Ochrona danych osobowych

dr inż. Bolesław Szomański

bolosz@wz.pw.edu.pl

Plan prezentacji

- Konstytucja
- Dyrektywy UE
- Ustawy
- Ustawa o Ochronie Danych Osobowych
- Rozporządzenie o Ochronie Danych Osobowych

Przepisy prawne

- Ochrona danych osobowych
- Podstawy prawne
  - Konstytucja
  - Umowy międzynarodowe,
    - Dyrektywy i inne akty Unii Europejskie
  - Ustawy
  - Rozporządzenia

Konstytucja RP

- Art. 31.
  - Wolność człowieka podlega ochronie prawnej.
- 1. Każdy jest obowiązany szanować wolności i prawa innych.
  - Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje.
- 2. Ograniczenia w zakresie korzystania z konstytucyjnych
- wolności i praw mogą być ustanawiane
  - tylko w ustawie i
  - tylko wtedy, gdy są konieczne w demokratycznym państwie
  - dla jego bezpieczeństwa lub porządku publicznego,
  - bądź dla ochrony środowiska, zdrowia i moralności publicznej,
  - albo wolności i praw innych osób.
  - Ograniczenia te nie mogą naruszać istoty wolności i praw.

Konstytucja RP

- Art. 51.
- 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy
  - do ujawniania 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.

Umowy międzynarodowe, Dyrektywy i inne akty Unii Europejskiej

- 1. KONWENCJA nr 108 Rady Europy z dnia 28 stycznia 1985 r. o
  - ochronie osób w związku z automatycznym przetwarzaniem danych osobowych
- 2. DYREKTYWA 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
- 3. ROZPORZĄDZENIE (WE) NR 45/2001
  - Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r.
  - o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych
  - przez instytucje i organy wspólnotowe i o
  - swobodnym przepływie takich danych
- 4. DYREKTYWA 2002/58/WE Parlamentu Europejskiego i
  - Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i
  - ochrony prywatności w sektorze łączności elektronicznej
  - (dyrektywa o prywatności i łączności elektronicznej)

Ustawy i Rozporządzenia

- 1. USTAWA z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
- 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
- 3 ROZPORZĄDZENIE PREZYDENTA RZECZYPOSPOLITEJ POLSKIEJ
    - z dnia 29 maja 1998 r. w
  - sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych
- 4. ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI
  - z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i
  - legitymacji służbowej inspektora
    - Biura Generalnego Inspektora Ochrony Danych Osobowych
- 5. ROZPORZĄDZENIE MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI
  - z dnia 29 kwietnia 2004 r. w sprawie wzoru zgłoszenia zbioru danych do
  - rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych

Inne Ustawy

- 1. USTAWA z dnia 18 lipca 2002 r. o
  - świadczeniu usług drogą elektroniczną
- 2. USTAWA z dnia 14 lutego 2003 r. o
  - udostępnianiu informacji gospodarczych
- 3. USTAWA z dnia 16 lipca 2004 r.
  - Prawo telekomunikacyjne
- 4. USTAWA z dnia 5 sierpnia 2010 r. o
  - ochronie informacji niejawnych
- 5. USTAWA z dnia 28 października 2002 r. o
  - odpowiedzialności podmiotów zbiorowych
  - za czyny zabronione pod groźbą kary

USTAWY

- 6. USTAWA z dnia 16 kwietnia 1993 r. o zwalczaniu
  - nieuczciwej konkurencji
- 7. USTAWA z dnia 29 czerwca 1995 r. o statystyce publicznej
- 8. USTAWA z dnia 26 stycznia 1984 r. Prawo prasowe
- 9. USTAWA z dnia 24 sierpnia 1991 r.
  - o ochronie przeciwpożarowej
- 10. USTAWA z dnia 22 sierpnia 1997 r. o ochronie osób i mienia
- 11. USTAWA z dnia 26 czerwca 1974 r. Kodeks pracy
- 12. USTAWA z dnia 23 kwietnia 1964 r. Kodeks cywilny
- 13. USTAWA z dnia 6 czerwca 1997 r. Kodeks karny
- 14. USTAWY o: Policji, ABW, AW, CBA, SG, …….

