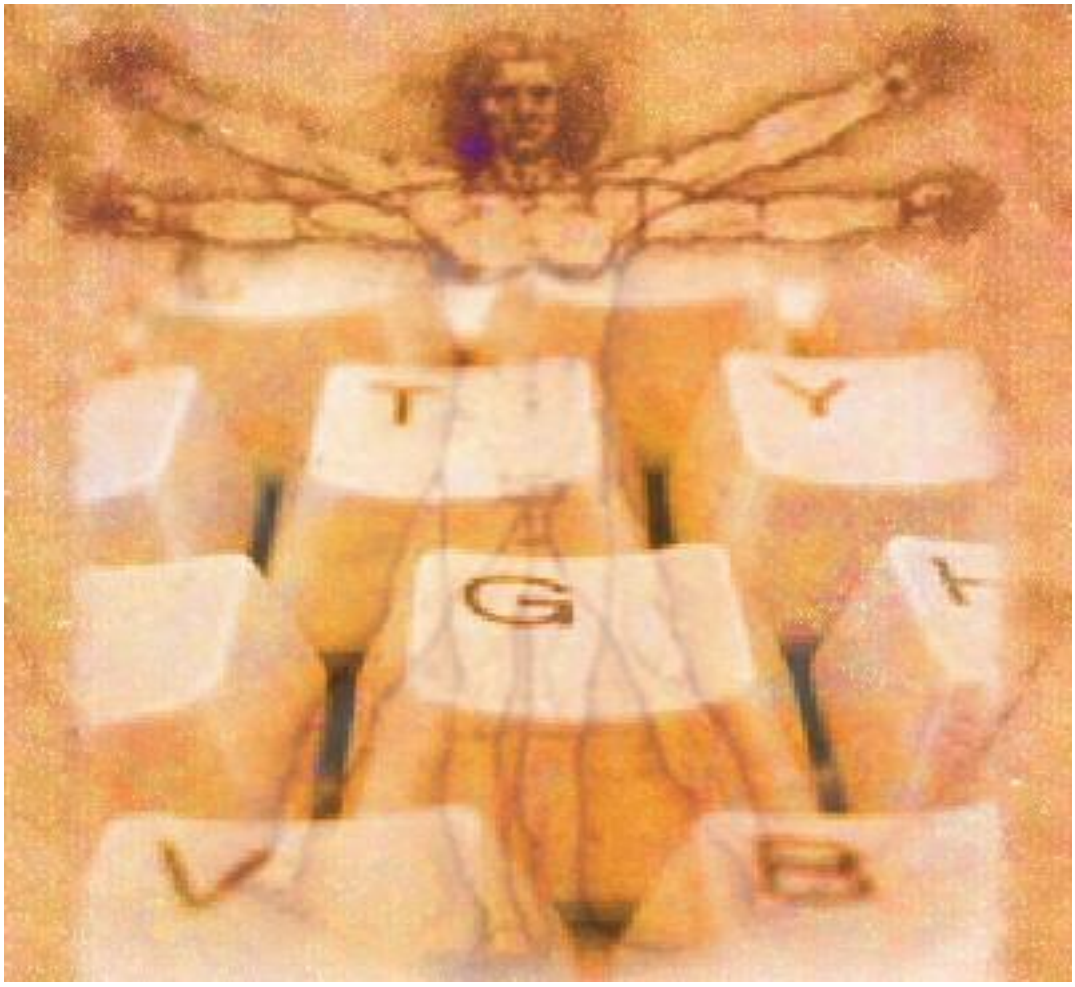


Ochrona danych osobowych w podmiotach oświatowych

Aspekty prawne i organizacyjne stosowania ustawy o ochronie danych osobowych

Krzysztof Sługocki

publikacja ta jest przeznaczona tylko do wspomagania realizacji szkoleń

wersja 1.04

Dzierżoniów, 18 listopad 2009

miejsce na Twoje notatki

Spis treści

W przygotowaniu tej publikacji wykorzystano treści dostępne na stronach internetowych Głównego Inspektora Danych Osobowych oraz systemu ISIP Kancelarii Sejmu RP.

Istotne pytania

Ważne zdania, myśli, idee

Tekst wprowadzający

Szkoła, poza wypełnianiem swoich dydaktyczno-wychowawczych obowiązków, powinna jednocześnie czuwać nad zapewnieniem ochrony prywatności dzieci.

Zgoda dyrektora szkoły, czy też poszczególnych nauczycieli lub wychowawców na przetwarzanie danych osobowych dzieci lub ich rodziców nie jest wystarczająca, by można było mówić o legalnym wykorzystywaniu tych danych. Aby można było mówić o działaniu legalnym konieczne byłoby uzyskanie zgody rodziców, czy opiekunów prawnych dzieci. Należy podkreślić, że zgoda na przetwarzanie danych osobowych wyrażona przez osoby małoletnie pozostaje bezskutecznym oświadczeniem woli do czasu jej potwierdzenia przez rodziców, czy też opiekunów prawnych małoletnich. Zgoda taka (osoby małoletniej, bez potwierdzenia) jest pozbawiona mocy prawnej w świetle obowiązujących przepisów ustawy z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy (Dz. U. Nr 9, poz. 59 z późn. zm.).

Jeśli dane osobowe uczniów nie zostają udostępnione bezpośrednio przez pracowników szkoły, niemniej jednak wskutek ich nieprawidłowego zachowania, dochodzi do pozyskania danych osobowych uczniów w zakresie, który pozwala na przykład przedstawicielowi firmy na dotarcie z ofertą marketingową do ich rodziców, to w pełni uzasadnione, w takich okolicznościach, jest poczucie zagrożenia prywatności tych osób. Dlatego też nauczyciele nie powinni, sami nie dysponując uprawnieniem do udostępnienia danych uczniów z dziennika zajęć lekcyjnych lub innych posiadanych przez szkołę dokumentów lub wyrażenia w imieniu dzieci skutecznej zgody na przetwarzanie danych, uciekać się do metod, których zastosowanie naraża na niebezpieczeństwo zarówno prywatność dzieci, jak i ich rodziców.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

Dane osobowe w systemie informacji oświatowej (wyjaśnienie GIODO)

Czy zgodne z ustawą o ochronie danych osobowych jest gromadzenie takich danych o nauczycielach jak ich imię, nazwisko czy adres zamieszkania w zbiorze danych o nauczycielach utworzonym na podstawie ustawy o systemie informacji oświatowej. Czy dane, które znajdą się w takiej bazie są bezpieczne?

Na podstawie przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.) legalność przetwarzania takich danych, jak np. imię, nazwisko, adres zamieszkania, uzależniona jest od spełnienia przez administratora danych jednej z przesłanek określonych w art. 23 ust. 1 tej ustawy. Gromadzenie danych osobowych, jako jedna z form ich przetwarzania, jest dopuszczalne m.in. wtedy, gdy jest niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (art. 23 ust. 1 pkt 2 ustawy). Tym samym ustawa o ochronie danych osobowych odsyła do przepisów szczególnych, regulujących działalność określonych podmiotów i instytucji, wskazujących w jakich przypadkach i w jakim zakresie mogą one przetwarzać, w tym udostępniać dane osobowe.

W dniu 1 stycznia 2005 r. wejdzie w życie ustawa z dnia 19 lutego 2004 r. o systemie informacji oświatowej (Dz. U. Nr 49, poz. 463).

Zakres danych o nauczycielach, wychowawcach i innych pracownikach pedagogicznych gromadzonych w związku z utworzeniem systemu informacji oświatowej określa art. 3 ust. 4 pkt 1 ustawy o systemie informacji oświatowej.

Zgodnie z tym przepisem, zbiór danych o nauczycielach, wychowawcach i innych pracownikach pedagogicznych zawiera następujące informacje: numer PESEL, płeć, rok urodzenia, formę i wymiar zatrudnienia, stopień awansu zawodowego, wykształcenie, przygotowanie pedagogiczne, a także informacje o formie kształcenia i doskonalenia, sprawowanych funkcjach i zajmowanych stanowiskach, rodzajach prowadzonych zajęć albo przyczynach nie prowadzenia zajęć, stażu pracy, wysokości wynagrodzenia, z wyszczególnieniem jego składników, wysokości dodatków, o których mowa w art. 54 ust. 3 i 5 ustawy z dnia 26 stycznia 1982 r. – Karta Nauczyciela (t.j. Dz. U. z 2003 r. Nr 118, poz. 1112 ze zm.).

Tym sposobem ustanowiona została materialno – prawna podstawa do pozyskiwania we wskazanym wyżej zakresie danych osobowych nauczycieli, wychowawców i innych pracowników pedagogicznych przez określone w przepisach powołanej ustawy podmioty prowadzące bazy danych oświatowych. Uprawnieniu do pozyskiwania tych danych przez wskazane wyżej podmioty odpowiada bezwzględny obowiązek osoby, której dane dotyczą, do ich udostępnienia.

W takim przypadku gromadzenie danych osobowych przez podmioty prowadzące bazy danych oświatowych znajduje uzasadnienie w 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych i z uwagi na to nie może być uznane za niezgodne z jej przepisami. Przewidziana w ustawie o systemie informacji oświatowej konstrukcja prawna uprawnienia określonych w niej podmiotów

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

do gromadzenia danych osobowych nauczycieli i odpowiadającego mu obowiązku do ich udostępnienia wyklucza możliwość uzależnienia udostępnienia wymienionych w jej art. 3 ust. 4 pkt 1 danych od wyrażenia zgody na ich przetwarzanie.

Odnosząc się natomiast do kwestii zabezpieczenia danych osobowych, należy zwrócić uwagę na treść art. 12 ustawy o systemie informacji oświatowej, który stanowi, iż "Podmioty prowadzące bazy danych oświatowych są obowiązane do stworzenia warunków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych, a w szczególności zabezpieczenia danych przed nieuprawnionym dostępem, nielegalnym ujawnieniem lub pozyskaniem, a także ich modyfikacją, uszkodzeniem, zniszczeniem lub utratą."

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

miejsce na Twoje notatki

Sprawozdanie Generalnego Inspektora Danych Osobowych

z działalności za rok 2004 – sprawy z zakresu oświaty

Przetwarzanie danych osobowych w sprawach związanych z oświatą uregulowane zostało w przepisach ustawy z dnia 7 września 1991 r. o systemie oświaty (tekst jednolity: Dz. U. z 2004 r. Nr 256, poz. 2572), ustawy z dnia 12 września 1990 r. o szkolnictwie wyższym (Dz. U. Nr 65, poz. 385 ze zm.), ustawy z dnia 26 stycznia 1982 r. Karta Nauczyciela (tekst jednolity: Dz. U. z 2003 r. nr 118, poz. 1112) oraz w przepisach wykonawczych do tych ustaw[1].

W omawianym obszarze wpłynęło w okresie sprawozdawczym 6 **skarg.**

Dotyczyły one w większości kwestii udostępniania danych osobom nieupoważnionym.

