Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa.

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

Uwagi ogólne.

Zgodnie z § 3 i § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024), zwanego dalej rozporządzeniem, administrator danych obowiązany jest do opracowania w formie pisemnej i wdrożenia polityki bezpieczeństwa. Pojęcie „polityka bezpieczeństwa", użyte w rozporządzeniu należy rozumieć, jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej (tutaj danych osobowych) wewnątrz określonej organizacji [1]. Należy zaznaczyć, że zgodnie z art. 36 ust. 2 oraz art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2015. poz. 2135, ze zm.), zwanej dalej ustawą, polityka bezpieczeństwa, o której mowa w rozporządzeniu powinna odnosić się całościowo do problemu zabezpieczenia danych osobowych u administratora danych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie jak i danych przetwarzanych w systemach informatycznych. W przypadku, gdy został powołany administrator bezpieczeństwa informacji, zgodnie z art. 36a.ust. 1 pkt 2 lit. b ustawy o ochronie danych osobowych, do jego zdań należy między innymi nadzorowanie opracowania i aktualizowanie przedmiotowej polityki bezpieczeństwa oraz przestrzeganie zasad w niej określonych.

Celem polityki bezpieczeństwa, jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych, o których mowa w § 36 ustawy. Polska Norma PN-ISO/IEC 27002:2013 [3] określająca praktyczne zasady zabezpieczenia informacji w obszarze technik informatycznych, jako cel polityki bezpieczeństwa wskazuje *zapewnienie przez kierownictwo wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami".* Zaznacza się, że dokument polityki bezpieczeństwa powinien deklarować zaangażowanie kierownictwa i wyznaczać podejście instytucji do zarządzania bezpieczeństwem informacji. Jako minimum w [3] wskazuje się, aby dokument określający politykę bezpieczeństwa uwzględniał wymagania wywodzące się ze strategii biznesowej, przepisów

prawnych i zapisów umów oraz zagrożeń istniejących w danym środowisku, w którym przetwarzanie ma miejsce. Zaleca się, aby polityka bezpieczeństwa informacji zawierała co najmniej takie elementy jak:

a) *kontrola dostępu;*
b) *klasyfikacja informacji (i postępowanie z nią);*
c) *bezpieczeństwo fizyczne i środowiskowe;*
d) *obszary związane z użytkownikiem końcowym, takie jak:*
    1) *akceptowane wykorzystanie aktywów;*
    2) *polityka czystego biurka i czystego ekranu;*
    3) *przekazywanie informacji;*
    4) *urządzenia mobilne i telepraca;*
    5) *ograniczenia dotyczące instalacji i stosowania oprogramowania;*
e) *kopie zapasowe;*
f) *przekazywanie informacji;*
g) *ochrona przed szkodliwym oprogramowaniem;*
h) *zarządzanie podatnościami technicznych;*
i) *zabezpieczenia kryptograficzne;*
j) *bezpieczeństwo komunikacji;*
k) *ochrona prywatności i informacji identyfikujących osoby.*

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

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

[1] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024), zwanego dalej rozporządzeniem, wydane zostało na podstawie delegacji ustawowej art. 39a ustawy o ochronie danych osobowych i jego zakres na podstawie art. 36 ust. 2 tejże ustawy ograniczony jest do przetwarzania danych osobowych.

komputerowego i oprogramowania. Stąd też w § 4 rozporządzenia ustawodawca wskazał, że polityka bezpieczeństwa powinna zawierać w szczególności:

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

Należy jednak zwrócić uwagę, że w wielu przypadkach, oprócz wymagań wskazanych w ww. rozporządzeniu mogą obowiązywać dodatkowo wymagania wskazane w innych regulacjach dotyczących określonych kategorii danych czy też określonego sektora gospodarki czy administracji. Przykładem takich regulacji są między innymi regulacje wynikające z ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jednolity Dz. U. z 2014 r. poz. 1114.), w tym głównie wymagania wskazane w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności[2], nazywane dalej Rozporządzeniem KRI.

