Ochrona danych osobowych w zinformatyzowanych placówkach publicznych

Andrzej Kaczmarek

Biuro
Generalnego Inspektora
Ochrony Danych Osobowych

11. 05. 2009 r. Wars

Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl

Podstawy prawne ochrony danych osobowych

Konstytucja Rzeczypospolitej Polskiej

(art. 7.)

Organy władzy publicznej działają na podstawie i w granicach prawa

(art. 47.)

Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

(art. 51.)

1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniani informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Podstawy prawne ochrony danych osobowych

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny

(Dz. U. Nr 15, poz. 93 ze zm.)

(art. 23.)

DOBRA OSOBISTE CZŁOWIEKA, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.

(art. 24.)

§ 1. Ten, czyje dobro osobiste zostaje zagrożone, może żądać zaniechania tego działania, usunięcia jego skutków, a także zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.

§ 2. Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych.

Podstawy prawne ochrony danych osobowych

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926
2. Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2011 r. Nr 139, poz. 814)
3. USTAWA z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2011 r. Nr 113, poz. 657)
4. USTAWA z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (Dz.U. z 2013 poz. 674)
5. ……

Podstawy prawne w zakresie informatyzacji przetwarzania danych osobowych

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926
2. Rozporządzenie ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)
3. Ustawa z dnia 17 lutego o informatyzacji działalności podmiotów realizujących zadania publiczne tekst jedn. (Dz. U. z 2013 r., poz. 814)
4. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U z 2013 r., poz. 267)

Podstawy prawne w zakresie informatyzacji przetwarzania danych osobowych

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz. U. z 2012 r., poz. 526)
2. Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych

Przetwarzanie danych osobowych w zinformatyzowanych systemach administracji

Ustawa o ochronie danych osobowych - Rola i odpowiedzialnosc ADO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Urząd administracji jako Administrator Danych Osobowych (ADO)

Administrator danych osobowych - organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 u.o.d.o., decydująca o celach i środkach przetwarzania danych osobowych (art. 7, pkt 4 u.o.d.o.).

Art. 3 u.o.d.o.

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,
   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.

www.giodo.gov.pl

Ustawa o ochronie danych osobowych - Rola i odpowiedzialnść ADO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Kto to jest przetwarzający dane (procesor) – art. 31 u.o.d.o.

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.

Ustawa o ochronie danych osobowych - Rola i odpowiedzialność ADO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Obowiązki administratora danych osobowych w zakresie formalno prawnym

1. Zapewnienie legalności przetwarzania danych osobowych (art. 23 ust 1 u.o.d.o.) – zgoda, przepis prawa, realizacja umowy, dobro publiczne, usprawiedliwione cele ADO;
2. Wykonanie obowiązku informacyjnego wobec podmiotów danych (art. 24, 25 i 33 u.o.d.o.)
3. Dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą (art. 26, 26a, 27 u.o.d.o.)
4. 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 – są to obowiązki wynikające z praw podmiotu danych, o których mowa w art. 32 u.o.d.o.
5. Uzyskanie zgody na przekazanie danych do państwa trzeciego – jeśli dotyczy – (art. 48 u.o.d.o.)

Ustawa o ochronie danych osobowych - Rola i odpowiedzialność ADO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

