POLITECHNIKA RZESZOWSKA
im. IGNACEGO ŁUKASIEWICZA

Prawa, normy i standardy

- Ustawa o ochronie danych osobowych z dnia 29.08.1997 r. (Dz.U. Nr 133, poz. 883) tekst jednolity z dnia 17.06.2002 r. (Dz.U. Nr 101,poz. 926)

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 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 dnia 1.05.2004r)

- Rozporządzenie Rady Ministrów z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

- Rozporządzenie Ministra Infrastruktury z dnia28.12.2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania

- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

Prawa, normy i standardy

- **Normy:**

  - PN-ISO/IEC 27001
  - PN-ISO/IEC 17799
  - PN-ISO/IEC 27005
  - ISO/IEC 22301
  - PN-ISO/IEC 24762
  - PN-ISO/IEC 20000-1:2014-01
  - PN-ISO/IEC 20000-2:2007

Prawa, normy i standardy

- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 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 dn 1.05.2004r.)**

- § 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.

Prawa, normy i standardy

- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 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 dn 1.05.2004r.)**

- § 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;
  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,

Prawa, normy i standardy

- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 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 dn 1.05.2004r.)**

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

➢Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania

- § 1. Rozporządzenie określa:
  1) szczegółowy wykaz danych niezbędnych do:
     a) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, inicjującego połączenie,
     b) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, do którego jest kierowane połączenie,
     c) określenia daty i godziny połączenia oraz czasu jego trwania,
     d) określenia rodzaju połączenia,
     e) określenia lokalizacji telekomunikacyjnego urządzenia końcowego;

➢Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania

- § 6. Danymi niezbędnymi w przypadku usługi dostępu do Internetu, usługi poczty elektronicznej i usługi telefonii internetowej:
  1) do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, inicjującego połączenie, są:
     a) identyfikator użytkownika,
     b) numer przydzielony użytkownikowi końcowemu, korzystającemu z dostępu dial-up,
     c) identyfikator użytkownika i numer przydzielony użytkownikowi końcowemu inicjującemu połączenie kierowane do publicznej sieci telekomunikacyjnej,
     d) adres IP,
     e) imię i nazwisko albo nazwa oraz adres użytkownika końcowego, któremu w czasie połączenia przypisano adres IP, a także identyfikator użytkownika lub przydzielony mu numer w telefonii internetowej,

- **Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania**

f) identyfikator zakończenia sieci, w którym użytkownik końcowy uzyskał dostęp do Internetu, w szczególności identyfikator cyfrowej linii abonenckiej DSL (Digital Subscriber Line), numer wykorzystywanego portu sieciowego lub adres MAC urządzenia końcowego inicjującego połączenie;

2) do ustalenia daty i godziny połączenia oraz czasu jego trwania są:

a) data i godzina każdorazowego połączenia i rozłączenia z Internetem, zgodnie z czasem lokalnym, wraz z przydzielonymi dynamicznie lub statycznie adresami IP wykorzystywanymi w czasie trwania połączenia oraz identyfikatorem użytkownika,

b) data i godzina zalogowania i wylogowania z usługi poczty elektronicznej i telefonii internetowej, zgodnie z czasem lokalnym.

- **Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania**

- § 7. Danymi niezbędnymi w przypadku usługi poczty elektronicznej i usługi telefonii internetowej do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, do którego jest kierowane połączenie, są:
  a) numer przydzielony użytkownikowi końcowemu, do którego jest kierowane połączenie w telefonii internetowej,
  b) imię i nazwisko albo nazwa oraz adres zarejestrowanego użytkownika końcowego usługi poczty elektronicznej lub usługi telefonii internetowej, do którego jest kierowane połączenie, oraz identyfikator tego użytkownika;

➢Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne

- Art. 180a.:

1. Z zastrzeżeniem art. 180c ust. 2 pkt 2, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt:
   1) zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi;
   2) udostępniać dane, o których mowa w pkt 1, uprawnionym podmiotom, a także Służbie Celnej, sądowi i prokuratorowi, na zasadach i w trybie określonych w przepisach odrębnych;
   3) chronić dane, o których mowa w pkt 1, przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, zgodnie z przepisami art. 159–175a, art. 175c i art. 180e.

➢Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

- Art. 18:
  1. Usługodawca może przetwarzać następujące dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi:
     1) nazwisko i imiona usługobiorcy,
     2) numer ewidencyjny PESEL lub – gdy ten numer nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość,
     3) adres zameldowania na pobyt stały,
     4) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 3,
     5) dane służące do weryfikacji podpisu elektronicznego usługobiorcy,
     6) adresy elektroniczne usługobiorcy.
  2. W celu realizacji umów lub dokonania innej czynności prawnej z usługobiorcą, usługodawca może przetwarzać inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia.

➢Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

- Art. 18:

5. Usługodawca może przetwarzać następujące dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną (dane eksploatacyjne):
   1) oznaczenia identyfikujące usługobiorcę nadawane na podstawie danych, o których mowa w ust. 1,
   2) oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca,
   3) informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną,
   4) informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.
6. Usługodawca udziela informacji o danych, o których mowa w ust. 1–5, organom państwa na potrzeby prowadzonych przez nie postępowań.