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

Określając obszar przetwarzania danych osobowych należy pamiętać, iż zgodnie z ustawą o ochronie danych osobowych, przetwarzaniem danych osobowych nazywamy jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. W związku z powyższym, określanie obszaru pomieszczeń, w którym przetwarzane są dane osobowe, powinno obejmować zarówno miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacja papierową szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np.

[2] Pełna nazwa: Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012 poz. 526).

macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco). Zgodnie z treścią §4 punkt 1, wskazanie miejsca przetwarzania danych osobowych powinno być określone poprzez określenie budynków, pomieszczeń lub części pomieszczeń, w których odbywa się przetwarzanie danych osobowych. Do obszaru przetwarzania danych należy zaliczyć również pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, uszkodzone komputery i inne urządzenia z nośnikami zawierającymi dane osobowe). Do obszaru przetwarzania danych osobowych administrator danych powinien zaliczyć również miejsce w sejfie bankowym, archiwum, serwerowni podmiotu, któremu powierzono przetwarzanie danych osobowych (np. w ramach usługi hostingu czy kolokacji) itp. jeśli wykorzystywane są one np. do przechowywania elektronicznych nośników informacji zawierających kopie zapasowe danych przetwarzanych w systemie informatycznym, czy też do składowania innych nośników danych, np. dokumentów źródłowych.

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

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

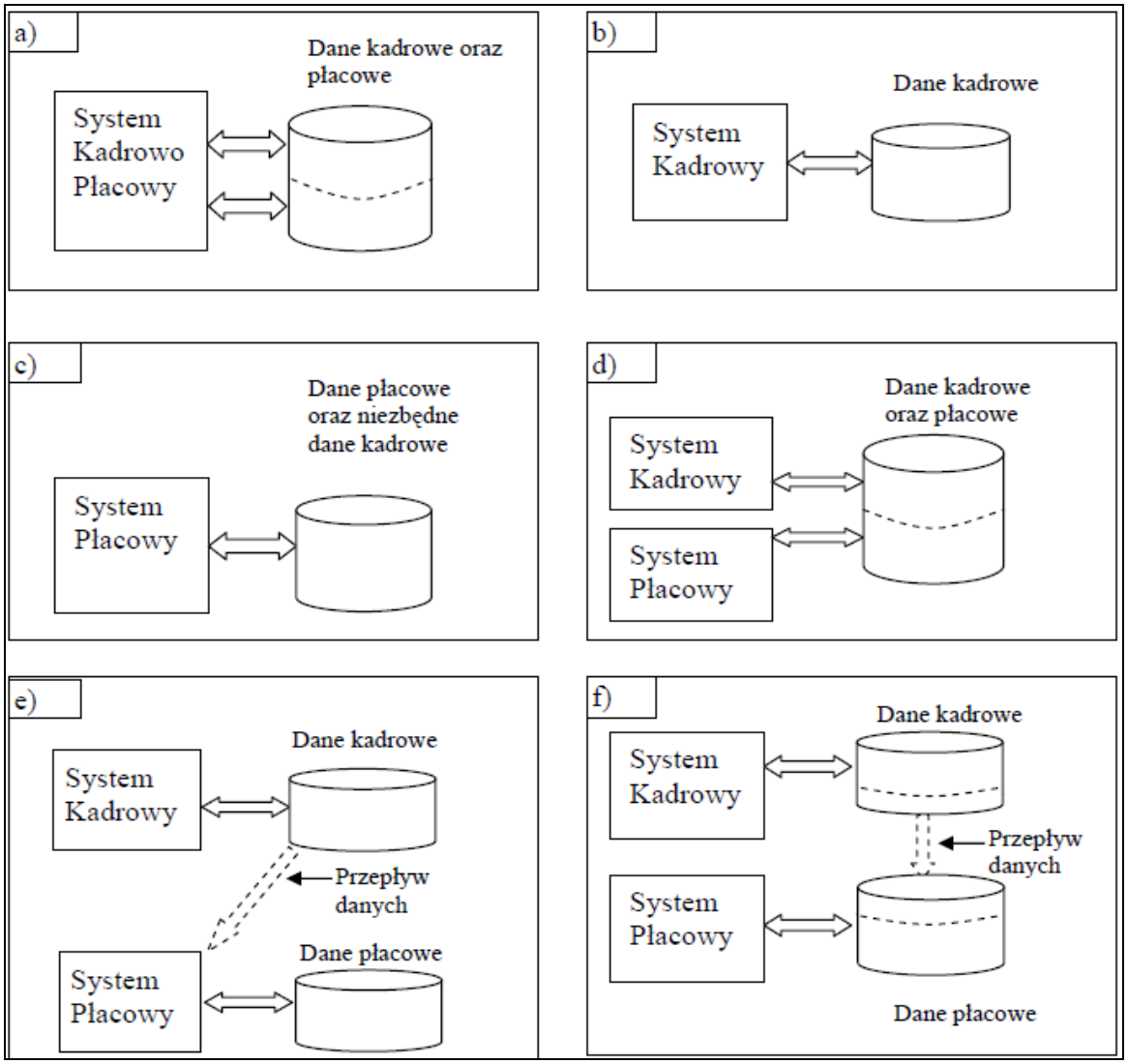
Ważnym elementem identyfikacji przetwarzanych zasobów informacyjnych jest wskazanie nazw zbiorów danych oraz systemów informatycznych (wraz ze wskazaniem programów składających się na dany system) używanych do ich przetwarzania. Stąd też oprócz wskazania obszaru przetwarzania danych, polityka bezpieczeństwa powinna identyfikować zbiory danych osobowych oraz systemy informatyczne używane do ich przetwarzania.