Przykładem takiej skargi może być sprawa udostępnienia przez pracownika szkoły językowej w Gdańsku danych osobowych słuchacza tej szkoły[2]. Dane udostępniono bez dokonania weryfikacji, czy osoba, która zwróciła się o udostępnienie jest osobą upoważnioną do ich otrzymania. Informacje te przekazano żonie słuchacza, nie mającej upoważnienia do ich pozyskania, która wykorzystała je następnie w prywatnym sporze. Dyrektorowi szkoły zasygnalizowano konieczność zastosowania takich środków bezpieczeństwa danych osobowych, które uniemożliwią tego typu zdarzenia w przyszłości. w sprawie tej skierowane zostało także zawiadomienie o popełnieniu przestępstwa z art. 51 ustawy o ochronie danych osobowych, polegającego na udostępnieniu danych osobie nieupoważnionej[3].

Zdarzył się także przypadek, iż placówka oświatowa przekazała do windykacji dane skarżącej, w sytuacji, gdy wprawdzie skarżąca zapisała się do szkoły, ale ze względów zdrowotnych nie podjęła w niej nauki i nie było podstawy do przetwarzania w ten sposób jej danych przez szkołę[4]. Osoby winne uchybień – w tym braku odnotowania, iż skarżąca informowała o niemożności podjęcia nauki oraz niesłusznego zakwalifikowania jej do grona dłużników – na skutek interwencji Generalnego Inspektora – zostały ukarane, a dane osobowe usunięto zarówno ze zbiorów szkoły, jak i podmiotu zajmującego się windykacją.

Podobna sprawa dotyczyła udostępnienia przez nauczyciela szkoły danych osobowych rodziców ucznia w trakcie prywatnego sporu pomiędzy rodzicami a nauczycielem[5]. Dyrektor szkoły – na skutek interwencji Generalnego Inspektora – wszczął postępowanie dyscyplinarne wobec nauczyciela, w związku

Istotne pytania

Ważne zdania, myśli, idee

[1] Obecnie obowiązuje również ustawa z dnia 19 lutego 2004 r. o systemie informacji oświatowej (Dz. U. Nr 49, poz. 463). Zgodnie z art. 1 tej ustawy, określa ona organizację i zasady działania systemu informacji oświatowej służącego uzyskiwaniu danych niezbędnych do prowadzenia polityki edukacyjnej państwa, podnoszenia jakości i upowszechniania edukacji oraz do usprawniania finansowania zadań oświatowych. Akt ten uzyskał jednak moc obowiązującą dopiero 1 stycznia 2005 r.

[2] GI-DS-430/291/04

[3] GI-DS-430/291/04/5411

[4] GI-DS-430/423/04

[5] GI-DS-430/829/04

ze stwierdzeniem, iż udostępnienie miało charakter samowolnego działania i nie wynikało z pełnionych obowiązków służbowych.

Nie wszystkie z rozpatrywanych skarg były uzasadnione. Przykładem może być skarga jednego z rodziców ucznia na przetwarzanie jego danych przez dyrektora szkoły i jego zastępcę, polegające na przesłaniu do skarżącego przez wicedyrektora korespondencji zawierającej jego dane osobowe[6]. Jak wykazało postępowanie, pomiędzy rodzicem a władzami szkoły istniał konflikt dotyczący przebiegu indywidualnego toku nauczania syna skarżącego, a korespondencja prowadzona przez szkołę i skarżącego miała ścisły związek z realizacją przez dyrektora i jego zastępcę zadań związanych z nauczaniem. w takich sytuacjach Generalny Inspektor informował skarżących, iż kwestionowane działania nie naruszają ustawy bowiem znajdują uzasadnienie w szczególnych przepisach prawa, a przetwarzanie jest dopuszczalne, gdyż pozostaje w ścisłym związku z wykonywaniem obowiązków wynikających z ustawy o systemie oświaty[7].

Skargi z obszaru oświaty, które wpłynęły do Generalnego Inspektora w 2004 r., nie dotyczyły tak szerokiej problematyki, jak miało to miejsce w latach ubiegłych. Jak przedstawiono powyżej, w analizowanym okresie sprawozdawczym przeważało kwestionowanie udostępniania danych osobowych skarżących podmiotom nieupoważnionym. w latach poprzednich natomiast przedmiotem skarg była głównie kwestia udostępniania przez dyrektorów szkół danych osobowych nauczycieli, zawartych w dokumentacji pracowniczej, występującym o to – w ramach uprawnień kontrolnych – gminom oraz udzielania rodzicom informacji o wynikach dzieci w nauce.

W porównaniu z rokiem ubiegłym odnotowano wyraźny wzrost liczby **pytań o interpretację przepisów** dotyczących przetwarzania danych osobowych w sektorze oświaty[8].

Pytania o interpretację przepisów dotyczące przetwarzania danych w oświacie, wpływające do Generalnego Inspektora w bieżącym okresie sprawozdawczym dotyczyły m.in.:

1) możliwości zgromadzenia przez dziennikarza danych osobowych uczniów klas maturalnych i umieszczenia ich w materiale prasowym[9],

[6] GI-DS-430/328/04

[7] GI-DEC-DS-194/04

[8] Przyczyną powyższego może być – jak wskazano w części poświęconej charakterystyce działalności Generalnego Inspektora (cześć I, lit C, pkt 3) – zmiana przepisów obowiązujących w oświacie, zwłaszcza zaś uchwalenie ustawy o systemie informacji oświatowej, która nałożyła na wskazane w niej podmioty obowiązek gromadzenia danych osobowych w tzw. bazach danych oświatowych.

[9] GI-DP-024/183/04. Udzielając odpowiedzi na pytanie skierowane w tej sprawie, Generalny Inspektor stwierdził, iż na podstawie informacji przekazanych w piśmie zastosowanie powinna znaleźć przesłanka zgody osoby, której dane dotyczą na przetwarzanie jej danych. Generalny Inspektor wskazał także, iż kwestię umieszczenia danych osobowych w materiale prasowym należy rozpatrywać w kontekście ustawy z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. Nr 5, poz. 24 ze zm.).

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

2) dopuszczalności udostępnienia przez dziekana uczelni wyższej danych osobowych studenta innemu studentowi[10],

3) legalności pozyskiwania przez szkoły bądź przez organ prowadzący szkołę danych osobowych nauczycieli, w tym informacji na temat wysokości pobieranej emerytury bądź renty, w związku z obowiązkiem dokonywania odpisu na zakładowy fundusz świadczeń socjalnych dla tych osób[11],

4) obowiązku rejestracji zbiorów danych osobowych administrowanych przez podmioty świadczące usługi edukacyjne[12],

5) zgodności z prawem wpisywania uwag o zachowaniu ucznia do dziennika lekcyjnego[13],

6) legalności prowadzenia przez Centralną Komisję do Spraw Stopni i Tytułów postępowania opiniodawczego w trybie niejawnym[14].

Podobnie jak w latach ubiegłych, Generalnego Inspektora pytano o dopuszczalność udostępniania przez szkoły wyższe rodzicom studentów, w związku z ciążącym na nich obowiązkiem alimentacyjnym, informacji o tym, czy dziec-

[10] GI-DP-024/216/04 Sprawa ta dotyczyła adresu zamieszkania studenta piszącego pracę magisterską na podobny temat, co temat pracy pytającego, w celu zacytowania wyników badań. w odpowiedzi Generalny Inspektor wskazał na art. 29 ust. 2 ustawy o ochronie danych osobowych.

[11] GI-DP-024/181/04, GI-DP-024/1714/04, GI-DP-024/2216, GI-DP-024/159/04. Generalny Inspektor zwrócił się do Ministra Edukacji Narodowej i Sportu z wnioskiem o zajęcie stanowiska w sprawie legalności pozyskiwania takich danych przez organ prowadzący szkołę (pismo z dnia 7 kwietnia 2004 r. o sygn. GI-DP-024/159/04). w odpowiedzi Minister Edukacji Narodowej i Sportu zauważył, iż kopia odcinka emerytury lub renty, która zawiera informacje na temat wysokości świadczenia otrzymywanego przez poszczególnych nauczycieli będących emerytami i rencistami nie jest konieczna do dokonania przez organ prowadzący szkołę odpisu na zakładowy fundusz świadczeń socjalnych w wysokości określonej w art. 53 ust. 2 ustawy Karta Nauczyciela. Dane dotyczące wysokości emerytur i rent nauczycieli powinny być zbierane i weryfikowane przez poszczególne szkoły, w których nauczyciele korzystają z przedmiotowego funduszu. Organ prowadzący powinien mieć natomiast możliwość dysponowania informacją o łącznej kwocie wypłaconych emerytur i rent w poszczególnych szkołach oraz listą emerytów i rencistów, umożliwiającą określenie odpowiedniej wysokości środków finansowych w budżecie na ten cel oraz weryfikację osób uprawnionych do korzystania z funduszu.

[12] GI-DP-024/214/04, GI-DP-024/316/04, GI-DP-024/426/04, GI-DP-024/657/04, GI-DP-024/736/04, GI-DP-024/764/04, GI-DP-024/1748/04.

[13] GI-DP-024/544/04 – w odpowiedzi Generalny Inspektor zwrócił uwagę na § 7 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz. U. Nr 23 poz. 225 ze zm.), który określa, jakiego rodzaju informacje powinny być zamieszczone dzienniku lekcyjnym.

[14] GI-DP-024/1537/04 Zagadnienie to powinno być rozstrzygane w oparciu o przepisy ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. Nr 65, poz. 595) oraz w oparciu o postanowienia Statutu Centralnej Komisji do Spraw Stopni i Tytułów.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

ko ich nadal studiuje[15]. Powtórzyły się także pytania dotyczące dopuszczalności upubliczniania list studentów z ich nazwiskami[16], w szczególności w połączeniu z wynikami egzaminów[17]. Ciągle aktualny pozostawał problem zgodności z prawem umieszczania na stronach internetowych szkół imion i nazwisk jej absolwentów, w celu udokumentowania historii szkoły[18]. Wpływały także pytania dotyczące udostępniania danych osobowych absolwentów w celu potwierdzenia, czy dana osoba faktycznie ukończyła określoną uczelnię[19]. w roku objętym sprawozdaniem nadal wątpliwości budziło umieszczanie na stronach internetowych szkół danych osobowych nauczycieli, w tym ich imion i nazwisk, adresu poczty elektronicznej, jak również informacji, jakich przedmiotów uczą i jaki posiadają tytuł naukowy[20]. Zdarzały się także pytania

[15] GI-DP-024/96/04, GI-DP-024/244/04, GI-DP-024/636/04, GI-DP-024/890/04, GI-DP-024/2299/04. Informacje na temat tego zagadnienia można odnaleźć w Sprawozdaniu Generalnego Inspektora z działalności za rok 2002, Część I, A. Sprawy z zakresu administracji publicznej, I. Przetwarzanie danych osobowych przez organy administracji samorządowej, I.3. Oświata, str. 22, jak i w Sprawozdaniu Generalnego Inspektora z działalności za rok 2003, Część II, A. Sprawy z zakresu administracji publicznej, 2. Oświata, str. 50.