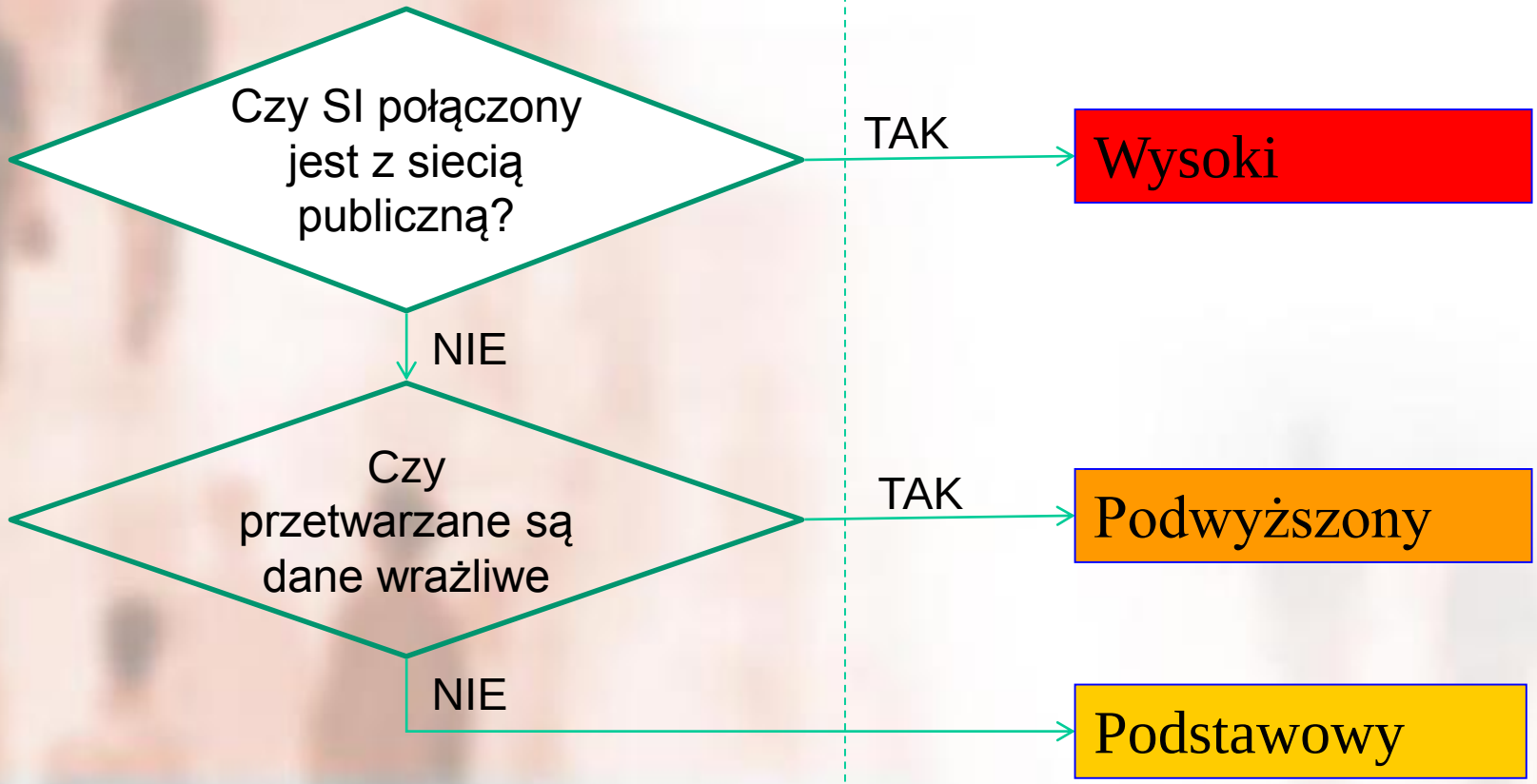
Obowiązki administratora danych osobowych w zakresie bezpieczeństwa danych osobowych

1. Zastosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie przed nieuprawnionym ujawnieniem, zmianą, utratą, uszkodzeniem lub zniszczeniem – (art. 36 ust. 1 u.o.d.o.)
2. Prowadzenie dokumentacji opisującej sposób przetwarzania danych oraz środki, o których mowa w ust. 1. – (art. 36 ust. 2)
3. Wyznaczenie administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1 – (art. 36 ust. 3)
4. Zapewnienie kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. - (art. 38)

Ustawa o ochronie danych osobowych
Wymagania dotyczące bezpieczeństwa

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Poziom zagrożeń, Kategorie danych	Wymagany poziom bezpieczeństwa