Istotne jest, aby w wykazie znalazły się informacje o wszystkich programach wykorzystywanych do przetwarzania danych w ramach danego zbioru, bez względu na to czy zarządzanie oraz administracja tymi programami leży w gestii administratora danych czy podmiotów zewnętrznych Na przykład wiele podmiotów realizujących zadania publiczne zobligowane jest na mocy przepisów prawa do wykorzystywania programów należących do podmiotów zewnętrznych, w szczególności placówki ochrony zdrowia zobligowane są do korzystanie z systemów udostępnianych i zarządzanych przez NFZ a szkoły do systemów udostępnianych i zarządzanych przez MEN. Pomimo braku decyzyjności w zakresie korzystania z ww. systemów administratorzy danych przetwarzają za ich pomocą dane w ramach zgłoszonych przez siebie do rejestru GIODO zbiorów i powinni pamiętać, aby uwzględnić te systemy w wykazie zbiorów danych wraz ze wskazaniem programów wykorzystywanych do ich przetwarzania.

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

Stąd też, w części polityki bezpieczeństwa identyfikującej zbiory danych osobowych oraz stosowane do ich przetwarzania programy powinny być zamieszczone nazwy zbiorów danych osobowych oraz nazwy używanych do ich przetwarzania programów komputerowych. Wykaz ten powinien zawierać informacje w zakresie precyzyjnej lokalizacji miejsca (budynek, pomieszczenie, nazwa komputera lub innego urządzenia np. macierzy dyskowej, biblioteki optycznej itp.), w których znajdują się zbiory danych osobowych przetwarzane na bieżąco oraz nazwy i lokalizacje programów (modułów programowych) używanych do ich przetwarzania. Ta części dokumentu polityki bezpieczeństwa, w przypadku, jeśli dokument ten ma spełniać jednocześnie wymagania zawarte w Rozporządzeniu KRI, tzn. jeśli administrator danych nie przygotowuje innych dokumentów związanych z zarządzaniem bezpieczeństwem danych przetwarzanych przy użyciu systemów informatycznych, powinna być dodatkowo rozszerzona o wykaz sprzętu i oprogramowania służącego do przetwarzania informacji. Zgodnie z § 20 ust 2

pkt 2 Rozporządzenia KRI, ww. wykaz sprzętu i oprogramowania, powinien obejmować zarówno rodzaj i konfigurację.



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.