[16] GI-DP-024/778/04. Generalny Inspektor poinformował, iż uprawnienie do umieszczania w miejscu powszechnie dostępnym listy osób przyjętych na dany kierunek studiów wynika z art. 141 ust. 4 ustawy o szkolnictwie wyższym, natomiast jako podstawę udostępnienia listy studentów wskazującej na ich przyporządkowanie do określonej grupy, np. dziekańskiej, laboratoryjnej, wskazał na przesłankę określoną w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych, gdyż działanie takie ma na celu zapewnienie sprawnej organizacji zajęć dydaktycznych na wyższej uczelni. z kolei umieszczenie w miejscu powszechnie dostępnym listy studentów zawierającej wyniki pracy semestralnej lub zawierającej dane osób, które zalegają z opłatami na rzecz uczelni będzie zgodne z przepisami ustawy o ochronie danych osobowych jedynie wtedy, gdy studenci ci wyrażą zgodę na powyższe działanie.

[17] GI-DP-024/198/04, GI-DP-024/425/04, GI-DP-024/903/04, GI-DP-024/1272/04, GI-DP-024/1040/04, GI-DP-024/1141/04, GI-DP-024/1339/04, GI-DP-024/1368/04, GI-DP-024/1783/04, GI-DP-024/1794/04, GI-DP-024/2311/04. Informacje na temat tego zagadnienia można odnaleźć również w Sprawozdaniu Generalnego Inspektora z działalności za rok 2002, Część I, A. Sprawy z zakresu administracji publicznej, I. Przetwarzanie danych osobowych przez organy administracji samorządowej, I.3. Oświata, str. 22, jak i w Sprawozdaniu Generalnego Inspektora
z działalności za rok 2003, Część II, A. Sprawy z zakresu administracji publicznej, 2. Oświata, str. 50.

[18] GI-DP-024/447/04, GI-DP-024/551/04, GI-DP-024/792/04.

[19] GI-DP-024/627/04, GI-DP-024/781/04 – w odpowiedziach Generalny Inspektor wskazywał na art. 29 ust. 2 ustawy o ochronie danych osobowych.

[20] GI-DP-024/536/04, GI-DP-024/802/04, GI-DP-024/1250/04. w sprawie tej Generalny Inspektor poinformował pytającego, iż takie informacje o pracowniku, jak jego imię i nazwisko, służbowy adres e-mail, czy też służbowy numer telefonu są ściśle związane z życiem zawodowym pracownika i z wykonywaniem przez niego obowiązków służbowych. z uwagi na to dane te mogą być wykorzystywane przez pracodawcę także bez zgody osoby, której one dotyczą. Powyższe stanowisko podzielił SN w wyroku z dnia 19 listopada 2003 r. o sygn. i PK 590/02. w wyroku tym SN wskazał, iż „Nazwisko (i imię) jest skierowanym na zewnątrz znakiem rozpoznawczym osoby fizycznej i ujawnienie go w celu jej identyfikacji nie może być zasadniczo uznane za bezprawne, o ile nie łączy się z naruszeniem innego dobra osobistego, np. czci, prywatności lub godności osobistej. Ujawnienie przez pracodawcę nazwiska

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

o to, czy informacje o wykształceniu nauczyciela podlegają ochronie[21]. Pytano także o dopuszczalność umieszczania na stronach internetowych uczelni m.in. zdjęć studentów wraz z ich imionami i nazwiskami[22].

Wątpliwości budziła również kwestia dopuszczalności żądania przez szkołę wyższą danych o stanie zdrowia studenta w postaci informacji o stwierdzeniu u niego schorzenia, o którym mowa w § 1 rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 18 września 1998 r. w sprawie rodzajów schorzeń uzasadniających obniżenie wskaźnika zatrudnienia osób niepełnosprawnych oraz sposobu jego obniżania (Dz. U. Nr 124, poz. 820 ze zm.). Po dokonaniu analizy przepisów prawa znajdujących zastosowanie w niniejszej sprawie[23], Generalny Inspektor uznał, iż szkoła wyższa jest upoważniona do żądania tego typu informacji.

Pojawiły się też pytania kwestionujące *ratio legis* ustawy o systemie informacji oświatowej, która weszła w życie dnia 1 stycznia 2005 r. Wątpliwości pytających wzbudził szeroki zakres danych podlegających obowiązkowemu udostępnieniu. Generalny Inspektor wyjaśnił, iż gromadzenie danych osobowych przez podmioty prowadzące bazy danych oświatowych znajduje uzasadnienie w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych i z uwagi na to nie może być uznane za niezgodne z jej przepisami. Wraz z wejściem w życie przepisów ustawy o systemie informacji oświatowej, ustawodawca ustanowił materialno – prawną podstawę do pozyskiwania we wskazanym w niej zakresie danych osobowych pracowników pedagogicznych przez określone w przepisach podmioty.

3.3 w 2004 r. do zaopiniowania Generalnemu Inspektorowi Ochrony Danych Osobowych skierowano 18 **projektów aktów prawnych** dotyczących omawianego sektora, do 5 z nich zostały zgłoszone uwagi. w 2003 r. przekazano 10 projektów, do których uwag nie zgłoszono. w 2002 r. wpłynęły 3 projekty aktów prawnych z tego zakresu, do 1 zgłoszono uwagi.

Jednym z zagadnień, które budziło wątpliwości Generalnego Inspektora w projektowanych przepisach, był zakres danych osobowych, jakie mają być pozyskiwane w związku ze składaniem wniosku o wydanie odpowiedniego

(imienia) pracownika bez jego zgody nie stanowi bezprawnego naruszenia dobra osobistego, jeżeli jest usprawiedliwione zadaniami i obowiązkami pracodawcy związanymi z prowadzeniem zakładu, jest niezbędne i nie narusza praw oraz wolności pracownika".

[21] GI-DP-024/640/04 – w odpowiedzi na to pismo Generalny Inspektor wskazał na odpowiednie przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 ze zm.).

[22] GI-DP-024/632/04 – Generalny Inspektor poinformował, że takie przetwarzanie danych będzie dopuszczalne za zgodą osoby, której dane te dotyczą. GI-DP-024/1237/04.

[23] w wyjaśnieniu powyższej sprawy Generalny Inspektor powołał się na przepisy ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. Nr 123, poz. 776 ze zm.) oraz aktów wykonawczych do niej. w szczególności Generalny Inspektor wskazał na przepisy art. 21 ust. 1, 2, 2b, 2f ustawy oraz na § 2a powołanego wyżej rozporządzenia. Powołał się także na przepisy rozporządzenia Ministra Gospodarki, Pracy i Polityki Społecznej z dnia 29 maja 2003 r. w sprawie określenia wzorów miesięcznych i rocznych informacji o zatrudnieniu, kształceniu lub o działalności na rzecz osób niepełnosprawnych (Dz. U. Nr 104, poz. 969 ze zm.).

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

dyplomu lub świadectwa przez zainteresowaną osobę na podstawie § 4 ust. 2 pkt 5 projektu rozporządzenia Ministra Infrastruktury w sprawie szczegółowego trybu wydawania dyplomów, świadectw, książeczek nurka i dziennika prac podwodnych oraz wzorów tych dokumentów[24]. Projektowany przepis nakładał bowiem na wnioskodawcę obowiązek dołączenia do wniosku o wydanie odpowiedniego dyplomu, kopii dowodu osobistego lub innego dokumentu potwierdzającego tożsamość. Generalny Inspektor wskazał, iż ze względu na obowiązujący stan prawny, na podstawie kopii dowodów tożsamości mogą być pozyskiwane dane w zbyt szerokim zakresie, nieadekwatnym do celu.

Zakres danych osobowych zamieszczanych w dowodzie osobistym został określony w art. 37 ustawy o ewidencji ludności i dowodach osobistych. Jednakże na podstawie art. 2 ust. 1 ustawy z dnia 20 sierpnia 1997 r. o zmianie ustawy o ewidencji ludności i dowodach osobistych oraz ustawy o działalności gospodarczej (Dz. U. Nr 113, poz. 733 ze zm.) dowody osobiste wydane przed dniem wejścia w życie niniejszej ustawy (tj. 1 stycznia 2001 r.) zachowują ważność do dnia 31 grudnia 2007 r. Wzory te, wydane przed wskazaną nowelizacją, zawierają więcej danych osobowych, niż to wynika z art. 37 ustawy o ewidencji ludności i dowodach osobistych. Są to np. informacje o kolejnych miejscach pracy, grupie krwi itd. Natomiast z treści projektowanego przepisu nie wynikało wprost, że dane te mają być ograniczone do niezbędnych (ponieważ nie określono takiego katalogu), a pozostałe powinny zostać np. zaczernione. Konieczność określenia zakresu danych wynikała ponadto z treści omawianego przepisu odsyłającego do „innych dokumentów potwierdzających tożsamość wnioskodawcy", bez wskazania konkretnych dokumentów, ani też zakresu niezbędnych danych, co mogło powodować naruszenie zasady adekwatności przetwarzania danych osobowych. Uwaga została uwzględniona.

W roku sprawozdawczym do **rejestracji** zgłaszano zbiory danych osobowych prowadzone w związku z wykonywaniem zadań związanych z funkcjonowaniem systemu oświaty. Zgłoszeń dokonywały zarówno podmioty wchodzące w skład systemu oświaty, o których mowa w art. 2 ustawy o systemie oświaty, jak i organy prowadzące szkoły i placówki oświatowe. Ogółem, w 2004 r. podmioty z omawianego sektora zgłosiły do rejestracji 46 zbiorów danych. w porównaniu z rokiem 2003 stanowi to spadek o 60% (zgłoszono wówczas 115 zbiorów danych, z czego szkoły wyższe zgłosiły 86 zbiorów dotyczących osób korzystających z zasobów bibliotecznych), a w porównaniu z rokiem 2002 – wzrost o 187% (zgłoszono 16 zbiorów danych).

Wnioskodawcy wypełniali zgłoszenia rejestracyjne bardziej poprawnie niż w latach ubiegłych, a występujące uchybienia dotyczyły głównie braku opisu środków technicznych i organizacyjnych zastosowanych w celach zabezpieczenia danych osobowych.

3.5 w okresie od 1 stycznia do 31 grudnia 2004 r. w podmiotach wykonujących zadania oświatowe przeprowadzono 1 **kontrolę** zgodności przetwarzania danych z przepisami o ich ochronie. Została ona podjęta w związku z prowadzonym postępowaniem skargowym.