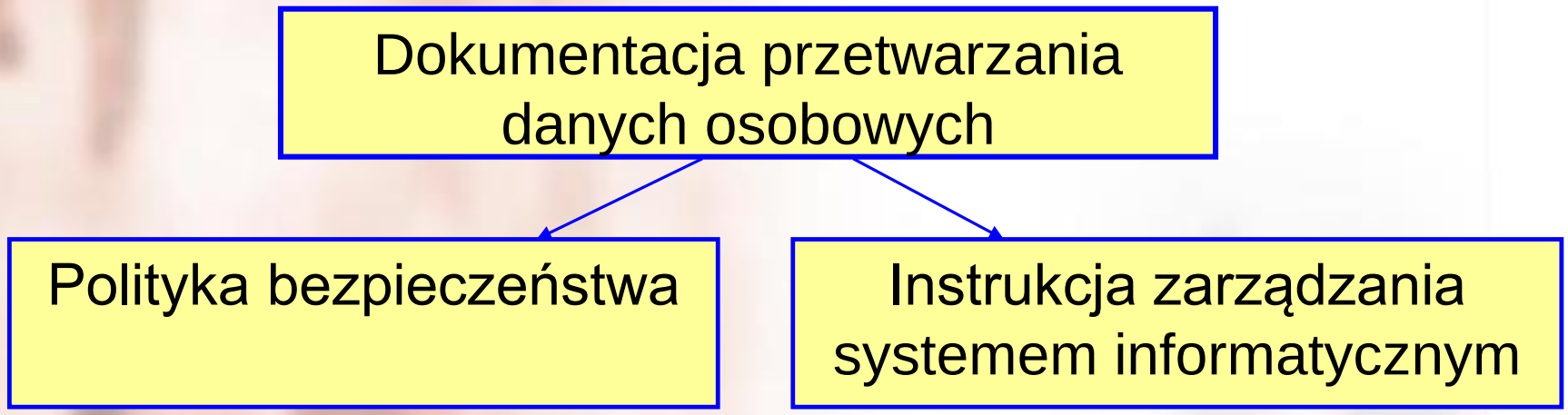
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

www.giodo.gov.pl

Ustawa o ochronie danych osobowych
Wymagania dotyczące dokumentacji

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Obowiązki administratora danych osobowych w zakresie dokumentacji przetwarzania danych osobowych ?



Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Ustawa o ochronie danych osobowych
Wymagania dotyczące polityki bezpieczeństwa

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Polityka bezpieczeństwa powinna zawierać (§ 4 rozporządzenia)

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.

Ustawa o ochronie danych osobowych
Wymagania dotyczące bezpieczeństwa

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Minimalne wymagania ochrony (załącznik do rozporządzenia)

Podstawowy

1) Zabezpieczenie obszaru przetwarzania;
2) Kontrola dostępu (indywidualne konto dla każdego użytkownika);
3) Zabezpieczenie przed szkodliwym oprogramowaniem i awarią zasilania;
4) Niepowtarzalność identyfikatora, odpowiednie parametry dotyczące hasła oraz obowiązek tworzenia kopi zapasowych;
5) Kryptograficzne zabezpieczenie komputerów przenośnych;
6) Odpowiednie procedury przenoszenia, likwidacji i napraw sprzętu;
7) Monitorowanie wdrożonych zabezpieczeń;

Podwyższony

8) Dodatkowa wymagania parametrów hasła dla danych wrażliwych;
9) Dodatkowe zabezpieczenie danych wrażliwych opuszczających obszar przetwarzania (ochrona kryptograficzna);
10) Opis sposobu zabezpieczenia o którym mowa w punkcie 9 i jego ochrona;

Wysoki

11) Kontrola i zabezpieczenie przepływy danych na styku z siecią publiczną;
12) Kryptograficzna ochrona danych przesyłanych w sieci publicznej;

www.giodo.gov.pl

Ustawa o ochronie danych osobowych
Wymagania dotyczące instrukcji zarządzania systemem