Należy jednak zaznaczyć, że administrator danych nie jest zobligowany, aby ww. informacje dotyczące inwentaryzacji sprzętu i oprogramowania zawarte były w dokumencie polityki bezpieczeństwa. W przypadku dużych jednostek organizacyjnych do inwentaryzacji sprzętu i oprogramowania używane są często specjalne systemy informatyczne zarządzające taką ewidencją[3]. Systemy takie są w stanie na bieżąco aktualizować takie wykazy i na żądanie wygenerować odpowiednie raporty zawierające informacje o zainstalowanym sprzęcie informatycznym i oprogramowaniu. W polityce bezpieczeństwa lub innym dokumencie informacje takie mogą być wówczas zamieszczone np. w formie odpowiedniego załącznika

[3] Artur Pęczak, Inwentaryzacja sprzętu i oprogramowania w urzędzie za pomocą narzędzi open source, IT w administracji, Prescom Sp. Z o.o. Wrocław 2015.

przedstawiającego przedmiotowy wykaz sprzętu i oprogramowania będącego raportem wygenerowanym z opisanego wyżej systemu. Dodatkowo można wówczas zamieścić tam informacje, że aktualne zestawienie sprzętu i oprogramowania dostępne jest w systemie informatycznym i wskazać jego nazwę.

Przy tworzeniu dokumentu *Polityki bezpieczeństwa* należy zwrócić uwagę, że bardzo często popełnianym aktualnie[4] błędem jest utożsamianie wykazu zbiorów danych, o których mowa w § 4 pkt. 2 rozporządzenia z rejestrem zbiorów danych osobowych, o którym mowa w art. 36a ust 2, pkt 2 ustawy. Utożsamianie takie jest błędne, gdyż wykaz zbiorów, o którym mowa w § 4 pkt 2 rozporządzenia powinien zawierać wszystkie zbiory danych przetwarzane przez administratora danych bez żadnych wyjątków, natomiast w rejestrze zbiorów prowadzonym przez ABI powinny się znaleźć zbiory z wyłączeniem zbiorów zwolnionych z obowiązku rejestracji, o których mowa w art. 43 ust 1 ustawy. Wynika to z odmienności celów prowadzenia wyżej wymienionych rejestrów (wykazów).

Dla wykazu zbiorów danych osobowych, o których mowa w § 4 pkt 2 rozporządzenia, który stanowi obligatoryjną część polityki bezpieczeństwa, celem jest zwrócenie uwagi administratora danych a także ABI, jeśli został powołany, na właściwe zabezpieczenie procesu przetwarzania danych w poszczególnych zbiorach, jak również procesów przekazywania danych pomiędzy poszczególnymi zbiorami. Wskazanie tego celu wynika z faktu, że w celu właściwej ochrony danych, ochrona należy objąć wszystkie zbiory, w których dane są przetwarzane oraz wszystkie kanały komunikacyjne poprzez które dane są wprowadzane lub udostępniane. Nie można mówić o właściwej ochronie danych, jeśli nie zidentyfikujemy i nie opiszemy wszystkich zasobów, w których te dane się znajdują i wszystkich kanałów, którymi są przesyłane. Warto zwrócić ponadto uwagę na fakt, że w rejestrze, o którym mowa w § 4 pkt 2 rozporządzenia powinny znaleźć się wszystkie zbiory danych osobowych, jak również ich części lub podzbiory, jeśli ze względów technicznych lub funkcjonalnych zostały one podzielony, o czym mowa w art. 7 pkt 1 u.o.d.o. W konsekwencji wykaz, o którym mowa w § 4 pkt 2 ww. rozporządzenia będzie w każdym przypadku wykazem bardziej licznym niż rejestr prowadzony przez ABI, czy wykaz zbiorów zgłoszony przez administratora do GIODO, gdyż zawierał on będzie również zbiory danych zwolnione z obowiązku rejestracji, o którym mowa w (art 43 ust. 1 u.o.d.o.).

[4] Opisany błąd pojawia się dokumentach polityki bezpieczeństwa opracowanych lub aktualizowanych po 1 styczna 2015 r. u administratorów danych, którzy powołali i zarejestrowali u GIODO administratorów bezpieczeństwa informacji i w związku z tym wyznaczeni przez nich ABI zobowiązani zostali do prowadzenie lokalnego rejestru zbiorów danych osobowych.