[24] Projekt przekazany pismem z dnia 12 lipca 2004 r. znak: SP-2-m-020-95/04, odpowiedź GI-DP-023/192/04/434.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

Kontrola wykazała, że jednostka kontrolowana najwięcej problemów miała z zastosowaniem odpowiednich środków organizacyjnych i technicznych zapewniających ochronę danych osobowych[25]. Jak bowiem ustalono, arkusze ocen uczniów nie były odpowiednio zabezpieczone – przechowywane były na odkrytym regale w pomieszczeniu, do którego dostęp miały także osoby postronne. Ponadto stwierdzono, że polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych nie zawierają wszystkich wymaganych elementów, o których mowa w rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, np. wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Postępowanie w ww. sprawie zostało umorzone ze względu na przywrócenie przez jednostkę kontrolowaną stanu zgodnego z prawem.

[25] GI-DIS-K-411/105/04

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

zmiany:

Dz. U. 2002.153.1271

Dz. U. 2004.33.285

Dz. U. 2004.25.219

USTAWA

z dnia 29 sierpnia 1997 r.
o ochronie danych osobowych.

ROZDZIAŁ 1

Przepisy ogólne

Art. 1. 1. Każdy ma prawo do ochrony dotyczących go danych osobowych.

2. Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą.

Art. 2. 1. Ustawa określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych.

2. Ustawę stosuje się do przetwarzania danych osobowych:

1) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,

2) w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

3. W odniesieniu do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, mają zastosowanie jedynie przepisy rozdziału 5.

Art. 3. 1. Ustawę stosuje się do organów państwowych, organów samorządu terytorialnego oraz do państwowych i komunalnych jednostek organizacyjnych.

2. Ustawę stosuje się również do:

1) podmiotów niepublicznych realizujących zadania publiczne,

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

2) osób fizycznych i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych

- które mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.

Art. 3a. 1. Ustawy nie stosuje się do:

1) osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych,

2) podmiotów mających siedzibę lub miejsce zamieszkania w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium Rzeczypospolitej Polskiej wyłącznie do przekazywania danych.

2. Ustawy, z wyjątkiem przepisów art. 14-19 i art. 36 ust. 1, nie stosuje się również do prasowej działalności dziennikarskiej w rozumieniu ustawy z dnia 26 stycznia 1984 r. - Prawo prasowe (Dz. U. Nr 5, poz. 24, z późn. zm.[1)]) oraz do działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą.

Art. 4. Przepisów ustawy nie stosuje się, jeżeli umowa międzynarodowa, której stroną jest Rzeczpospolita Polska, stanowi inaczej.

Art. 5. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw.

Art. 6.[1)] 1. W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Art. 7. Ilekroć w ustawie jest mowa o:

1) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,

2) przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opra-

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

cowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

2a)[2)] systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

2b)[2)] zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

3) usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

4) administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,

5) zgodzie osoby, której dane dotyczą - rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,

6) odbiorcy danych - rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) przedstawiciela, o którym mowa w art. 31a,

d) podmiotu, o którym mowa w art. 31,

e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

7) państwie trzecim - rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego.

ROZDZIAŁ 2

Organ ochrony danych osobowych

Art. 8. 1. Organem do spraw ochrony danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych, zwany dalej „Generalnym Inspektorem".

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

2. Generalnego Inspektora powołuje i odwołuje Sejm Rzeczypospolitej Polskiej za zgodą Senatu.

3. Na stanowisko Generalnego Inspektora może być powołany ten, kto łącznie spełnia następujące warunki:

1) jest obywatelem polskim i stale zamieszkuje na terytorium Rzeczypospolitej Polskiej,

2) wyróżnia się wysokim autorytetem moralnym,

3) posiada wyższe wykształcenie prawnicze oraz odpowiednie doświadczenie zawodowe,

4) nie był karany za przestępstwo.

4. Generalny Inspektor w zakresie wykonywania swoich zadań podlega tylko ustawie.

5. Kadencja Generalnego Inspektora trwa 4 lata, licząc od dnia złożenia ślubowania. Po upływie kadencji Generalny Inspektor pełni swoje obowiązki do czasu objęcia stanowiska przez nowego Generalnego Inspektora.

6. Ta sama osoba nie może być Generalnym Inspektorem więcej niż przez dwie kadencje.

7. Kadencja Generalnego Inspektora wygasa z chwilą jego śmierci, odwołania lub utraty obywatelstwa polskiego.

8. Sejm, za zgodą Senatu, odwołuje Generalnego Inspektora, jeżeli:

1) zrzekł się stanowiska,

2) stał się trwale niezdolny do pełnienia obowiązków na skutek choroby,

3) sprzeniewierzył się złożonemu ślubowaniu,

4) został skazany prawomocnym wyrokiem sądu za popełnienie przestępstwa.

Art. 9. Przed przystąpieniem do wykonywania obowiązków Generalny Inspektor składa przed Sejmem następujące ślubowanie:

„Obejmując stanowisko Generalnego Inspektora Ochrony Danych Osobowych uroczyście ślubuję dochować wierności postanowieniom Konstytucji Rzeczypospolitej Polskiej, strzec prawa do ochrony danych osobowych, a powierzone mi obowiązki wypełniać sumiennie i bezstronnie."

Ślubowanie może być złożone z dodaniem słów „Tak mi dopomóż Bóg".

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

Art. 10. 1. Generalny Inspektor nie może zajmować innego stanowiska, z wyjątkiem stanowiska profesora szkoły wyższej, ani wykonywać innych zajęć zawodowych.

2. Generalny Inspektor nie może należeć do partii politycznej, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością jego urzędu.

Art. 11. Generalny Inspektor nie może być bez uprzedniej zgody Sejmu pociągnięty do odpowiedzialności karnej ani pozbawiony wolności. Generalny Inspektor nie może być zatrzymany lub aresztowany, z wyjątkiem ujęcia go na gorącym uczynku przestępstwa i jeżeli jego zatrzymanie jest niezbędne do zapewnienia prawidłowego toku postępowania. O zatrzymaniu niezwłocznie powiadamia się Marszałka Sejmu, który może nakazać natychmiastowe zwolnienie zatrzymanego.

Art. 12. Do zadań Generalnego Inspektora w szczególności należy:

1) kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

2) wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonania przepisów o ochronie danych osobowych,

3) prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach,

4) opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,

5) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,

6) uczestniczenie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

Art. 12a. 1. Na wniosek Generalnego Inspektora Marszałek Sejmu może powołać zastępcę Generalnego Inspektora. Odwołanie zastępcy Generalnego Inspektora następuje w tym samym trybie.

2. Generalny Inspektor określa zakres zadań swojego zastępcy.

3. Zastępca Generalnego Inspektora powinien spełniać wymogi określone w art. 8 ust. 3 pkt 1, 2 i 4 oraz posiadać wyższe wykształcenie i odpowiednie doświadczenie zawodowe.

Art. 13. 1. Generalny Inspektor wykonuje swoje zadania przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych, zwanego dalej Biurem.

2.(uchylony).

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

3. Organizację oraz zasady działania Biura określa statut nadany, w drodze rozporządzenia, przez Prezydenta Rzeczypospolitej Polskiej.

Art. 14. W celu wykonania zadań, o których mowa w art. 12 pkt 1 i 2, Generalny Inspektor, zastępca Generalnego Inspektora lub upoważnieni przez niego pracownicy Biura, zwani dalej ,,inspektorami", mają prawo:

1) wstępu, w godzinach od 6^{00} do 22^{00}, za okazaniem imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym zlokalizowany jest zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,

2) żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego,

3) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,

4) przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,

5) zlecać sporządzanie ekspertyz i opinii.

Art. 15. 1. Kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych osobowych są obowiązani umożliwić inspektorowi przeprowadzenie kontroli, a w szczególności umożliwić przeprowadzenie czynności oraz spełnić żądania, o których mowa w art. 14 pkt 1-4.

2.[5)] W toku kontroli zbiorów, o których mowa w art. 43 ust. 1 pkt 1a, inspektor przeprowadzający kontrolę ma prawo wglądu do zbioru zawierającego dane osobowe jedynie za pośrednictwem upoważnionego przedstawiciela kontrolowanej jednostki organizacyjnej.

Art. 16. 1. Z czynności kontrolnych inspektor sporządza protokół, którego jeden egzemplarz doręcza kontrolowanemu administratorowi danych.

2. Protokół podpisują inspektor i kontrolowany administrator danych, który może wnieść do protokołu umotywowane zastrzeżenia i uwagi.

3. W razie odmowy podpisania protokołu przez kontrolowanego administratora danych, inspektor czyni o tym wzmiankę w protokole, a odmawiający podpisu może, w terminie 7 dni, przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi.

Art. 17. 1. Jeżeli na podstawie wyników kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych, występuje do Generalnego Inspektora o zastosowanie środków, o których mowa w art. 18.

2. Na podstawie ustaleń kontroli inspektor może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

osobom winnym dopuszczenia do uchybień i poinformowania go, w określonym terminie, o wynikach tego postępowania i podjętych działaniach.

Art. 18. 1. W przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:

1) usunięcie uchybień,

2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,

3) zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,

4) wstrzymanie przekazywania danych osobowych za granicę,

5) zabezpieczenie danych lub przekazanie ich innym podmiotom,

6) usunięcie danych osobowych.

2. Decyzje Generalnego Inspektora, o których mowa w ust. 1, nie mogą ograniczać swobody działania podmiotów zgłaszających kandydatów lub listy kandydatów w wyborach na urząd Prezydenta Rzeczypospolitej Polskiej, do Sejmu, do Senatu i do organów samorządu terytorialnego, a także w wyborach do Parlamentu Europejskiego, pomiędzy dniem zarządzenia wyborów a dniem głosowania.

2a.[6)] Decyzje Generalnego Inspektora, o których mowa w ust. 1, w odniesieniu do zbiorów określonych w art. 43 ust. 1 pkt 1a, nie mogą nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa.

3. W przypadku gdy przepisy innych ustaw regulują odrębnie wykonywanie czynności, o których mowa w ust. 1, stosuje się przepisy tych ustaw.

Art. 19. W razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

Art. 20. Generalny Inspektor składa Sejmowi, raz w roku, sprawozdanie ze swojej działalności wraz z wnioskami wynikającymi ze stanu przestrzegania przepisów o ochronie danych osobowych.

Art. 21. 1. Strona może zwrócić się do Generalnego Inspektora z wnioskiem o ponowne rozpatrzenie sprawy.

2. Na decyzję Generalnego Inspektora w przedmiocie wniosku o ponowne rozpatrzenie sprawy stronie przysługuje skarga do sądu administracyjnego.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

Art. 22. Postępowanie w sprawach uregulowanych w niniejszej ustawie prowadzi się według przepisów Kodeksu postępowania administracyjnego, o ile przepisy ustawy nie stanowią inaczej.

Art. 22a. Minister właściwy do spraw administracji publicznej określi, w drodze rozporządzenia, wzór upoważnienia i legitymacji służbowej, o których mowa w art. 14 pkt 1, uwzględniając konieczność imiennego wskazania inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych.