USTAWA O OCHRONIE DANYCH OSOBOWYCH

- 1. Podstawowe pojęcia i definicje
- 2. Zasady przetwarzania danych osobowych
- 3. Warunki dopuszczalności
  - przetwarzania danych osobowych
- 4. Generalny Inspektor Danych Osobowych (GIODO)
- 5. Rejestracja zbiorów
- 6. Prawa osób, których dane są przetwarzane
- 7. Obowiązki administratorów danych osobowych
- 8. Ochrona przetwarzania danych osobowych
- 9. Udostępnianie danych osobowych
- 10. Powierzanie przetwarzania danych osobowych
- 11. Odpowiedzialność karna i finansowa

UoDO –Pojęcia i definicje

- Dane osobowe - Art. 6.
- 1. 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.

Dane osobowe wrażliwe –Art. 2i7

- Dane osobowe ujawniające
  - pochodzenie rasowe lub etniczne, poglądy polityczne,
  - przekonania religijne lub filozoficzne,
  - przynależność wyznaniową, partyjną lub związkową,
  - jak również dane o stanie zdrowia, kodzie genetycznym,
  - nałogach lub życiu seksualnym oraz dane dotyczące skazań,
  - orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń
  - wydanych w postępowaniu sądowym lub administracyjnym
  - są danymi wrażliwymi
- Zbiór danych - Art. 7.
  - Każdy posiadający strukturę zestaw danych o charakterze osobowym,
  - dostępnych według określonych kryteriów, niezależnie od tego,
  - czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Art. 27

- Doraźny zbiór danych – Art. 2.
  - Zbiór danych osobowych sporządzanych wyłącznie ze
  - względów technicznych, szkoleniowych lub w związku z
  - dydaktyką w szkołach wyższych, a po ich wykorzystaniu
  - niezwłocznie usuwanych albo poddanych anonimizacji.
- Przetwarzanie danych – Art. 7.
  - 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.
- Zgoda osoby, której dane dotyczą – Art. 7.
  - 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.

Administrator danych – Art. 7.

- Organ, jednostka organizacyjna, podmiot lub osoba, decydujące
  - o celach i środkach przetwarzania danych osobowych:
  - organy państwowe, organy samorządu terytorialnego oraz
    - państwowe i komunalne jednostki organizacyjne,
  - podmioty niepubliczne realizujące zadania publiczne,
  - osoby fizyczne i osoby prawne oraz
  - jednostki organizacyjne niebędące 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,

ABI – Art. 36.

- o ile przetwarzają dane osobowe przy
- wykorzystaniu środków technicznych znajdujących się na
- terytorium Rzeczypospolitej Polskiej.

- Administrator danych wyznacza
- administratora bezpieczeństwa informacji, nadzorującego
  - przestrzeganie zasad ochrony przetwarzania danych osobowych, chyba że
  - sam wykonuje te czynności.

UoDO - Zasady przetwarzania danych osobowych

- Legalność – zgodność z przepisami
- Celowość – istnienie celu przetwarzania
  - (chyba że przepis innej ustawy zezwala
    - na przetwarzanie danych
  - bez ujawniania faktycznego celu ich zbierania-Art. 24.)
- Poprawność – zgodność ze stanem faktycznym
- Istotność – zgodność z celem przetwarzania
- Terminowość – określony przedział
  - czasowy przetwarzania

UoDO - Warunki dopuszczalności przetwarzania danych osobowych

- Osoba, której dane dotyczą, wyrazi na to zgodę
  - (chyba że chodzi o usunięcie dotyczących jej danych).
- Jest to niezbędne dla zrealizowania uprawnienia lub
  - spełnienia obowiązku wynikającego z przepisu prawa.
- 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.
- Jest niezbędne do wykonania określonych prawem zadań
  - realizowanych dla dobra publicznego.

UoDO

- 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
    - (np. marketing bezpośredni własnych produktów lub
    - usług administratora danych,
- Dochodzenie roszczeń z tytułu
  - prowadzonej działalności gospodarczej .

UoDO – Warunki dopuszczalności przetwarzania danych osobowych - odstępstwa

- Przetwarzanie bez zgody:
  - Jeżeli przetwarzanie danych jest niezbędne dla
  - ochrony żywotnych interesów osoby, której dane dotyczą, a
    - uzyskanie zgody jest niemożliwe, można przetwarzać dane bez zgody tej osoby,
    - do czasu, gdy uzyskanie zgody będzie możliwe.
- Przetwarzanie w innym celu:
  - Dane są niezbędne do badań naukowych, dydaktycznych,
  - historycznych, statystycznych lub
    - badania opinii publicznej, a ich przetwarzanie nie narusza praw lub
    - wolności osoby, której dane dotyczą.
- Przetwarzanie danych w zbiorach doraźnych