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Instrukcja zarządzania SI powinna zawierać (§ 5 rozporządzenia)

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania kopii zapasowych:
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania szkodliwego;
7) Sposób realizacji odnotowań o udostępnieniach danych;
8) Procedury wykonywania przeglądów, napraw, likwidacji sprzętu

Ustawa o ochronie danych osobowych
Wymagania dotyczące funkcjonalności

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Wymagania dotyczące funkcjonalności (§ 7 rozporządzenia)

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu;
   2) identyfikatora użytkownika wprowadzającego dane, chyba że dostęp do systemu posiada wyłącznie jedna osoba;
   3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
   4) informacji o odbiorcach, 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.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Ustawa o informatyzacji. Wymogi bezpieczeństwa

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Rozdział IV. § 20

§ 20. 1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

§ 20. 2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

Ustawa o informatyzacji. Wymogi bezpieczeństwa

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 20. 2. Wymagane działania:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

Ustawa o informatyzacji. Wymogi bezpieczeństwa

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 20. 2. Wymagane działania: c.d.

5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;

6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

Ustawa o informatyzacji. Wymogi bezpieczeństwa

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 20. 2. Wymagane działania: c.d.

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

Ustawa o informatyzacji. Wymogi bezpieczeństwa

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 20. 2. Wymagane działania: c.d.

12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,
b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
d) stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
e) zapewnieniu bezpieczeństwa plików systemowych,
f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych.
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

Ustawa o informatyzacji. Wymogi bezpieczeństwa

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 20. 2. Wymagane działania: c.d.

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjecie działań korygujących;

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

Rozdział IV. § 20. 3

Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie **Polskiej Normy PN-ISO/IEC 27001**, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:. **1) PN-ISO/IEC 17799, 2) PN-ISO/IEC 27005, 3) PN-ISO/IEC 24762**

Ustawa o informatyzacji. Wymogi bezpieczeństwa

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 21 – Wymagania dotyczące rozliczalności

1. Rozliczalność w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach).
2. W dziennikach systemów, o których mowa w ust. 1, odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do:
   1) systemu z uprawnieniami administracyjnymi;
   2) konfiguracji systemu, w tym konfiguracji zabezpieczeń;
   3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa (patrz u.o.d.o; ustawa o systemie informacji w ochronie zdrowia)

Ustawa o informatyzacji. Wymogi bezpieczeństwa

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 21 – Wymagania dotyczące rozliczalności c.d.

3. Poza informacjami wymienionymi w ust. 2 mogą być odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci:
   1) działań użytkowników nieposiadających uprawnień administracyjnych;
   2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu;
   3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny w zakresie wynikającym z analizy ryzyka.
4. Informacje w dziennikach systemów, o których mowa w ust. 2 i 3, przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.
5. Zapisy dzienników systemów mogą być składowane na zewnętrznych informatycznych nośnikach danych w warunkach zapewniających bezpieczeństwo informacji. W uzasadnionych przypadkach dzienniki systemów mogą być prowadzone na nośniku papierowym.

Ustawa o informatyzacji. Wymogi dotyczące funkcjonalności

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 15 Wymagania dotyczące funkcjonalności

1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

2. W przypadku gdy w danej sprawie brak jest przepisów, norm lub standardów, o których mowa w ust. 1, stosuje się standardy uznane na poziomie międzynarodowym, w szczególności opracowane przez:
   1) Internet Engineering Task Force (IETF) i publikowane w postaci Request For Comments (RFC),
   2) World Wide Web Consortium (W3C) i publikowane w postaci W3C Recommendation (REC)

Bezpieczeństwo korespondencji i wymiany danych

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. **Wymiana danych między systemami – przekazywanie danych w trybie wnioskowym (art. 15 ust. 3 ustawy o inf.) .**
2. **Elektroniczne przekazywanie danych między systemami (art. 16 ustawy o inf.)**
3. **Elektroniczne doręczanie pism (art. 39^1 KPA)**
4. **Elektroniczne potwierdzanie doręczenia (art. 46 KPA)**
5. **Bezpieczeństwo uwierzytelnienia (art. 20a ustawy i inf.)**

www.giodo.gov.pl

Przekazywanie danych – art. 15 ustawy o informatyzacji..