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

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

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

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

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

W wyniku takiego powiązania wiadomym się staje jakie towary, ile i kiedy zakupił dany klient pomimo, że ani w tablicy identyfikującej tego klienta nie ma tych informacji, ani w zamówieniu nie są wskazane bezpośredni dane o tym kliencie. W rezultacie, z pokazanych w tablicy 1 relacji 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].*

Zakres danych przetwarzanych o kliencie oznaczony wyżej jako *„Zakres 1",* jak łatwo zauważyć, powstał na skutek relacji, jaka istnieje pomiędzy obiektami *„dane adresowe klienta"* i *namówienia klienta".* Relacja ta spowodowała, że zakres danych, zawarty w obiekcie *„dane adresowe klienta",* powiększony został o dane zawarte w obiektach *namówienia klienta".* Warto tutaj zauważyć, że w obiekcie oznaczonym *zamówienia klienta",* zamawiany towar wskazany został bezpośrednio poprzez określenie jego nazwy, a nie relacji z obiektem, w którym opisane są wszystkie dane na jego temat. Zapis taki spowodował, że dane o sprzedawanych towarach zapisane w obiektach oznaczonych *„sprzedawane towary",* pomimo, że fizycznie zapisane są w tym samym zbiorze danych, nie poszerzają zakresu danych o kliencie oznaczony jako *„Zakres1".*

Identyfikator klienta	Imię	Nazwisko	Kod pocztowy	Miejscowość	Ulica	Nr domu/ mieszkania

⇧

Identyfikator zamówienia	**Identyfikator klienta**	Nazwa towaru	Ilość towaru	Wartość zamówienia	Data zamówienia	Data odbioru

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

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

Skróty i oznaczenia poszczególnych kategorii danych oraz wprowadzane ze względów technicznych indeksy i klucze, w celu podwyższenia efektywności przetwarzania, sprawiają często, że techniczny opis struktury zbioru danych, a zwłaszcza postać, w jakiej ta struktura jest zapisana w systemie informatycznym, nie zawsze są wystarczająco przejrzyste. Stąd też, stosując się do § 4 pkt 3 rozporządzenia, należy w polityce bezpieczeństwa wskazać poszczególne grupy informacji oraz istniejące między nimi relacje identyfikując w ten sposób pełny zakres danych osobowych, jakie przetwarzane są w określonym zbiorze. Opisując struktury zbiorów danych nie jest konieczne przedstawianie pełnej dokumentacji struktury bazy danych z wyszczególnieniem oryginalnych nazw poszczególnych pól informacyjnych, stosowanych kluczy, czy też definicji wbudowanych obiektów funkcyjnych takich jak: procedury, funkcje, pakiety, i wyzwalacze[5] [8].

Wymóg wskazania powiązań pomiędzy polami informacyjnymi w strukturze zbiorów danych, określony w § 4 pkt 3 rozporządzenia, należy rozumieć jako wymóg wskazania wszystkich tych danych, występujących w strukturze zbioru, które poprzez występujące relacje można skojarzyć

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

z określoną osobą. Tak, np. ze struktury zbioru pokazanej w tablicy 1, wynika, iż do danych, które można skojarzyć z osobą o podanym imieniu i nazwisku, należą nie tylko dane zawarte w tym obiekcie, ale również dane zawarte w obiekcie o nazwie „zamówienia klienta". Połączenie to, zgodnie z definicją danych osobowych, powoduje poszerzenie zakresu tych danych osobowych klienta, o dane zawarte w obiekcie „zamówienia klienta".

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

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

a) *dane adresowe klienta (imię, nazwisko, kod pocztowy, miejscowość, ulica, nr domu), oraz*
b) *wszystkich składanych przez danego klienta zamówieniach (nazwa towaru, ilość towaru, wartość zamówienia, data zamówienia i data odbioru). "*

W przytoczonym przykładzie opisu tekstowego, informacja o powiązaniach pomiędzy poszczególnymi polami informacyjnymi występującymi w strukturze zbioru, została przedstawiona w tekście, poprzez wskazanie w punkcie b), że w strukturze zbioru są też informacje *o wszystkich składanych przez **danego** klienta zamówieniach* (powiązanie zamówienia z danymi klienta, które należy rozumieć jako dane adresowe wymienione w punkcie a).