UoDO –Przetwarzanie wrażliwych danych osobowych

- Przetwarzanie jest zabronione
- chyba, że:
  - 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,
  - 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,

UoDO –Przetwarzanie wrażliwych danych osobowych

- 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,

UoDO –Przetwarzanie wrażliwych danych osobowych

- 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.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.przetwarzanie danych jest prowadzone przez stronę w
  - celu realizacji praw i obowiązków wynikających z
  - orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

UoDO - Generalny Inspektor Danych Osobowych (GIODO)

- GIODO organem **do spraw** ochrony danych osobowych.
- Powołuje **i odwołuje go** Sejm **Rzeczypospolitej Polskiej**
  - za zgodą Senatu.
- **W zakresie wykonywania swoich zadań** GIODO podlega
  - tylko ustawie.
- **Wykonuje swoje zadania** przy pomocy
  - Biura Generalnego Inspektora Ochrony Danych Osobowych, którego
  - organizację oraz zasady działania określa statut nadany,
  - w drodze rozporządzenia, przez Prezydenta Rzeczypospolitej Polskiej.

GIODO

- Generalny Inspektor, zastępca Generalnego Inspektora lub
- upoważnieni przez niego pracownicy Biura, mają prawo:
  - 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,
  - żądać złożenia pisemnych lub ustnych wyjaśnień oraz
    - wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
    - wglądu do wszelkich dokumentów i wszelkich danych mających
    - bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,
  - przeprowadzania oględzin urządzeń, nośników oraz
    - systemów informatycznych służących do przetwarzania danych,
  - zlecać sporządzanie ekspertyz i opinii.

UoDO - Rejestracja zbiorów – Art. 40. – 41.

- Administrator danych jest obowiązany zgłosić zbiór danych
- do rejestracji oraz każdą zmianę w terminie 30 dni
- od dnia dokonania:
  - 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, ewentualne oznaczenie podmiotu, któremu
    - powierzono przetwarzanie danych i adres jego siedziby
      - lub miejsce zamieszkania,
  - wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych,
  - cel przetwarzania danych,
  - opis kategorii osób, których dane dotyczą, oraz
  - zakres przetwarzanych danych,

UoDO - Rejestracja zbiorów

- Sposób zbierania oraz udostępniania danych,
- informację o odbiorcach lub kategoriach odbiorców
  - którym dane mogą być przekazywane,
- opis środków technicznych i organizacyjnych
  - zastosowanych w celach zabezpieczenia danych osobowych oraz
- informację o sposobie wypełnienia warunków technicznych
  - i organizacyjnych zgodnie z Rozporządzeniem MSWiA
- informację dotyczącą ewentualnego przekazywania
  - danych do państwa trzeciego.

UoDO - Rejestracja zbiorów – wyjątki (Art. 43.)

- Nie rejestruje się zbiorów:
  - objętych tajemnicą państwową ze względu na obronność
    - lub bezpieczeństwo państwa, ochronę życia i zdrowia ludzi,
    - mienia lub bezpieczeństwa i porządku publicznego,
  - które zostały uzyskane w wyniku czynności
    - operacyjno-rozpoznawczych przez
    - funkcjonariuszy organów uprawnionych do tych czynności,
  - przetwarzanych przez właściwe organy dla
    - potrzeb postępowania sądowego oraz
    - na podstawie przepisów o Krajowym Rejestrze Karnym,
  - przetwarzanych przez
    - Generalnego Inspektora Informacji Finansowej,

UoDO - Rejestracja zbiorów

- przetwarzanych przez właściwe organy na potrzeby udziału
  - Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz
  - Systemie Informacji Wizowej,
- dotyczących osób należących do kościoła lub innego związku wyznaniowego,
  - o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego,
- przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na
  - podstawie umów cywilnoprawnych, a także
  - dotyczących osób u nich zrzeszonych lub uczących się,
- dotyczących osób korzystających z ich usług medycznych, obsługi notarialnej,
  - adwokackiej, radcy prawnego, rzecznika patentowego,
  - doradcy podatkowego lub biegłego rewidenta,
- tworzonych na podstawie przepisów dotyczących wyborów
  - do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i
  - sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej,
  - wójta, burmistrza, prezydenta miasta oraz
  - dotyczących referendum ogólnokrajowego i referendum lokalnego,

UoDO - Rejestracja zbiorów

- dotyczących osób pozbawionych wolności na podstawie ustawy,
  - w zakresie niezbędnym do wykonania tymczasowego aresztowania lub
  - kary pozbawienia wolności,
- przetwarzanych wyłącznie w celu wystawienia faktury, rachunku lub
  - prowadzenia sprawozdawczości finansowej,
- powszechnie dostępnych,
- przetwarzanych w celu przygotowania rozprawy wymaganej do
  - uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,
- przetwarzanych w zakresie drobnych
  - bieżących spraw życia codziennego.