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. Podmiot prowadzący rejestr publiczny zapewnia podmiotowi publicznemu albo podmiotowi niebędącemu podmiotem publicznym, realizującym zadania publiczne na podstawie odrębnych przepisów albo na skutek powierzenia lub zlecenia przez podmiot publiczny ich realizacji, nieodpłatny dostęp do danych zgromadzonych w prowadzonym rejestrze, w zakresie niezbędnym do realizacji tych zadań.
2. Dane, o których mowa w ust. 1, powinny być udostępniane za pomocą środków komunikacji elektronicznej i mogą być wykorzystane wyłącznie do realizacji zadań publicznych
3. Rada Ministrów określi, w drodze rozporządzenia, sposób, zakres i tryb udostępniania danych, o których mowa w ust. 1, mając na uwadze potrzebę usprawnienia realizacji zadań publicznych, zapewnienia szybkiego i bezpiecznego dostępu do danych oraz zabezpieczenia wykorzystania danych do celów realizacji zadań publicznych.

ROZPORZĄDZENIE RADY MINISTRÓW z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (D.U. 2005.205.1692)

www.giodo.gov.pl

Ustawa o informatyzacji – przekazywanie danych na wniosek

GIODO
Generalny Inspektor Ochrony Danych Osobowych

ROZPORZĄDZENIE RADY MINISTRÓW z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym

§ 1. Rozporządzenie określa sposób, zakres i tryb udostępniania danych zgromadzonych w rejestrze publicznym, zwanym dalej *„rejestrem”*, podmiotowi publicznemu albo podmiotowi niebędącemu podmiotem publicznym, realizującym zadania publiczne na podstawie odrębnych przepisów albo na skutek powierzenia lub zlecenia przez podmiot publiczny ich realizacji.
§ 2.1. Dane zgromadzone w rejestrze udostępnia się podmiotom, o których mowa w § 1, na ich wniosek złożony w formie pisemnej albo elektronicznej.

§ 4. 1. Podmiot, któremu udostępniono dane zgromadzone w rejestrze, zabezpiecza otrzymane dane przed dostępem osób nieupoważnionych lub nieuprawnioną zmianą ich zawartości oraz przed ich wykorzystaniem niezgodnym z celem, dla którego zostały uzyskane.
2. Podmiot, któremu udostępniono dane zgromadzone w rejestrze, odpowiada za bezpieczeństwo i integralność uzyskanych danych.

www.giodo.gov.pl

Ustawa o informatyzacji – przekazywanie danych na wniosek

GIODO
Generalny Inspektor Ochrony Danych Osobowych

WNIOSEK
o udostępnienie danych zgromadzonych w rejestrze publicznym

1. .....
(wskazanie zadania publicznego i podstawy prawnej jego realizacji przez podmiot ubiegający się o udostępnienie danych zgromadzonych w rejestrze, którego wykonanie wymaga udostępnienia tych danych)

.....

2. .....
(określenie rejestru, w którym są zgromadzone dane, które mają być udostępnione)

3. .....
(zakres żądanych danych i wskazanie sposobu ich udostępniania)

.....

4. .....
(wskazanie okresu udostępnienia danych)

..... zobowiązuje się do
(nazwa podmiotu)

wykorzystywania udostępnionych danych wyłącznie do realizacji zadania publicznego wskazanego w pkt 1.