ROZDZIAŁ 3

Zasady przetwarzania danych osobowych

Art. 23. 1. Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

1) osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,

2) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,

3) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,

5) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

2. Zgoda, o której mowa w ust. 1 pkt 1, może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.

3. Jeżeli przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a spełnienie warunku określonego w ust. 1 pkt 1 jest niemożliwe, można przetwarzać dane bez zgody tej osoby, do czasu, gdy uzyskanie zgody będzie możliwe.

4.[9)] Za prawnie usprawiedliwiony cel, o którym mowa w ust. 1 pkt 5, uważa się w szczególności:

1) marketing bezpośredni własnych produktów lub usług administratora danych,

2) dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Art. 24. 1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,

2) celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,

3) prawie dostępu do treści swoich danych oraz ich poprawiania,

4) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

2.[10)] Przepisu ust. 1 nie stosuje się, jeżeli:

1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,

2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

Art. 25. 1. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,

2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych,

3) źródle danych,

4) prawie dostępu do treści swoich danych oraz ich poprawiania,

5) uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8.

2. Przepisu ust. 1 nie stosuje się, jeżeli:

1) przepis innej ustawy przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą,

2) (uchylony).

3) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań określonych w ust. 1 wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania,

4) (uchylony).

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

5) dane są przetwarzane przez administratora, o którym mowa w art. 3 ust. 1 i ust. 2 pkt 1, na podstawie przepisów prawa,

6)[11)] osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

Art. 26. 1. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

1) przetwarzane zgodnie z prawem,

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

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

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

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

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

2) z zachowaniem przepisów art. 23 i 25.

Art. 26a.[12)] 1. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.

2. Przepisu ust. 1 nie stosuje się, jeżeli rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględnia wniosek osoby, której dane dotyczą.

Art. 27. 1.[13)] Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

2. Przetwarzanie danych, o których mowa w ust. 1, jest jednak dopuszczalne, jeżeli:

1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych,

2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony,

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,

4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych,

5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,

6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,

7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,

8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

9)[14)] jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone,

10)[14)] przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Art. 28. 1. (skreślony).[15)]

2. Numery porządkowe stosowane w ewidencji ludności mogą zawierać tylko oznaczenie płci, daty urodzenia, numer nadania oraz liczbę kontrolną.

3. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne.

Art. 29. 1. W przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, administrator danych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

2. Dane osobowe, z wyłączeniem danych, o których mowa w art. 27 ust. 1, mogą być także udostępnione w celach innych niż włączenie do zbioru, innym osobom i podmiotom niż wymienione w ust. 1, jeżeli w sposób wiarygodny uzasadnią potrzebę posiadania tych danych, a ich udostępnienie nie naruszy praw i wolności osób, których dane dotyczą.

3. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis innej ustawy stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

4. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Art. 30. Administrator danych odmawia udostępnienia danych osobowych ze zbioru danych podmiotom i osobom innym niż wymienione w art. 29 ust. 1, jeżeli spowodowałoby to:

1) ujawnienie wiadomości stanowiących tajemnicę państwową,

2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,

3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,

4) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

Art. 31. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

3. Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

4. W przypadkach, o których mowa w ust. 1-3, 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.

5. Do kontroli zgodności przetwarzania danych przez podmiot, o którym mowa w ust. 1, z przepisami o ochronie danych osobowych stosuje się odpowiednio przepisy art. 14-19.

Art. 31a. W przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim, administrator danych jest obowiązany wyznaczyć swojego przedstawiciela w Rzeczypospolitej Polskiej.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

ROZDZIAŁ 4

Prawa osoby, której dane dotyczą

Art. 32. 1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:

1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna - jej miejsca zamieszkania oraz imienia i nazwiska,

2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze,

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,

5a) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2,

6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane,

7) wniesienia, w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5, pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,

8) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach, wymienionych w art. 23 ust. 1 pkt 4 i 5, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych,

9)[16)] wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem art. 26a ust. 1.

2.[17)] W przypadku wniesienia żądania, o którym mowa w ust. 1 pkt 7, administrator danych zaprzestaje przetwarzania kwestionowanych danych osobowych albo bez zbędnej zwłoki przekazuje żądanie Generalnemu Inspektorowi, który wydaje stosowną decyzję.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

3. W razie wniesienia sprzeciwu, o którym mowa w ust. 1 pkt 8, dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator danych może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.[18)]

3a.[19)] W razie wniesienia żądania, o którym mowa w art. 32 ust. 1 pkt 9, administrator danych bez zbędnej zwłoki rozpatruje sprawę albo przekazuje ją wraz z uzasadnieniem swojego stanowiska Generalnemu Inspektorowi, który wydaje stosowną decyzję.

4. Jeżeli dane są przetwarzane dla celów naukowych, dydaktycznych, historycznych, statystycznych lub archiwalnych, administrator danych może odstąpić od informowania osób o przetwarzaniu ich danych w przypadkach, gdy pociągałoby to za sobą nakłady niewspółmierne z zamierzonym celem.

5. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1-5, nie częściej niż raz na 6 miesięcy.

Art. 33. 1. Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie jej danych osobowych, informacji, o których mowa w art. 32 ust. 1 pkt 1-5a, a w szczególności podać w formie zrozumiałej:

1) jakie dane osobowe zawiera zbiór,

2) w jaki sposób zebrano dane,

3) w jakim celu i zakresie dane są przetwarzane,

4) w jakim zakresie oraz komu dane zostały udostępnione.

2. Na wniosek osoby, której dane dotyczą, informacji, o których mowa w ust. 1, udziela się na piśmie.

Art. 34. W sprawach informowania i udostępniania danych osobie, której dane dotyczą, stosuje się przepisy art. 30.

Art. 35. 1. W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy.

2. W razie niedopełnienia przez administratora danych obowiązku, o którym mowa w ust. 1, osoba, której dane dotyczą, może się zwrócić do Generalnego Inspektora z wnioskiem o nakazanie dopełnienia tego obowiązku.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

3.[20)] Administrator danych jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

ROZDZIAŁ 5

Zabezpieczenie danych osobowych

Art. 36. 1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

3. Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.

Art. 37. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

Art. 38. Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Art. 39. 1. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

1) imię i nazwisko osoby upoważnionej,

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

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

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

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

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

ROZDZIAŁ 6

Rejestracja zbiorów danych osobowych

Art. 40. Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1.

Art. 41. 1. Zgłoszenie zbioru danych do rejestracji powinno zawierać:

1) wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych,

2) oznaczenie podmiotu prowadzącego zbiór i adres jego siedziby lub miejsca zamieszkania, w tym numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany, oraz podstawę prawną upoważniającą do prowadzenia zbioru, a w przypadku podmiotu, o którym mowa w art. 31a, oznaczenie tego podmiotu i adres jego siedziby lub miejsce zamieszkania,

3) cel przetwarzania danych,

3a) opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych,

4) sposób zbierania oraz udostępniania danych,

4a)[22)] informację o odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane,

5) opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36-39,

6) informację o sposobie wypełnienia warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a,

7) informację dotyczącą ewentualnego przekazywania danych do państwa trzeciego.

2. Administrator danych jest obowiązany zgłaszać Generalnemu Inspektorowi każdą zmianę informacji, o której mowa w ust. 1, w terminie 30 dni od dnia dokonania zmiany w zbiorze danych. Do zgłaszania zmian stosuje się odpowiednio przepisy o rejestracji zbiorów danych.

Art. 42. 1. Generalny Inspektor prowadzi ogólnokrajowy, jawny rejestr zbiorów danych osobowych. Rejestr powinien zawierać informacje, o których mowa w art. 41 ust. 1 pkt 1-4a i 7.

2. Każdy ma prawo przeglądać rejestr, o którym mowa w ust. 1.

3. Na żądanie administratora danych może być wydane zaświadczenie o zarejestrowaniu zgłoszonego przez niego zbioru danych, z zastrzeżeniem ust. 4.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

4. Generalny Inspektor wydaje administratorowi danych, o których mowa w art. 27 ust. 1, zaświadczenie o zarejestrowaniu zbioru danych niezwłocznie po dokonaniu rejestracji.

Art. 43. 1. Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych:

1) objętych tajemnicą państwową ze względu na obronność lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego,

1a)[24)] które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności,

2)[25)] przetwarzanych przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym,

2a)[26)] przetwarzanych przez Generalnego Inspektora Informacji Finansowej,

2b) przetwarzanych przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej,

3) dotyczących osób należących do kościoła lub innego związku wyznaniowego, o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego,

4) przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się,

5)[27)] dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,

6) tworzonych na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczących referendum ogólnokrajowego i referendum lokalnego,

7) dotyczących osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności,

8) przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,

9) powszechnie dostępnych,

10) przetwarzanych w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

11) przetwarzanych w zakresie drobnych bieżących spraw życia codziennego.

2. W odniesieniu do zbiorów, o których mowa w ust. 1 pkt 1 i 3, oraz zbiorów, o których mowa w ust. 1 pkt 1a, przetwarzanych przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne, Generalnemu Inspektorowi nie przysługują uprawnienia określone w art. 12 pkt 2, art. 14 pkt 1 i 3--5 oraz art. 15--18.

Art. 44. 1. Generalny Inspektor wydaje decyzję o odmowie rejestracji zbioru danych, jeżeli:

1) nie zostały spełnione wymogi określone w art. 41 ust. 1,

2) przetwarzanie danych naruszałoby zasady określone w art. 23-30,

3) urządzenia i systemy informatyczne służące do przetwarzania zbioru danych zgłoszonego do rejestracji nie spełniają podstawowych warunków technicznych i organizacyjnych, określonych w przepisach, o których mowa w art. 39a.

2. Odmawiając rejestracji zbioru danych, Generalny Inspektor, w drodze decyzji administracyjnej, nakazuje:

1) ograniczenie przetwarzania wszystkich albo niektórych kategorii danych wyłącznie do ich przechowywania lub

2) zastosowanie innych środków, o których mowa w art. 18 ust. 1.",

3. (uchylony).

4. Administrator danych może zgłosić ponownie zbiór danych do rejestracji po usunięciu wad, które były powodem odmowy rejestracji zbioru.

5. W razie ponownego zgłoszenia zbioru do rejestracji administrator danych może rozpocząć ich przetwarzanie po zarejestrowaniu zbioru.

Art. 44a. Wykreślenie z rejestru zbiorów danych osobowych jest dokonywane, w drodze decyzji administracyjnej, jeżeli:

1) zaprzestano przetwarzania danych w zarejestrowanym zbiorze,

2) rejestracji dokonano z naruszeniem prawa.

Art. 45.(uchylony).