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

4. Sposób przepływu danych pomiędzy systemami.

W punkcie tym należy przedstawić sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach, do przetwarzania których systemy te są wykorzystywane. Przedstawiając przepływ danych można posłużyć się np. schematami, jak na rys. 1, które wskazują, z jakimi zbiorami danych system lub moduł systemu współpracuje, czy przepływ informacji pomiędzy zbiorem danych a systemem informatycznym jest jednokierunkowy np. informacje pobierane są tylko do odczytu, czy dwukierunkowy (do odczytu i do zapisu). W sposobie przepływu danych pomiędzy poszczególnymi systemami należy zamieścić również informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (przy wykorzystaniu zewnętrznych nośników danych) lub półautomatycznie - za pomocą teletransmisji (przy wykorzystaniu specjalnych funkcji eksportu/importu danych), wykonywanych w określonych odstępach czasu. Taki

przepływ danych występuje np. często pomiędzy systemami Kadrowym i Płacowym (Rys. 1) oraz pomiędzy systemami Kadrowym, Płacowym a systemem Płatnik służącym do rozliczeń pracowników z ZUS. Dla identyfikacji procesów przetwarzania danych osobowych szczególne znaczenie ma specyfikacja przepływu danych w systemach z rozproszonymi bazami danych. W rozproszonej bazie danych, dane zlokalizowane są w różnych miejscach oddalonych od siebie terytorialnie i mogą zawierać, w zależności od lokalizacji, różne zakresy danych (tzw. niejednorodne oraz federacyjne, rozproszone bazy danych) [7]. Należy również pamiętać, aby sposób przepływu danych pomiędzy systemami nie ograniczał się wyłącznie do systemów należących do administratora danych, ale uwzględniał również przepływ do podmiotów zewnętrznych zaangażowanych w proces przetwarzania danych osobowych np. do systemów podmiotów, którym powierzono przetwarzanie danych osobowych lub podmiotów, którym dane przekazywane są na podstawie przepisów prawa. 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 przepływ danych do państwa trzeciego[6] z wynikającymi z tego tytułu konsekwencjami[7]. 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 dane są przekazywane oraz ogólnych informacji na temat sposobu przesyłania danych (Internet, poczta elektroniczna, inne rozwiązania), które mogą decydować o rodzaju narzędzi niezbędnych do zapewnienia ich bezpieczeństwa podczas teletransmisji.

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

Poprawne wykonanie zadań wymienionych w punktach 2 i 3 polityki bezpieczeństwa oraz przeprowadzona analiza przepływu danych powinna dać odpowiedź w zakresie klasyfikacji poszczególnych systemów informatycznych z punktu widzenia kategorii przetwarzanych danych

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

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

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

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

W tej części polityki bezpieczeństwa należy określić środki techniczne i organizacyjne niezbędne dla zapewnienia przetwarzanym danym poufności i integralności. Środki te powinny zapewnić jednocześnie rozliczalność wszelkich działań powodujących przetwarzanie danych osobowych. Należy pamiętać, iż środki, o których mowa wyżej, powinny być określone po uprzednim przeprowadzeniu wnikliwej analizy zagrożeń i ryzyka związanych z przetwarzaniem danych osobowych. Analiza zagrożeń i ryzyka powinna obejmować cały proces przetwarzania danych osobowych. Powinna uwzględniać podatność stosowanych systemów informatycznych na określone zagrożenia. Przy czym, podatność systemu należy tutaj rozumieć, jako słabość w systemie, która może umożliwić zaistnienie zagrożenia np. włamania do systemu i utraty poufności danych. Podatnością taką jest np. brak mechanizmu kontroli dostępu do danych, który może spowodować zagrożenie przetwarzania danych przez nieupoważnione osoby. Analizując środowisko przetwarzania danych należy ocenić ryzyko zaistnienia określonych zagrożeń. Ryzyko to można określić, jako prawdopodobieństwo wykorzystania określonej podatności systemu na istniejące w danym środowisku zagrożenia. Ważnym jest, aby zastosowane środki techniczne i organizacyjne niezbędne do zapewnienia poufności i integralności przetwarzanych danych były adekwatne do zagrożeń wynikających ze sposobu, jak również kategorii przetwarzanych danych osobowych. Środki te powinny zapewniać rozliczalność wszelkich działań (osób i systemów) podejmowanych w celu przetwarzania danych osobowych. Powinny one spełniać wymogi określone w art. 36 do 39 ustawy oraz być adekwatne do wymaganych poziomów bezpieczeństwa, o których mowa w § 6 rozporządzenia. W odniesieniu do rozliczalności działań podejmowanych przy przetwarzaniu danych osobowych

zastosowane środki powinny w szczególności wspomagać kontrolę administratora nad tym, jakie dane osobowe i przez kogo zostały do zbioru wprowadzone (art. 38 ustawy).