..... Oświadcza, że spełnia
(nazwa podmiotu)

warunki zabezpieczeń technicznych i organizacyjnych niezbędnych do uzyskania dostępu do danych zgromadzonych w rejestrze wskazanym w pkt 2.

www.giodo.gov.pl

Stosowane praktyki – przekazywania danych

USTAWA z dnia 6 kwietnia 1990 r. o Policji (tekst jednolity: Dz. U. 2011 r. Nr 287 poz. 1687)

Art. 20 ust. 15. Policja *może uzyskiwać, gromadzić* i przetwarzać informacje, w tym również dane osobowe ze zbiorów prowadzonych na podstawie odrębnych przepisów przez organy władzy publicznej… Administratorzy danych gromadzonych w tych rejestrach są obowiązani do nieodpłatnego ich udostępniania.

Art. 20 ust. 16. Organy władzy publicznej prowadzące rejestry, o których mowa w ust. 15, mogą, w drodze decyzji, wyrazić zgodę na udostępnianie za pomocą urządzeń telekomunikacyjnych informacji zgromadzonych w rejestrach jednostkom organizacyjnym Policji, bez konieczności składania pisemnych wniosków, jeżeli jednostki te:

1) posiadają urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie dane uzyskał;
2) **posiadają zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania;**
3) jest to uzasadnione specyfiką lub zakresem wykonywania zadań albo prowadzonej działalności.

Stosowane praktyki – przekazywania danych

GIODO
Generalny Inspektor Ochrony Danych Osobowych

USTAWA z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy (tekst jednolity: Dz. U. 2013 r. poz. 674)

Art. 33 ust. 6. Informacje dotyczące bezrobotnych, poszukujących pracy i cudzoziemców na terytorium RP są przetwarzane przez powiatowe urzędy pracy, w szczególności z wykorzystaniem systemów teleinformatycznych i dokumentów elektronicznych.

Art. 33 ust. 7. Informacje, o których mowa w ust. 6, są udostępniane publicznym służbom zatrudnienia lub innym podmiotom, realizującym zadania na podstawie ustawy lub odrębnych przepisów albo na skutek powierzenia.

Art. 33 ust. 8. Informacje, o których mowa w ust. 6, mogą być pozyskiwane, wymieniane lub udostępniane na wniosek…lub z wykorzystaniem systemów teleinformatycznych, jeżeli powiatowy urząd pracy oraz podmiot, o którym mowa w ust. 7, spełniają łącznie następujące warunki:

1) posiadają możliwość identyfikacji osoby uzyskującej informacje w systemie oraz zakresu, daty i celu ich uzyskania;
2) **<u>posiadają zabezpieczenia uniemożliwiające wykorzystanie informacji niezgodnie z celem ich uzyskania</u>**;
3) zapewniają, że dostęp do danych osobowych jest nadzorowany i rejestrowany zgodnie z przepisami o ochronie danych osobowych.

www.giodo.gov.pl

Stosowane praktyki – przekazywania danych

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Projekt ustawy o zmianie ustawy o świadczeniach rodzinnych oraz niektórych innych ustaw

Art. 23b. 1. Organ właściwy oraz marszałek województwa prowadzący postępowanie w sprawie świadczeń rodzinnych są obowiązani do samodzielnego uzyskania od organów podatkowych, organów emerytalno-rentowych oraz z rejestrów publicznych, w drodze wymiany informacji w postaci elektronicznej lub w drodze pisemnej, odpowiednio:

1) zaświadczenia lub informacji o dochodzie podlegającym opodatkowaniu podatkiem dochodowym od osób fizycznych, na zasadach określonych w art. 27, art. 30b, art. 30c i art. 30e ustawy z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych, każdego członka rodziny, wydanych przez naczelnika właściwego urzędu skarbowego, zawierających dane o wysokości:
   a) dochodu,
   b) składek na ubezpieczenia społeczne odliczonych od dochodu,
   c) należnego;
2) informacji o wieku dziecka;
3) zaświadczenia lub informacji o wysokości składek na ubezpieczenie zdrowotne, w tym informacji o wysokości składek od poszczególnych płatników i okresach opłacania przez nich składek;
4) ……