Art. 46. 1. Administrator danych może, z zastrzeżeniem ust. 2, rozpocząć ich przetwarzanie w zbiorze danych po zgłoszeniu tego zbioru Generalnemu Inspektorowi, chyba że ustawa zwalnia go z tego obowiązku.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

2. Administrator danych, o których mowa w art. 27 ust. 1, może rozpocząć ich przetwarzanie w zbiorze danych po zarejestrowaniu zbioru, chyba że ustawa zwalnia go z obowiązku zgłoszenia zbioru do rejestracji.

Art. 46a. Minister właściwy do spraw administracji publicznej określi, w drodze rozporządzenia, wzór zgłoszenia, o którym mowa w art. 41 ust. 1, uwzględniając obowiązek zamieszczenia informacji niezbędnych do stwierdzenia zgodności przetwarzania danych z wymogami ustawy.

ROZDZIAŁ 7

Przekazywanie danych osobowych do państwa trzeciego

Art. 47.1. Przekazanie danych osobowych do państwa trzeciego może nastąpić, jeżeli państwo docelowe daje gwarancje ochrony danych osobowych na swoim terytorium przynajmniej takie, jakie obowiązują na terytorium Rzeczypospolitej Polskiej.

2. Przepisu ust. 1 nie stosuje się, gdy przesłanie danych osobowych wynika z obowiązku nałożonego na administratora danych przepisami prawa lub postanowieniami ratyfikowanej umowy międzynarodowej.

3. Administrator danych może jednak przekazać dane osobowe do państwa trzeciego, jeżeli:

1) osoba, której dane dotyczą, udzieliła na to zgody na piśmie,

2) przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą, lub jest podejmowane na jej życzenie,

3) przekazanie jest niezbędne do wykonania umowy zawartej w interesie osoby, której dane dotyczą, pomiędzy administratorem danych a innym podmiotem,

4) przekazanie jest niezbędne ze względu na dobro publiczne lub do wykazania zasadności roszczeń prawnych,

5) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą,

6) dane są ogólnie dostępne.

Art. 48. W przypadkach innych niż wymienione w art. 47 ust. 2 i 3 przekazanie danych osobowych do państwa trzeciego, które nie daje gwarancji ochrony danych osobowych przynajmniej takich, jakie obowiązują na terytorium Rzeczypospolitej Polskiej, może nastąpić po uzyskaniu zgody Generalnego Inspektora, pod warunkiem że administrator danych zapewni odpowiednie zabezpieczenia w zakresie ochrony prywatności oraz praw i wolności osoby, której dane dotyczą.".

ROZDZIAŁ 8

Przepisy karne

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

Art. 49. 1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 50. Kto administrując zbiorem danych przechowuje w zbiorze dane osobowe niezgodnie z celem utworzenia zbioru, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 51. 1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 52. Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 53. Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 54. Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

ROZDZIAŁ 9

Zmiany w przepisach obowiązujących, przepisy przejściowe i końcowe

Art. 55-60. (pominięte).[30)]

Art. 61. 1. Podmioty określone w art. 3, prowadzące w dniu wejścia w życie ustawy zbiory danych osobowych w systemach informatycznych, mają obowiązek złożenia wniosków o zarejestrowanie tych zbiorów w trybie określonym w art. 41, w terminie 18 miesięcy od dnia jej wejścia w życie, chyba że ustawa zwalnia ich z tego obowiązku.

2. Do czasu rejestracji zbioru danych osobowych w trybie określonym w art. 41, podmioty, o których mowa w ust. 1, mogą prowadzić te zbiory bez rejestracji.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

Art. 62. Ustawa wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia,[31)] z tym że:

1) art. 8-11, art. 13 i 45 wchodzą w życie po upływie 2 miesięcy od dnia ogłoszenia,

2) art. 55-59 wchodzą w życie po upływie 14 dni od dnia ogłoszenia.

[1)] Niniejsza ustawa dokonuje w zakresie swojej regulacji wdrożenia dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.).".

[1)] W brzmieniu ustalonym przez art. 1 pkt 1 ustawy z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych (Dz. U. Nr 100, poz. 1087), która weszła w życie z dniem 3 października 2001 r.

[2)] Dodany przez art. 1 pkt 2 ustawy, o której mowa w przypisie 1.

[2)] Dodany przez art. 1 pkt 2 ustawy, o której mowa w przypisie 1.

[3)] Ze zmianą wprowadzoną przez art. 1 pkt 3 ustawy, o której mowa w przypisie 1.

[4)] Oznaczenie ust. 1 nadane przez art. 1 pkt 4 ustawy, o której mowa w przypisie 1.

[5)] Dodany przez art. 1 pkt 4 ustawy, o której mowa w przypisie 1.

[6)] Dodany przez art. 1 pkt 5 ustawy, o której mowa w przypisie 1.

[7)] W brzmieniu ustalonym przez art. 1 pkt 6 lit. a) tiret pierwsze ustawy, o której mowa w przypisie 1.

[8)] W brzmieniu ustalonym przez art. 1 pkt 6 lit. a) tiret drugie ustawy, o której mowa w przypisie 1.

[9)] Dodany przez art. 1 pkt 6 lit. b) ustawy, o której mowa w przypisie 1.

[10)] W brzmieniu ustalonym przez art. 1 pkt 7 ustawy, o której mowa w przypisie 1.

[11)] Dodany przez art. 1 pkt 8 ustawy, o której mowa w przypisie 1.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

[11)] Dodany przez art. 1 pkt 8 ustawy, o której mowa w przypisie 1.

[12)] Dodany przez art. 1 pkt 9 ustawy, o której mowa w przypisie 1.

[13)] Ze zmianą wprowadzoną przez art. 1 pkt 10 lit. a) ustawy, o której mowa w przypisie 1.

[14)] Dodany przez art. 1 pkt 10 lit. b) ustawy, o której mowa w przypisie 1.

[14)] Dodany przez art. 1 pkt 10 lit. b) ustawy, o której mowa w przypisie 1.

[15)] Przez art. 1 pkt 11 ustawy, o której mowa w przypisie 1.

[16)] Dodany przez art. 1 pkt 12 lit. a) ustawy, o której mowa w przypisie 1.

[17)] Ze zmianą wprowadzoną przez art. 1 pkt 12 lit. b) ustawy, o której mowa w przypisie 1.

[18)] Zdanie drugie dodane przez art. 1 pkt 12 lit. c) ustawy, o której mowa w przypisie 1.

[19)] Dodany przez art. 1 pkt 12 lit. d) ustawy, o której mowa w przypisie 1.

[20)] Dodany przez art. 1 pkt 13 ustawy, o której mowa w przypisie 1.

[21)] Ze zmianą wprowadzoną przez art. 1 pkt 14 ustawy, o której mowa w przypisie 1.

[22)] Dodany przez art. 1 pkt 15 lit. a) ustawy, o której mowa w przypisie 1.

[23)] Dodany przez art. 1 pkt 15 lit. b) ustawy, o której mowa w przypisie 1.

[24)] Dodany przez art. 1 pkt 16 lit. a) ustawy, o której mowa w przypisie 1.

[25)] W brzmieniu ustalonym przez art. 29 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. Nr 50, poz. 580), która weszła w życie z dniem 22 czerwca 2001 r.

[26)] Dodany przez art. 47 ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł (Dz. U. Nr 116, poz. 1216), która weszła w życie z dniem 23 czerwca 2001 r.

[27)] W brzmieniu ustalonym przez art. 11 ustawy z dnia 11 kwietnia 2001 r. o zmianie ustawy o doradztwie podatkowym oraz niektórych innych ustaw (Dz. U. Nr 42, poz. 474), która weszła w życie z dniem 11 czerwca 2001 r., i ze zmianą wprowadzoną przez art. 71 ustawy z dnia 11 kwietnia 2001 r. o rzecznikach patentowych (Dz. U. Nr 49, poz. 509), która weszła w życie z dniem 22 sierpnia 2001 r.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

[28)] Ze zmianą wprowadzoną przez art. 47 ustawy z dnia 21 stycznia 2000 r. o zmianie niektórych ustaw związanych z funkcjonowaniem administracji publicznej (Dz. U. Nr 12, poz. 136), która weszła w życie z dniem 23 lutego 2000 r.

[29)] W brzmieniu ustalonym przez art. 192 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. Nr 74, poz. 676), która weszła w życie z dniem 29 czerwca 2002 r.

[30)] Zamieszczone w obwieszczeniu.

[31)] Ustawa została ogłoszona dnia 29 października 1997 r.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

miejsce na Twoje notatki

Dz. U. z 2004 r. Nr 100, poz. 1024

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

Na podstawie art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271 oraz z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285) zarządza się, co następuje:

§ 1.

Rozporządzenie określa:

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

§ 2.

Ilekroć w rozporządzeniu jest mowa o:

1) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";
2) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
3) haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
4) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
5) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
6) telentransmisji – rozumie się przez to przesyłanie informacji za po-

Istotne pytania

Ważne zdania, myśli, idee

średnictwem sieci telekomunikacyjnej

7) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

8) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

9) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;

10) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

11) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 3.

1. Na dokumentację, o której mowa w § 1 pkt 1, składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „instrukcją".

2. Dokumentację, o której mowa w § 1 pkt 1, prowadzi się w formie pisemnej.

3. Dokumentację, o której mowa w § 1 pkt 1, wdraża administrator danych.

§ 4.

Polityka bezpieczeństwa, o której mowa w § 3 ust. 1, zawiera w szczególności:

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

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

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

4) sposób przepływu danych pomiędzy poszczególnymi systemami;

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

§ 5.

Instrukcja, o której mowa w § 3 ust. 1, zawiera w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

5) sposób, miejsce i okres przechowywania:

a) elektronicznych nośników informacji zawierających dane osobowe,

b) kopii zapasowych, o których mowa w pkt 4,

6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia;

7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4;

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

§ 6.

1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza się poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym:
   1) podstawowy;
   2) podwyższony;
   3) wysoki.
2. Poziom co najmniej podstawowy stosuje się, 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.
3. Poziom co najmniej podwyższony stosuje się, 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.
4. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.
5. Opis środków bezpieczeństwa stosowany na poziomach, o których mowa w ust. 1, określa załącznik do rozporządzenia.

§ 7.

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwa-

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

rzania 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.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. 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.

§ 8.

System informatyczny służący do przetwarzania danych, który został dopuszczony przez właściwą służbę ochrony państwa do przetwarzania informacji niejawnych, po uzyskaniu certyfikatu wydanego na podstawie przepisów ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.) spełnia wymogi niniejszego rozporządzenia pod względem bezpieczeństwa na poziomie wysokim.

§ 9.

Administrator przetwarzanych w dniu wejścia w życie niniejszego rozporządzenia danych osobowych jest obowiązany dostosować systemy informatyczne służące do przetwarzania tych danych do wymogów określonych w § 7 oraz w załączniku do rozporządzenia w terminie 6 miesięcy od dnia wejścia w życie niniejszego rozporządzenia.

§ 10.