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

W odniesieniu do podmiotów, które zobligowane są prawnie spełniać wymagania zawarte w ustawie o informatyzacji podmiotów realizujących zadania publiczne, w tym spełniać warunki dotyczące zarządzania bezpieczeństwem wskazane w rozporządzeni KRI, dokument polityki bezpieczeństwa w tej części powinien zawierać elementy związane z realizacja działań wymienionych w § 20 ust 2 na które składają się:

1) *zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;*
2) *utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;*
3) *przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;*
4) *podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu*

adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

5) *bezzwłoczna zmiana uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;*
6) *zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:*
   a. *zagrożenia bezpieczeństwa informacji,*
   b. *skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,*
   c. *stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;*
7) *zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:*
   a. *monitorowanie dostępu do informacji,*
   b. *czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,*
   b) *zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;*
8) *ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;*
9) *zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;*
10) *zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;*
11) *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;*
12) *zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:*
   a. *dbałości o aktualizację oprogramowania,*
   b. *minimalizowaniu ryzyka utraty informacji w wyniku awarii,*
   c. *ochronie przed błędami, utratą, nieuprawnioną modyfikacją,*
   d. *stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,*
   e. *zapewnieniu bezpieczeństwa plików systemowych,*

f. redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g. niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

b) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13) bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;

14) zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Dodatkowo w przypadku podmiotów zobowiązanych do przestrzegania przepisów w zakresie zarządzania bezpieczeństwem określonych w rozporządzeniu KRI, opracowana dokumentacja przetwarzania danych osobowych powinna obejmować zagadnienia związane z dokumentowaniem operacji wykonywanych na danych przetwarzanych w tych systemach oraz operacji wykonywanych na konfiguracji systemów informatycznych (§21 ust 1,2 i 3 rozporządzenia KRI). Obligatoryjnie wymagane jest, aby system odnotowywał działania użytkowników lub obiektów systemowych polegające na dostępie do:

1) *systemu z uprawnieniami administracyjnymi;*
2) *konfiguracji systemu, w tym konfiguracji zabezpieczeń;*
3) *przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.*

Należy przy tym pamiętać, że dobre praktyki zarządzania bezpieczeństwem danych wymagają w powyższym zakresie, aby dostępu do odnotowywanych operacji (plików zawierających te dane), w zakresie uprawnień do usuwania danych lub ich modyfikacji nie posiadały osoby, których działania są w tych plikach odnotowywane.

Szarzej pojęcia i modele, o których mowa wyżej, jak również zagadnienia w zakresie zarządzania i planowania bezpieczeństwa systemów informatycznych, opisane zostały m.in. w Polskich Normach [2,3, 4, 5].

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

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

Literatura:

1. PNT-02000: Zabezpieczenia w systemach informatycznych - Terminologia, PKN,1998
2. PNT-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999
3. PN-ISO/IEC 27002:2013 Technika Informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zabezpieczania informacji, PKN, 2014
4. PN-ISO/IEC 27005:2011 Technika Informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji.
5. PN-ISO/IEC 27005:2011 Technika Informatyczna. Techniki bezpieczeństwa. Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.
6. Tomasz Pełech, Gazeta IT nr 6(25) 20 czerwiec 2004
7. Andrzej Białas, Eugeniusz Januła i inni; (red. Andrzej Białas) Podstawy bezpieczeństwa systemów teleinformatycznych; Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2002
8. Paul Beynon-Davies, Systemy baz danych, Wydawnictwo Naukowo-Techniczne, Warszawa 1998.

Opracował:
Andrzej Kaczmarek