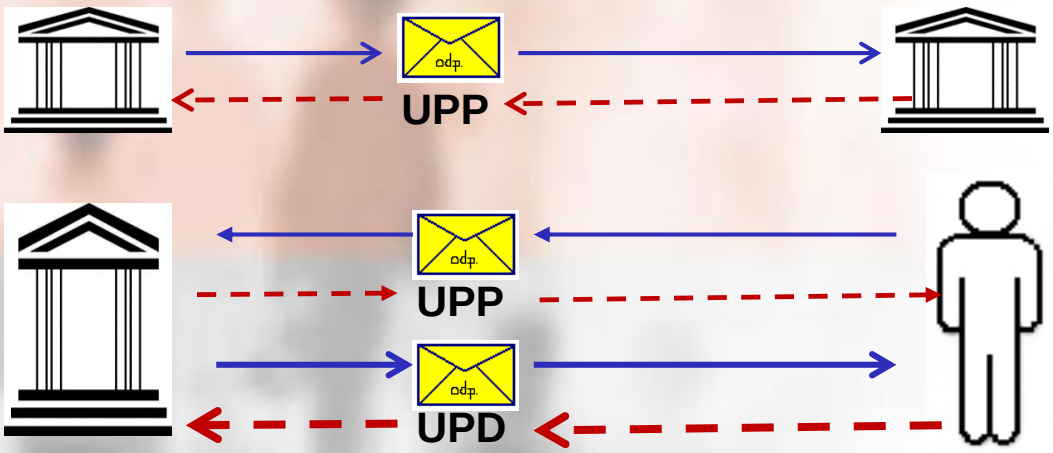
Bezpieczne przekazywanie pism do urzędu lub obywatela

GIODO
Generalny Inspektor Ochrony Danych Osobowych

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych

Rozporządzenie określa:

1) warunki organizacyjno-techniczne doręczania dokumentów elektronicznych, w tym reguły tworzenia elektronicznej skrzynki podawczej;
2) formę urzędowego poświadczania odbioru dokumentów elektronicznych przez adresatów;
3) sposób sporządzania i doręczania pism w formie dokumentów elektronicznych;
4) sposób udostępniania kopii dokumentów elektronicznych oraz warunki bezpieczeństwa udostępniania formularzy i wzorów dokumentów.



www.giodo.gov.pl

Elektroniczne doręczanie pism (po 11 maja) - Art. 39[1] KPA.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

§ 1. Doręczenie następuje za pomocą środków komunikacji elektronicznej w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.), jeżeli strona lub inny uczestnik postępowania:

1) złoży podanie w formie dokumentu elektronicznego przez elektroniczną skrzynkę podawczą organu administracji publicznej;
2) wystąpi do organu administracji publicznej o takie doręczenie i wskaże organowi administracji publicznej adres elektroniczny;
3) wyrazi zgodę na doręczanie pism w postępowaniu za pomocą tych środków i wskaże organowi administracji publicznej adres elektroniczny.

Art. 63 § 5 Urzędowe poświadczenie odbioru (UPP) podania wniesionego w formie dokumentu elektronicznego zawiera:

1) informację o tym, że pisma w sprawie będą doręczane za pomocą środków komunikacji elektronicznej;
2) pouczenie o prawie do rezygnacji z doręczania pism za pomocą środków komunikacji elektronicznej, o którym mowa w art. 39[1] § 1d.

