć wszelkie urządzenia oraz programy umożliwiające dokonanie zapisu, odczytu, kasowania, przechowywania danych osobowych hostingobiorcy. Do systemu tego należą również urządzenia i programy zabezpieczające dane przed skutkami awarii zasilania oraz działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do danych. Zgodnie z przyjętą definicją do systemu informatycznego zalicza się również procedury zarządzania procesem przetwarzania danych (procedury nadawania uprawnień do przetwarzania danych, procedury wykonywania kopii zapasowych itp.).

Ze względu na fakt, iż pomiędzy systemami informatycznymi hostingodawcy i hostingobiorcy zachodzi teletransmisja danych z wykorzystaniem infrastruktury sieci teleinformatycznej stanowiącej element sieci publicznej Internet, teletransmisja ta – jako jeden z elementów procesu przetwarzania danych – powinna zapewniać im integralność, niezaprzeczalność oraz poufność. Zapewnienie takiej teletransmisji wymaga zastosowania odpowiedniego mechanizmu szyfrowania danych, np. bezpiecznego protokołu SSL. Ponadto obydwa współpracujące ze sobą systemy powinny być odpowiednio zabezpieczone przed zagrożeniami pochodzącymi z sieci publicznej – m.in. poprzez zastosowanie specjalistycznych urządzeń typu firewall, urządzeń służących wykrywaniu prób nieuprawnionego dostępu, programów antywirusowych, jak również opracowanie i wdrożenie odpowiednich procedur zarządzania.

Analizując z informatycznego punktu widzenia problematykę hostingu, należy przyjąć że system informatyczny służący do przetwarzania danych będzie się składał z dwóch części, z których jedna będzie po stronie hostingodawcy, a druga po stronie hostingobiorcy. Szczegółowa specyfikacja poszczególnych części takiego systemu jest indywidualna dla każdego przypadku. Indywidualny jest również podział zadań w zakresie zapewnienia dla danego systemu zgodności z przepisami prawa, w tym problem zapewnienia bezpieczeństwa przetwarzania danych i wzajemnej współpracy obydwu stron.

Zatem należy uznać, że zarówno hostingodawca, jak i hostingobiorca powinni dostosować swoje systemy informatyczne do warunków wymaganych w rozporządzeniu. W odniesieniu do systemu informatycznego hostingodawcy warunki, o których mowa w rozporządzeniu, musi spełniać w szczególności ta część systemu, która wykorzystywana jest przez hostingobiorcę, który przetwarza dane osobowe. Jeżeli chodzi o wzajemne relacje pomiędzy nimi, to należy zaznaczyć, że warunki odnoszące się do systemu hostingodawcy oraz środki techniczne i organizacyjne, jakie powinien on zastosować w związku z przetwarzaniem przez hostingobiorcę danych osobowych powinny być zidentyfikowane i jednoznacznie określone w umowie pomiędzy tymi podmiotami. Stroną decydującą o tym, czy z usług danego hostingodawcy można skorzystać, czy jego system spełnia warunki, jakim powinny odpowiadać systemy używane do przetwarzania danych osobowych jest administrator danych osobowych, który z usług takich zamierza korzystać.

Serwer bazy danych sam w sobie jest systemem informatycznym. Załóżmy, że przechowuję w nim dane osobowe, np. listę z adresami osób. Producenci takich systemów nie dostarczają wbudowanych mechanizmów do ewidencjonowania operacji na rekordach (zapisach) w poszczególnych tabelach takich, jak data wprowadzenia danych i identyfikator użytkownika, który dane wprowadził. Można zatem wnioskować, że system taki nie spełnia wymogów prawa z zakresu danych osobowych. Jak zatem traktować zbiór danych osobowych zawarty w bazie danych, np. tabelę z listą adresów osób fizycznych? Jak traktować sam serwer bazy danych – aplikację, która de facto staje się systemem informatycznym?

Ustawa nie precyzuje, jakie technologie informatyczne powinny być używane podczas przetwarzania danych osobowych. Obliguje jednak ich administratora do użytkowania systemów informatycznych zgodnych z jej wymogami. Dlatego też decyzja o wykorzystaniu konkretnego systemu informatycznego do przetwarzania danych osobowych powinna być determinowana zgodnością tego systemu z obowiązującymi przepisami (ustawą i rozporządzeniem). Odnosząc się jednak do przedstawionej w pytaniu sytuacji, należy zaznaczyć, że o tym, jakie pola informacyjne wystąpią w tworzonej bazie danych zawsze decyduje użytkownik. W każdej bazie danych, w której jest możliwe utworzenie pola dla imienia i nazwiska osoby, jest również możliwe utworzenie pola dla innych wymaganych informacji – takich jak np. data wprowadzenia danych czy identyfikator użytkownika, który te dane wprowadził. W wielu bazach danych jest ponadto możliwość umieszczenia procedury, która dany wpis wykona automatycznie (np. czynności odnotowania daty utworzenia nowego wpisu, jak i nazwy użytkownika wprowadzającego ten wpis). Natomiast, jeżeli któraś z wymaganych funkcjonalności w samej bazie danych nie występuje, to bazy takiej nie można wykorzystać jako samodzielnego systemu do przetwarzania danych osobowych. Nie oznacza to jednak, że nie można jej użyć jako składnika systemu informatycznego, który w połączeniu z określonym oprogramowaniem spełni wszystkie wymagane przepisami prawa funkcjonalności.

Czy system informatyczny służący do adresowania kopert, w których wysyłane są informacje o bieżącej działalności naszej instytucji (wystawy, wykłady itp.) można uznać za system „służący do przetwarzania danych osobowych i ograniczony wyłącznie do edycji tekstu w celu udostępnienia go na piśmie", o którym mowa w § 7 rozporządzenia? Na dane osobowe przetwarzane w tym systemie składają się takie pola, jak imię i nazwisko, stanowisko, nazwa instytucji, adres i kod pocztowy. Dane te są drukowane na kopertach, które następnie wysyła się za pomocą Poczty Polskiej lub rozwozi na adresy odpowiednich instytucji. Czy jest to jedyny sposób wykorzystywania tych danych?

Zgodnie z treścią § 7 rozporządzenia spełnienie wymogów określonych w tym paragrafie nie jest wymagane dla zbiorów danych osobowych służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie.

Wskazane w pytaniu cechy systemu informatycznego służącego do „przetwarzania danych osobowych w celu adresowania kopert" nie w pełni określają właściwości tego systemu. W ww. opisie nie wskazano, czy przetwarzane w tym systemie dane osobowe są niezwłocznie usuwane z tego systemu po ich wykorzystaniu (tj. po wykonaniu nadruku danych adresowych na kopertach) czy też po wydrukowaniu są w dalszym ciągu przechowywane w tym systemie.

Gdyby dane osobowe przetwarzane w ww. systemie były niezwłocznie usuwane po sporządzeniu wydruku (po osiągnięciu celu dla którego zostały wprowadzone), to należy uznać, że zbiór ten służy wyłącznie do edycji tekstu w celu udostępnienia go na piśmie. Gdyby ww. warunek nie był spełniony, to należy wówczas uznać, że zbiór, o którym mowa, służy wyłącznie do edycji tekstu w celu udostępnienia go na piśmie i powinien spełniać wszystkie wymogi określone w § 7 ust. 1 rozporządzenia.