UoDO – dopuszczenie do przetwarzania danych - Art. 46.

- Administrator danych (niewrażliwych) może
  - rozpocząć ich przetwarzanie
  - w zbiorze danych po zgłoszeniu tego zbioru do GIODO.
- Administrator danych wrażliwych może
  - rozpocząć ich przetwarzanie w zbiorze danych
  - po zarejestrowaniu
    - (otrzymuje informację o rejestracji) zbioru.

UoDO - Prawa osób, których dane są przetwarzane

- Do uzyskania informacji o swoich prawach.
- Do kontroli przetwarzania danych, które jej dotyczą,
  - zawartych w zbiorach danych, czyli
  - uzyskania wyczerpującej informacji
    - (oraz podania w powszechnie zrozumiałej formie treści):
    - celu, zakresie i sposobie przetwarzania
    - danych zawartych w takim zbiorze,
    - 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,
    - od kiedy przetwarza się w zbiorze dane jej dotyczące,

UoDO - Prawa osób

- źródle, z którego pochodzą dane jej dotyczące,
  - chyba że administrator danych jest zobowiązany do zachowania w tym
  - zakresie tajemnicy państwowej, służbowej lub zawodowej,
- sposobie udostępniania danych, a w szczególności informacji o
  - odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
- 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,

UoDO - Prawa osób

- wniesienia pisemnego, umotywowanego żądania zaprzestania
  - przetwarzania jej danych ze względu na jej szczególną sytuację,
- wniesienia sprzeciwu wobec przetwarzania jej danych
  - w przypadkach, gdy administrator danych zamierza je
  - w celach marketingowych lub wobec
  - przekazywania jej danych osobowych innemu
  - administratorowi danych,

❑ Osoba zainteresowana może skorzystać z prawa do

- informacji nie częściej niż raz na 6 miesięcy.

UoDO - Obowiązki administratorów danych osobowych

❑ W przypadku zbierania danych osobowych od osoby,

- której one dotyczą

❑ Administrator danych jest obowiązany poinformować tę osobę o:

- adresie swojej siedziby i pełnej nazwie
  - (lub miejscu swojego zamieszkania oraz imieniu i nazwisku)
- celu zbierania danych, a w szczególności o znanych mu
  - w czasie udzielania informacji lub przewidywanych odbiorcach lub
  - kategoriach odbiorców danych,
- prawie dostępu do treści swoich danych oraz ich poprawiania,
  - dobrowolności albo obowiązku podania danych, a
- jeżeli taki obowiązek istnieje, jego podstawie prawnej,
  - chyba, że przepis innej ustawy zezwala na przetwarzanie danych bez
  - ujawniania faktycznego celu ich zbierania lub osoba, której
  - dane dotyczą, posiada te informacje.

UoDO - Obowiązki administratorów danych osobowych, cd.

❑ W przypadku zbierania danych osobowych

- nie od osoby, której one dotyczą

❑ Administrator danych bezpośrednio po utrwaleniu

- zebranych danych jest
- obowiązany poinformować tę osobę dodatkowo o źródle danych oraz
- o przysługujących jej prawach.

❑ Po zakwestionowaniu przetwarzania danych przez osobę, której dane dotyczą:

- Administrator danych zaprzestaje przetwarzania kwestionowanych
  - danych osobowych albo
- bez zbędnej zwłoki przekazuje żądanie
  - Generalnemu Inspektorowi, który wydaje stosowną decyzję.

UoDO - Obowiązki administratorów danych osobowych, cd.

❑ W razie wniesienia sprzeciwu 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.

❑ Wydawanie upoważnień do przetwarzania danych osobowych

❑ Do przetwarzania danych mogą być dopuszczone

- wyłącznie osoby posiadające upoważnienie
- nadane przez administratora danych.

UoDO - Obowiązki administratorów danych osobowych, cd.