Rozporządzenie wchodzi w życie z dniem uzyskania przez Rzeczpospolitą Polską członkostwa w Unii Europejskiej.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (poz. 1024)

A. Środki bezpieczeństwa na poziomie podstawowym

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;

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

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.

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

B. Środki bezpieczeństwa na poziomie podwyższonym

VIII

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.

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

Instrukcja zarządzania systemem informatycznym, o której mowa w § 5 rozporządzenia, rozszerza się o sposób stosowania środków, o których mowa w pkt IX załącznika.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

XI

Administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa określone w części a załącznika, o ile zasady zawarte w części B nie stanowią inaczej.

C. Środki bezpieczeństwa na poziomie wysokim

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.

XIV

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

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa.

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

Uwagi ogólne.

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

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

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

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

   1) zgodność z prawem i wymaganiami wynikającymi z umów;

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

2) wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa;

3) zapobieganie i wykrywanie wirusów oraz innego złośliwego oprogramowania;

4) zarządzanie ciągłością działania biznesowego;

5) konsekwencje naruszenia polityki bezpieczeństwa;

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

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

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

Dokument, o którym mowa w § 4 rozporządzenia w zakresie przedmiotowym powinien koncentrować się na bezpieczeństwie przetwarzania danych osobowych, co wynika z art. 36 ustawy o ochronie danych osobowych[26]. Prawidłowe zarządzanie zasobami, w tym również zasobami informacyjnymi, zwłaszcza w aspekcie bezpieczeństwa informacji, wymaga właściwej identyfikacji tych zasobów [2] oraz określenia miejsca i sposobu ich przechowywania. Wybór zaś odpowiednich dla poszczególnych zasobów metod zarządzania ich ochroną i dystrybucją zależny jest od zastosowanych nośników informacji, rodzaju zastosowanych urządzeń, sprzętu komputerowego i oprogramowania. Stąd też w § 4 rozporządzenia ustawodawca wskazał, że polityka bezpieczeństwa powinna zawierać w szczególności:

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

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

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

9) sposób przepływu danych pomiędzy poszczególnymi systemami;

10) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.

[26] 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.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

miejsce na Twoje notatki

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

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

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

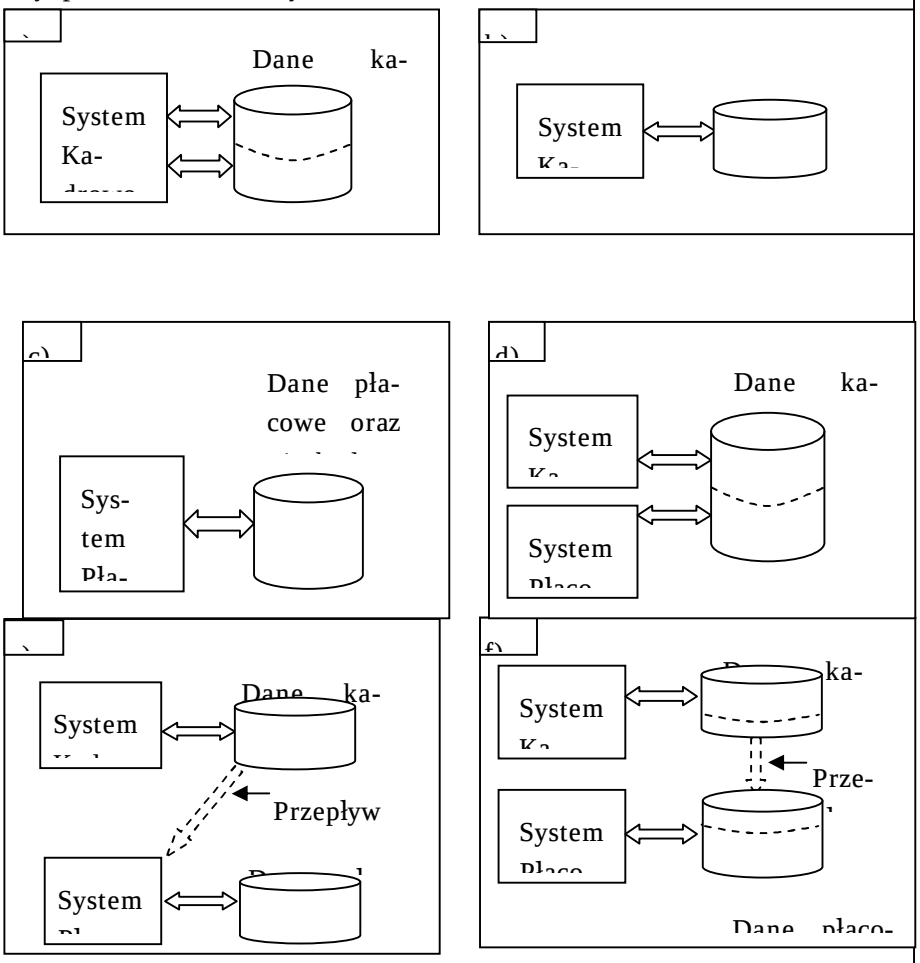
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Ważnym elementem identyfikacji przetwarzanych zasobów informacyjnych jest wskazanie nazw zbiorów danych oraz systemów informatycznych używanych do ich przetwarzania. Stąd też oprócz wskazania obszaru przetwarzania danych, polityka bezpieczeństwa powinna identyfikować zbiory danych

Istotne pytania

Ważne zdania, myśli, idee

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



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

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

Stąd też, w części polityki bezpieczeństwa identyfikującej zbiory danych osobowych oraz stosowane do ich przetwarzania programy powinny być zamieszczone nazwy zbiorów danych osobowych oraz nazwy używanych do ich przetwarzania programów komputerowych.

Wykaz ten powinien zawierać informacje w zakresie precyzyjnej lokalizacji miejsca (budynek, pomieszczenie, nazwa komputera lub innego urządzenia np. macierzy dyskowej, biblioteki optycznej itp.), w których znajdują się zbiory danych osobowych przetwarzane na bieżąco oraz nazwy i lokalizacje programów (modułów programowych) używanych do ich przetwarzania.

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

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

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

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

oraz informacje o towarach w zakresie:

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

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

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

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

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

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

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

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

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

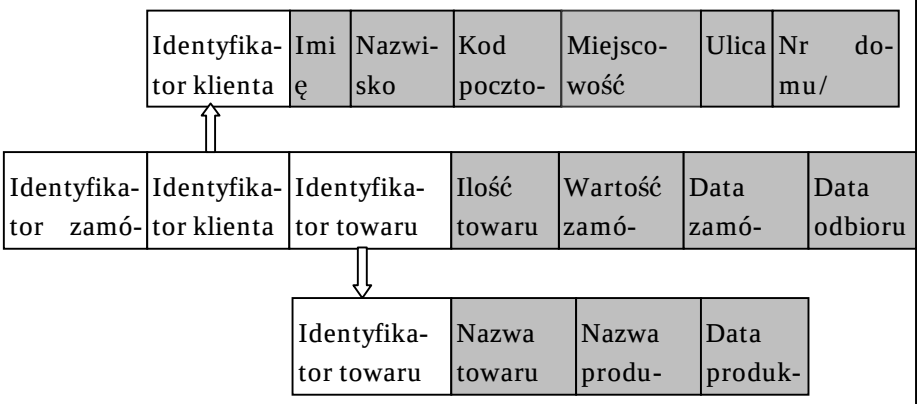
miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

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

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



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

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

Skróty i oznaczenia poszczególnych kategorii danych oraz wprowadzane ze względów technicznych indeksy i klucze, w celu podwyższenia efektywności przetwarzania, sprawiają często, że techniczny opis struktury zbioru danych, a zwłaszcza postać, w jakiej ta struktura jest zapisana w systemie informatycznym, nie zawsze są wystarczająco przejrzyste.

Stąd też, stosując się do § 4 pkt 3 rozporządzenia, należy w polityce bezpieczeństwa wskazać poszczególne grupy informacji oraz istniejące między nimi relacje identyfikując w ten sposób pełny zakres danych osobowych, jakie przetwarzane są w określonym zbiorze. Opisując struktury zbiorów danych nie jest konieczne przedstawianie pełnej dokumentacji struktury bazy danych z wyszczególnieniem oryginalnych nazw poszczególnych pól informacyjnych, stosowanych kluczy, czy też definicji wbudowanych obiektów funkcyjnych takich jak: procedury, funkcje, pakiety, i wyzwalacze[27] [4].

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

[27] 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)

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

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

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

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

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

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

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

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

4. Sposób przepływu danych pomiędzy systemami.

W punkcie tym należy przedstawić sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach, do przetwarzania których systemy te są wykorzystywane. Przedstawiając przepływ danych można posłużyć się np. schematami, jak na rys. 1, które wskazują, z jakimi zbiorami danych system lub moduł systemu współpracuje, czy przepływ informacji pomiędzy zbiorem danych a systemem informatycznym jest jednokierunkowy np. informacje pobierane są tylko do odczytu, czy dwukierunkowy (do odczytu i do zapisu). w sposobie przepływu danych pomiędzy poszczególnymi systemami należy zamieścić również informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (przy wykorzystaniu zewnętrznych nośników danych) lub półautomatycznie – za pomocą teletransmisji (przy wykorzystaniu specjalnych funkcji eksportu/importu danych), wykonywanych w określonych odstępach czasu. Taki przepływ danych występuje np. często pomiędzy systemami Kadrowym i Płacowym (Rys. 1f) oraz pomiędzy systemami Kadrowym, Płacowym a systemem Płatnik służącym do rozliczeń pracowników z ZUS. Dla identyfikacji procesów przetwarzania danych osobowych szczególne znaczenie ma specyfikacja przepływu danych w systemach z rozproszonymi bazami danych. w rozproszonej bazie danych, dane zlokalizowane są w różnych miejscach oddalonych od siebie terytorialnie i mogą zawierać, w zależności od

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

lokalizacji, różne zakresy danych (tzw. niejednorodne oraz federacyjne, rozproszone bazy danych) [5]. Dla systemów korporacyjnych o zasięgu międzynarodowym, informacja o przepływie danych pomiędzy oddziałami korporacji znajdującymi się w państwach nie należących do Europejskiego Obszaru Gospodarczego musi być traktowana jako przepływ danych do państwa trzeciego[28] z wynikającymi z tego tytułu konsekwencjami[29]. 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 z punktu widzenia uzyskiwanego wyniku porównać do opisu relacji pomiędzy poszczególnymi polami informacyjnymi w strukturach zbiorów danych, co przedstawiono w punkcie 3. w przypadku przepływu danych pomiędzy systemami informatycznymi relacje, jakie powstają pomiędzy danymi przetwarzanymi w zbiorach poszczególnych systemów, nie wynikają z ich struktury. w przypadku przepływu danych pomiędzy systemami, dane z poszczególnych zbiorów łączone są dynamicznie poprzez wykonanie określonych funkcji systemu lub odpowiednio zdefiniowanych procedur zewnętrznych.