Podmiot zobowiązany ponosi koszty związane z zapewnieniem technicznych i organizacyjnych możliwości wykonania postanowienia sądu lub prokuratora

➢Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

- Art.20:
  1. Usługodawca, który przetwarza dane osobowe usługobiorcy, jest obowiązany zapewnić usługobiorcy dostęp do aktualnej informacji o:
     1) możliwości korzystania z usługi świadczonej drogą elektroniczną anonimowo lub z wykorzystaniem pseudonimu, o ile są spełnione warunki określone w art. 22 ust. 2,
     2) udostępnianych przez usługodawcę środkach technicznych zapobiegających pozyskiwaniu i modyfikowaniu przez osoby nieuprawnione, danych osobowych przesyłanych drogą elektroniczną,
     3) podmiocie, któremu powierza przetwarzanie danych, ich zakresie i zamierzonym terminie przekazania, jeżeli usługodawca zawarł z tym podmiotem umowę o powierzenie do przetwarzania danych, o których mowa w art. 18 ust. 1, 2, 4 i 5.
  2. Informacje, o których mowa w ust. 1, powinny być dla usługobiorcy stale i łatwo dostępne za pomocą systemu teleinformatycznego, którym się posługuje.

➢Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

- Art.21.:

1. W przypadku uzyskania przez usługodawcę wiadomości o korzystaniu przez usługobiorcę z usługi świadczonej drogą elektroniczną niezgodnie z regulaminem lub z obowiązującymi przepisami (niedozwolone korzystanie), usługodawca może przetwarzać dane osobowe usługobiorcy w zakresie niezbędnym do ustalenia odpowiedzialności usługobiorcy, pod warunkiem że utrwali dla celów dowodowych fakt uzyskania oraz treść tych wiadomości.

2. Usługodawca może powiadomić usługobiorcę o jego nieuprawnionych działaniach z żądaniem ich niezwłocznego zaprzestania, a także o skorzystaniu z uprawnienia, o którym mowa w ust. 1.

❖ Postępowanie cywilne:

- Sąd może zobowiązać administratora portalu do przekazania informacji o użytkowniku

• Podstawa prawna:

– Prawo prasowe

– Kodeksu postępowania cywilnego

- **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**

- Art.15.:
  1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem: funkcjonalności, niezawodności, używalności, wydajności, przenoszalności, pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnych standardów i metodyk
  2. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.
  3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.

Prawa, normy i standardy

➢ **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**

- Art.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 – w odniesieniu do ustanawiania zabezpieczeń;
   2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;
   3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.
4. Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

➢Polityka Bezpieczeństwa Systemów Teleinformatycznych – struktura i zapisy.

- Metody zapewnienia bezpieczeństwa danych
- Monitorowanie temperatury i wilgotności.
- Monitoring pomieszczeń.
- Zabezpieczenie urządzeń teleinformatycznych przed:
  - Nieautoryzowanym dostępem.
  - Awariami.
  - Zakłóceniami pracy.
- Zabezpieczenie okablowania strukturalnego oraz zasilającego.
- Prowadzenie rejestru licencji na systemy i aplikacje.
- Zarządzanie bezpieczeństwem sieci:
  - Zarządzanie urządzeniami sieciowymi może odbywać się poprzez komunikacje zaszyfrowaną;
  - Lokalnie;
  - Z wydzielonego segmentu sieci;

Polityka Bezpieczeństwa Systemu

➢Polityka Bezpieczeństwa Systemów Teleinformatycznych – struktura i zapisy.

- Polityka dostępu do zasobów sieci wewnętrznej
- Polityka dostępu do systemów teleinformatycznych
- Polityka dostępu Internetu
- Monitorowanie i pomiary:
  - Zapisy związane z bezpieczeństwem
  - Archiwizacja logów bezpieczeństwa przez okres ? lat;
  - Zasady przeglądu logów
  - Prowadzenie logów kopii zapasowych
  - Synchronizacja zegarów z NTP
- Prowadzenie dzienników administracyjnych:
  - Prowadzenie dzienników administracyjnych w zakresie istotnych czynności;
  - Prowadzenie dzienników awarii systemów;
  - Prowadzenie rejestru kopii zapasowych tworzonych na nośnikach zewnętrznych;
  - Należy stosować logowanie i archiwizowanie zapisów z temperatury oraz wilgotności

➢Polityka Bezpieczeństwa Systemów Teleinformatycznych – struktura i zapisy.

- Zabezpieczenia kryptograficzne:
  - Dostęp zdalny;
  - Dyski komputerów przenośnych;
  - Nośniki zewnętrzne, w tym pendrive;
- Praca na odległość:
  - Zabezpieczenia urządzeń mobilnych: AV, szyfrowanie komunikacji;
  - Odłączenie zdalnych sesji podczas określonego czasu bezczynności;
- Zarządzanie zmianami i konfiguracją:
  - Wnioskowanie o zmianę
  - Ocena ryzyka wprowadzenia zmiany
  - Zabezpieczenie przed wprowadzeniem zmiany
  - Zapisy wprowadzonej zmiany
  - Potwierdzenie realizacji
  - Priorytet oraz istotność zmiany