- Administrator danych jest obowiązany
  - zapewnić kontrolę nad tym, jakie dane osobowe,
  - Kiedy i przez kogo zostały do zbioru
    - wprowadzone oraz komu są przekazywane.
- Administrator danych prowadzi
  - ewidencję osób upoważnionych do ich
    - przetwarzania,która powinna zawierać:
  - imię i nazwisko osoby upoważnionej,

UoDO – Obowiązki administratora

  - datę nadania i ustania oraz
    - zakres upoważnienia do przetwarzania danych osobowych,
  - identyfikator, jeżeli dane są przetwarzane w
    - systemie informatycznym.
- Osoby, które zostały upoważnione
  - do przetwarzania danych, są obowiązane zachować
  - w tajemnicy te dane osobowe oraz
  - sposoby ich zabezpieczenia.

UoDO – Udostępnianie danych osobowych

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

UoDO – Udostępnianie danych osobowych

  - 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.

UoDO – Powierzanie przetwarzania danych osobowych

- **Art. 31.**
  - **1.Administrator danych może powierzyć**
    - **innemu podmiotowi, w drodze umowy zawartej na piśmie,**
      - przetwarzanie danych.
  - **2.Podmiot ten może przetwarzać dane wyłącznie w zakresie i**
    - **celu przewidzianym w umowie.**
  - **3.Podmiot ten jest obowiązany przed rozpoczęciem**
    - **przetwarzania danych podjąć wymagane**
      - środki zabezpieczające zbiór danych oraz
    - **spełnić wymagania określone w Rozporządzeniu MSWiA.**
    - **Nie musi natomiast zgłaszać zbioru do rejestracji!!!!**

UoDO – Udostępnianie danych osobowych

- **4.W zakresie przestrzegania tych przepisów podmiot**
  - **ponosi odpowiedzialność jak administrator danych.**
- **5.Odpowiedzialność za przestrzeganie przepisów ustawy spoczywa na administratorze danych,**
  - **co nie wyłącza odpowiedzialności podmiotu, który**
  - **zawarł umowę, za przetwarzanie danych**
  - **niezgodnie z tą umową.**

UoDO - Odpowiedzialność karna i finansowa

- **Art. 49. Przetwarzanie**
  - **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.**
  - **Jeśli dotyczy to danych wrażliwych,**
    - **sprawca podlega grzywnie, karze ograniczenia wolności albo**
    - **pozbawienia wolności do lat 3.**

Art. 50. Niewłaściwe administrowanie

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

UoDO - Odpowiedzialność karna i finansowa

- **Art. 51. Niewłaściwe udostępnianie**
  - **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.**
  - **Jeżeli sprawca działa nieumyślnie, podlega grzywnie,**
    - **karze ograniczenia wolności albo pozbawienia wolności do roku.**
- **Art. 52. Niewłaściwe zabezpieczanie**
  - **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.**

UoDO - Odpowiedzialność karna i finansowa

- **Art. 53. Brak rejestracji**
  - **Kto będąc do tego obowiązany nie zgłasza do**
    - **rejestracji zbioru danych, podlega grzywnie,**
    - **karze ograniczenia wolności albo pozbawienia wolności do roku.**
- **Art. 54. Niewłaściwe informowanie osób**
  - **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.**

1. Ochrona przetwarzania danych osobowych – Rozporządzenie MSWiA

- **Polityka bezpieczeństwa**
  - **wykaz budynków, pomieszczeń lub części pomieszczeń,**
    - **tworzących obszar, w którym przetwarzane są dane osobowe;**
  - **wykaz zbiorów danych osobowych wraz**
    - **ze wskazaniem programów zastosowanych do**
    - **przetwarzania tych danych;**
  - **opis struktury zbiorów danych wskazujący**
    - **zawartość poszczególnych pól informacyjnych i**
      - powiązania między nimi;
  - **sposób przepływu danych pomiędzy poszczególnymi systemami;**
  - **określenie środków technicznych i organizacyjnych**
    - **niezbędnych dla zapewnienia poufności, integralności i**
    - **rozliczalności przetwarzanych danych.**

Ochrona przetwarzania danych osobowych – Rozporządzenie MSWiA

- **Instrukcja zarządzania systemem informatycznym**
- **służącym do przetwarzania danych osobowych**
  - **procedury nadawania uprawnień do przetwarzania danych**
    - **i rejestrowania tych uprawnień w systemie informatycznym oraz**
    - **wskazanie osoby odpowiedzialnej za te czynności;**
  - **stosowane metody i środki uwierzytelnienia oraz**
    - **procedury związane z ich zarządzaniem i użytkowaniem;**
  - **procedury rozpoczęcia, zawieszenia i zakończenia pracy**
    - **przeznaczone dla użytkowników systemu;**
  - **procedury tworzenia kopii zapasowych zbiorów danych oraz**
    - **programów i narzędzi programowych służących do ich przetwarzania;**