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

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

W tej części polityki bezpieczeństwa należy określić środki techniczne i organizacyjne niezbędne dla zapewnienia przetwarzanym danym poufności i integralności. Środki te powinny zapewnić jednocześnie rozliczalność wszel-

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

[29] 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.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

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

Ryzykiem dla przetwarzania danych osobowych w systemie informatycznym podłączonym do sieci Internet jest np. możliwość przejęcia lub podglądu tych danych przez osoby nieupoważnione. Ryzyko to będzie tym większe im mniej skuteczne będą stosowane zabezpieczenia. Sygnalizacja istniejącego zagrożenia pozwala podjąć odpowiednie działania zapobiegawcze. Ważne jest często samo uświadomienie istnienia określonych zagrożeń np. wynikających z przetwarzania danych w systemie informatycznym podłączonym do sieci Internet czy też zagrożeń spowodowanych stosowaniem niesprawdzonych pod względem bezpieczeństwa technologii bezprzewodowej transmisji danych. Zidentyfikowane zagrożenia można minimalizować m.in. poprzez stosowanie systemów antywirusowych, mechanizmów szyfrowania, systemów izolacji i selekcji połączeń z siecią zewnętrzną (firewall), itp. Dla dużych systemów informatycznych (systemów połączonych z sieciami publicznymi, systemów z rozproszonymi bazami danych, itp.) wybór właściwych środków wymaga posiadania wiedzy specjalistycznej. Prawidłowe opracowanie polityki bezpieczeństwa przetwarzania danych osobowych w ww. zakresie jest procesem złożonym, wymagającym m.in. znajomości podstawowych pojęć i modeli używanych do opisywania sposobów zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele, o których mowa, jak również zagadnienia w zakresie zarządzania i planowania bezpieczeństwa systemów informatycznych, opisane zostały m.in. w Polskich Normach [2,3].

Podczas określania środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i integralności przetwarzanych danych, jak również rozliczalności podejmowanych w tym celu działań, należy kierować się m.in. klasyfikacją poziomów bezpieczeństwa wprowadzoną w § 6 rozporządzenia. Dla każdego z wymienionych tam poziomów, które powinny być

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

zidentyfikowane po wykonaniu zadań wymienionych w punktach 2, 3 i 4 polityki bezpieczeństwa, niezbędne jest zapewnienie co najmniej takich środków bezpieczeństwa, które spełniają minimalne wymagania określone w załączniku do rozporządzenia.

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

Literatura:

1. PN-I-02000: Zabezpieczenia w systemach informatycznych – Terminologia, PKN,1998
2. PN-I-13335-1: Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999
3. PN-ISO/IEC 17799 Technika Informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, 2003
4. Tomasz Pelech, Gazeta IT nr 6(25) 20 czerwiec 2004
5. Andrzej Bialas, Eugeniusz Janula i inni; (red. Andrzej Bialas) Podstawy bezpieczeństwa systemów teleinformatycznych; Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2002
6. Paul Beynon-Davies, Systemy baz danych, Wydawnictwo Naukowo-Technicznе, Warszawa 1998.
7. Lech Banachowski, Bazy Danych – Tworzenie aplikacji, Akademicka Oficyna Wydawnicza PLJ, Warszawa 1998.

Przygotował: A. Kaczmarek

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

miejsce na Twoje notatki

Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

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

Opracowana instrukcja powinna być 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, zaś 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. w przypadku, gdy administrator danych, do przetwarzania danych wykorzystuje nie jeden, lecz kilka systemów informatycznych, wówczas stosownie do podobieństwa zastosowanych rozwiązań powinien opracować jedną, ogólną instrukcję zarządzania lub opracować oddzielne instrukcje dla każdego z użytkowanych systemów. w zależności, zatem od przyjętego rozwiązania, inny będzie zakres opracowanych zagadnień w małych podmiotach, w których dane osobowe przetwarzane są przy pomocy jednego lub kilku komputerów i inny w dużych podmiotach, w których funkcjonują rozbudowane lokalne sieci komputerowe z dużą ilością serwerów i stacji roboczych przetwarzających dane przy użyciu wielu systemów informatycznych.

W instrukcji, o której mowa, powinny być wskazane systemy informatyczne, których ona dotyczy, ich lokalizacje, 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 ta powinna obejmować zagadnienia dotyczące zapewnienia 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,

Istotne pytania

Ważne zdania, myśli, idee

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 przetwarzanych danych, w odniesieniu do każdego z wymienionych wyżej punktów, w treści instrukcji powinny być wskazane odpowiednie dla stosowanych systemów informatycznych zasady postępowania. Ogólne wskazówki dotyczące zagadnień, jakie powinny być zawarte w instrukcji w odniesieniu do wyżej wymienionych punktów przedstawiono poniżej.

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 identyfikatora w systemie informatycznym, jak również zasady nadawania lub modyfikacji uprawnień użytkownika do zasobów systemu informatycznego. Powyższe zasady 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 haslami 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 procedur oraz rejestrowanie i wyrejestrowywanie użytkowników w systemie informatycznym.

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

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

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 osoby odpowiedzialne za przydział haseł. Wskazanie to może być określone funkcjonalnie lub personalnie. 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, takie jak wymogi dotyczące ich powtarzalności czy też wymogi dotyczące 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 zgodnie z pkt IV ppk 2 załącznika do rozporządzenia, hasło użytkownika powinno być zmieniane nie rzadziej niż co 30 dni i składać się co najmniej z 6 znaków, jeżeli w systemie nie są przetwarzane dane, o których mowa w art. 27 ustawy lub 8 znaków, jeżeli takie dane są przetwarzane (pkt VII załącznika). 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 przypadku zastosowania innych niż identyfikator i hasło metod weryfikacji tożsamości użytkownika, np. kart mikroprocesorowych czy też metod biometrycznych w instrukcji powinny być zawarte wytyczne w zakresie ich stosowania. Dla kart mikroprocesorowych np. należy wskazać sposób ich personalizacji, zaś dla metod biometrycznych sposób pobierania danych biometrycznych w procesie rejestrowania użytkownika w systemie oraz sposób ich przechowywania.

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 uruchamiania 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 poufności 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 przypadku braku możliwości zalogowania się użytkownika na jego konto czy też w przypadku stwierdzenia fizycznej ingerencji w przetwarzane dane lub użytkowane narzędzia programowe lub sprzętowe.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

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 kopie będą wykonywane oraz narzędzia programowe i urządzenia, które mają być do tego celu wykorzystywane. w procedurze wykonywania kopii 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 w przypadku, gdy procedury wykonywania tych kopii są złożone, może się odwoływać do procedur szczegółowych dedykowanych 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. Wymogi te nakazują, aby urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawiać zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadzać w sposób uniemożliwiający ich odczytanie.

5. **Sposób, miejsce i okres przechowywania:**

   a) **elektronicznych nośników informacji zawierających dane osobowe,**

   b) **kopii zapasowych, o których mowa w §5 pkt. 4 rozporządzenia.**

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

   Przy opracowywaniu zaleceń dotyczących sposobu i czasu przechowywania nośników informacji należy uwzględnić, iż zgodnie z wymogami pkt IV ppkt 4a załącznika do rozporządzenia, kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Należy uwzględnić wymogi określone w pkt IV ppkt 4b załącznika do rozporządzenia nakazujące, aby kopie awaryjne bezzwłocznie usuwać po ustaniu ich użyteczności.

   W przypadku przekazywania nośników informacji podmiotom zewnętrznym w celu bezpiecznego ich przechowywania, np. stosowane dość często deponowanie kopii zapasowych w skarbcach bankowych, należy określić procedury przekazywania nośników informacji tym podmiotom

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

oraz wskazać metody zabezpieczania przekazywanych nośników informacji przed dostępem osób nieuprawnionych podczas ich transportu/przekazywania.

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, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia należy określić obszary systemu informatycznego narażone na ingerencję wirusów komputerowych oraz wszelkiego rodzaju innego szkodliwe oprogramowanie. Należy wskazać możliwe źródła przedostania się szkodliwego oprogramowania do systemu oraz działania, jakie należy podejmować, aby minimalizować możliwość zainstalowania się takiego oprogramowania. Niezależnie od wskazania czynności profilaktycznych przed przedostaniem się do systemu oprogramowania szkodliwego, w instrukcji należy wskazać zastosowane narzędzia programowe, których zadaniem jest przeciwdziałanie skutkom szkodliwego działania takiego oprogramowania. Należy wskazać oprogramowanie antywirusowe, które zostało zainstalowane, określić metody i częstotliwość aktualizacji definicji wirusów oraz osoby odpowiedzialne za zarządzanie tym oprogramowaniem. Powinny być przedstawione również procedury postępowania użytkowników na okoliczność zidentyfikowania określonego typu zagrożeń. Użytkownik powinien być poinformowany o czynnościach, które powinien wykonać w przypadku, gdy oprogramowanie zabezpieczające wskazuje zaistnienie zagrożenia. w przypadku, gdy stosowane są inne niż oprogramowanie antywirusowe metody ochrony przed szkodliwym oprogramowaniem należy je wskazać i przedstawić procedury związane z ich stosowaniem. Do metod takich mogą należeć m. in. fizyczne odłączenie urządzeń umożliwiających odczyt danych z wymiennych nośników informatycznych poszczególnych stacji komputerowych (np. odłączenie stacji CD, stacji dyskietek, itp.) i wyznaczenie wydzielonego stanowiska w sieci komputerowej do wymiany danych za pomocą nośników zewnętrznych.

7. **Sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4.**

   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 udostępnieniach danych odbiorcom, w rozumieniu art. 7 pkt. 6 ustawy, zawierające informacje komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione, 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. Przy czym szczególną uwagę zwrócić należy na fakt, iż nie jest wystarczające odnotowanie w formie papierowej informacji, o których mowa w § 7 ust. 1 pkt 4, zatem instrukcja nie może przewidywać takiego sposobu realizacji wspomnianego wymogu, gdyż byłoby to niezgodne z przedstawioną w ustawie definicją systemu informatycznego.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee

Zauważyć należy również, iż w przypadku 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. w sytuacji, 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 dedykowanym odnotowaniu informacji, o których mowa w § 7 ust. 1 pkt 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. Należy wskazać podmioty i osoby uprawnione do dokonywania przeglądów i konserwacji systemu informatycznego. Procedury wykonywania czynności konserwacyjnych systemu, w przypadku, gdy czynności te zleca się osobom nie posiadającym upoważnień do przetwarzania danych (np. specjalistom z firm zewnętrznych), powinny określać sposób, w jaki czynności te nadzorowane są przez administratora danych. w przypadku przekazywania do naprawy nośników informatycznych zawierających dane osobowe należy określić sposób usuwania danych osobowych z tych nośników, przed ich przekazaniem. 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.

miejsce na Twoje notatki

Istotne pytania

Ważne zdania, myśli, idee