Potwierdzenie doręczenia pisma (po 11 maja) - Art. 46 KPA

GIODO
Generalny Inspektor Ochrony Danych Osobowych

§ 4. W celu doręczenia pisma w formie dokumentu elektronicznego organ administracji publicznej przesyła na adres elektroniczny adresata zawiadomienie zawierające:

1) wskazanie, że adresat może odebrać pismo w formie dokumentu elektronicznego;
2) wskazanie adresu elektronicznego, z którego adresat może pobrać pismo i pod którym powinien dokonać potwierdzenia doręczenia pisma;
3) pouczenie dotyczące sposobu odbioru pisma, a w szczególności sposobu identyfikacji pod wskazanym adresem elektronicznym w systemie teleinformatycznym organu administracji publicznej, oraz informację o wymogu podpisania urzędowego poświadczenia odbioru w sposób wskazany w art. 20a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Art. 20a ustawy o informatyzacji

1. Identyfikacja użytkownika systemów teleinformatycznych udostępnianych przez podmioty określone w art. 2 następuje przez zastosowanie kwalifikowanego certyfikatu przy zachowaniu zasad przewidzianych w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.), lub profilu zaufanego ePUAP.
2. Podmiot publiczny, który używa do realizacji zadań publicznych systemów teleinformatycznych, może umożliwiać użytkownikom identyfikację w tym systemie przez zastosowanie innych technologii, chyba że przepisy odrębne przewidują obowiązek dokonania czynności w siedzibie podmiotu publicznego.

Potwierdzenie doręczenia pisma (po 11 maja) - Art. 46 KPA

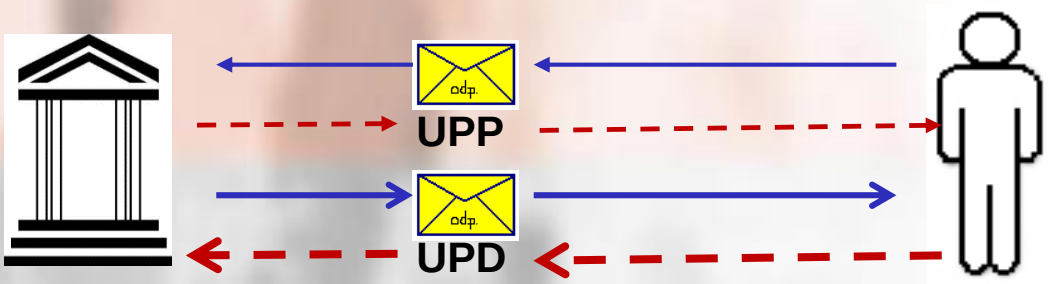
GIODO
Generalny Inspektor Ochrony Danych Osobowych

§ 5. W przypadku nieodebrania pisma w formie dokumentu elektronicznego w sposób, o którym mowa w § 4 pkt 3, organ administracji publicznej po upływie 7 dni, licząc od dnia wysłania zawiadomienia, przesyła powtórne zawiadomienie o możliwości odebrania tego pisma.

§ 6. W przypadku nieodebrania pisma doręczenie uważa się za dokonane po upływie czternastu dni, licząc od dnia przesłania pierwszego zawiadomienia.

§ 7. Zawiadomienia, o których mowa w § 4 i 5, mogą być automatycznie tworzone i przesyłane przez system teleinformatyczny organu administracji publicznej, a odbioru tych zawiadomień nie potwierdza się.

§ 8. W przypadku uznania pisma w formie dokumentu elektronicznego za doręczone na podstawie § 6 organ administracji publicznej umożliwia adresatowi pisma dostęp do treści pisma w formie dokumentu elektronicznego przez okres co najmniej 3 miesięcy od dnia uznania pisma w formie dokumentu elektronicznego za doręczone oraz do informacji o dacie uznania pisma za doręczone i datach wysłania zawiadomień, o których mowa w § 4 i 5, w swoim systemie teleinformatycznym.



Wymagane atrybutu bezpieczeństwa:

- Poufność (protokoły szyfrowane)
- Autentyczność (certyfikat kwalifikowany, profil zaufany ePUAP)
- Niezaprzeczalnosć (podpis elektroniczny)

www.giodo.gov.pl

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Dziękuję za uwagę

Andrzej Kaczmarek

Biuro Generalnego Inspektora Ochrony Danych Osobowych

A_Kaczmarek@giodo.gov.pl

www.giodo.gov.pl