Rozporządzenie MSWiA (RoDO)

- **sposób, miejsce i okres przechowywania:**
  - **elektronicznych nośników informacji**
    - zawierających dane osobowe,
  - **kopii zapasowych,**
- **sposób zabezpieczenia systemu informatycznego**
  - **przed działalnością niebezpiecznego oprogramowania;**
- **sposób realizacji wymogów, dotyczących szczególnych**
  - **informacji o przetwarzaniu**
- **procedury wykonywania przeglądów i konserwacji systemów oraz**
  - **nośników informacji służących do przetwarzania danych.**

Ochrona przetwarzania danych osobowych – Rozporządzenie MSWiA

- **Uwzględniając kategorie przetwarzanych danych**
  - **oraz zagrożenia wprowadza się**
- **poziomy bezpieczeństwa przetwarzania danych**
- **osobowych w systemie informatycznym:**
  - **1) podstawowy;**
  - **2) podwyższony;**
  - **3) wysoki.**

Ochrona przetwarzania danych osobowych – Rozporządzenie MSWiA

- **Poziom podstawowy**
  - **Warunki: nie przetwarza się danych wrażliwych, żadne z**
    - **urządzeń systemu informatycznego,**
      - służącego do przetwarzania danych osobowych
      - nie jest połączone z siecią publiczną
  - **Wymagania: Środki bezpieczeństwa na**
  - **poziomie podstawowym – Załącznik A**

Ochrona przetwarzania danych osobowych – Rozporządzenie MSWiA

- **Poziom podwyższony**
  - **Warunki: w systemie informatycznym przetwarzane są**
    - **dane osobowe wrażliwe,**
    - **żadne z urządzeń systemu informatycznego,**
    - **służącego do przetwarzania danych osobowych**
    - **nie jest połączone z siecią publiczną**
  - **Wymagania: Środki bezpieczeństwa**
    - **na poziomie podwyższonym – Załącznik B**

Ochrona przetwarzania danych osobowych – Rozporządzenie MSWiA

- **Poziom wysoki**
  - **Warunki: przynajmniej**
    - **jedno urządzenie systemu informatycznego,**
    - **służącego do przetwarzania danych osobowych,**
      - połączone jest z siecią publiczną
  - **Wymagania: Środki bezpieczeństwa**
    - **na poziomie wysokim – Załącznik C**

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

- **A. Środki bezpieczeństwa na poziomie podstawowym**

- I
- 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.
- 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:
  - w systemie tym rejestrowany był dla każdego użytkownika
    - odrębny identyfikator;
  - dostęp do danych był możliwy wyłącznie
    - po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

- System informatyczny służący do przetwarzania
- danych osobowych zabezpiecza się, w szczególności przed:
  - 1) działaniem oprogramowania, którego
    - **celem jest uzyskanie nieuprawnionego dostępu**
    - **do systemu informatycznego;**
  - 2) utratą danych spowodowaną awarią zasilania lub
    - **zakłóceniami w sieci zasilającej.**

IV

- 1. Identyfikator użytkownika, który
  - utracił uprawnienia do przetwarzania danych,
  - nie może być przydzielony innej osobie.
- 2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła,
  - jego zmiana następuje nie rzadziej niż co 30 dni.
  - Hasło składa się co najmniej z 6 znaków.
- 3. Dane osobowe przetwarzane w systemie informatycznym
  - zabezpiecza się przez wykonywanie kopii zapasowych
  - zbiorów danych oraz programów służących do przetwarzania danych.
- 4. Kopie zapasowe:
  - a) przechowuje się w miejscach zabezpieczających je przed
    - nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
  - b) usuwa się niezwłocznie po ustaniu ich użyteczności.

V

- Osoba użytkująca komputer przenośny
  - zawierający dane osobowe zachowuje
  - szczególną ostrożność podczas jego
  - transportu, przechowywania i użytkowania poza obszarem,
    - o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje
    - środki ochrony kryptograficznej wobec
    - przetwarzanych danych osobowych.

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
    - o z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
  - przekazywane poza obszar,
    - o o którym mowa w § 4 pkt 1 rozporządzenia,
    - o zabezpiecza się w sposób zapewniający
      - **poufność i integralność tych danych.**

X

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

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.