

Ochrona danych osobowych w szkole wyższej

Beata Konieczna
beata_konieczna@wp.pl

UKSW, dnia 9 marca 2009 r.

1

Agenda cz. 1

- **Podstawy prawne ochrony danych osobowych**
- **Podstawowe pojęcia i definicje dotyczące ochrony danych osobowych**
- **Zasady przetwarzania danych osobowych w szkole wyższej**

2

Agenda cz. 2

- **Podmioty odpowiedzialne za przetwarzanie i ochronę danych osobowych w szkole wyższej**
- **Zasady udostępniania danych osobowych**
- **Prawa osób, których dane dotyczą**

3

Agenda cz. 3

- **Zabezpieczanie danych osobowych w szkole wyższej**
- **Odpowiedzialność dyscyplinarna i karna za naruszenie przepisów o ochronie danych osobowych**

4

Dlaczego to szkolenie jest ważne? Bo odpowie m.in. pytania:

- Dlaczego znajomość wiedzy z zakresu ochrony danych osobowych nam nie zaszkodzi, ale wręcz pomoże?
- Jakie obowiązki wiążą się z przetwarzaniem danych osobowych?
- Z czym muszę się liczyć, jeżeli nie będę przestrzegać zasad przetwarzania i ochrony danych osobowych?

5

Odpowiedzialność karna

- 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.

6

Odpowiedzialność karna

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**

7

Odpowiedzialność karna

Art. 49.2 – przetwarzanie danych wrażliwych
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**

8

Odpowiedzialność karna

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.

Naruszenie obowiązku szczególnej staranności

9

Odpowiedzialność karna

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.

Naruszenie obowiązku informacyjnego

10

Odpowiedzialność karna

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.

Naruszenie obowiązku związanego z udostępnianiem danych osobowych

11

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (spros. Dz. U. z 2001, Nr 28, poz. 319)

Art. 47

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

12

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (spros. Dz. U. z 2001, Nr 28, poz. 319)

Art. 51.1

Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jej osoby.

Art. 51. 2. *Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.*

Art. 51. 3. *Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.*

Art. 51. 4. *Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.*

13

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, która reguluje zagadnienia ochrony i przetwarzania danych osobowych.

14

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004, Nr 100, poz. 1024);

15

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. Nr 229, poz. 1536)

16

Kto musi stosować ustawę o ochronie danych osobowych:

- organy państwowe, organy samorządu terytorialnego oraz państwowe i komunalne jednostki organizacyjne podmiotów niepublicznych realizujących 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, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej.
- państwo trzecie – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego

17

Kto jest zwolniony z obowiązku stosowania ustawy?

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.
- 3) 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.) oraz do działalności literackiej lub artystycznej, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą.

18

Jakich danych nie dotyczy ustawa o ochronie danych osobowych?

- Działaniem ustawy objęte są tylko przypadki przetwarzania danych **osób fizycznych**.
- Nie ma podstaw do stosowania, nawet *per analogiam*, przepisów ustawy do przetwarzania danych odnoszących się wyłącznie do:
- osób prawnych

19

Jakich danych nie dotyczy ustawa o ochronie danych osobowych?

- Jednostek organizacyjnych nieposiadających osobowości prawnej
- np. klubów, stowarzyszeń, grup nieformalnych
- Dane dotyczące rodów czy rodzin (przykład: "pierwsze wzmianki o rodzinie X pochodzą z XVIII wieku,,")

20

Pytanie?

- Czy ochrona danych osobowych ma odnosić się tylko do osób żywych czy też rozciągać się na **osoby zmarłe**?

21

- Ustawa polska nie rozstrzyga tej kwestii wprost.
- Niemniej zarówno fakt, że pojęcie "osoba fizyczna" stosowane jest w prawie w odniesieniu do osób żywych, jak i treść większości przepisów ustawy wskazuje na to, iż poza zakresem stosowania ustawy pozostają dane o określonych osobach nieżyjących.

22

Reasumując:

- Ograniczenia w przetwarzaniu takich danych występują ze względu na ochronę powszechnych dóbr osobistych (kult pamięci osoby zmarłej) oraz - na gruncie komentowanej ustawy - wtedy, gdy dane dotyczące zmarłego należy równocześnie traktować jako dotyczące określonej żyjącej osoby

23

Zdaniem GIODO:

- Generalny Inspektor Ochrony Danych Osobowych w piśmie z dnia 12 lutego 2001 r. (znak GI-DP-024/145/01/427) uznał, że regulacja ustawy o ochronie danych osobowych **dotyczy wyłącznie osób żyjących**, a w związku z tym nie stawia ona żadnych przeszkód zarówno w uzyskiwaniu informacji, jak i publikowaniu biografii dotyczących osób zmarłych.
- Rozpowszechnianie informacji dotyczących zmarłych poddane jest natomiast tym ograniczeniom, które mają swe źródło w powszechnej ochronie dóbr osobistych w ramach dobra osobistego określanego jako "kult pamięci osoby zmarłej"

24

Ochrona danych osobowych w szkole wyższej:

■ USTAWA

z dnia 27 lipca 2005 r.

Prawo o szkolnictwie wyższym

Dz. U. z dnia 30 sierpnia 2005 r. ze zm.

25

Ochrona danych osobowych w szkole wyższej m.in:

- Z punktu widzenia „dziekanatów”:
- Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 2 listopada 2006 r. w sprawie dokumentacji przebiegu studiów - Dz. U. z dnia 8 grudnia 2006 r.
- Z punktu widzenia „kadr”:
- Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobem prowadzenia akt osobowych pracowników – Dz. U. nr 62, poz. 286 ze zm.

26

Zastosowanie ustawy o ochronie danych osobowych w szkołach wyższych:

- Ustawa ma zastosowanie do wszystkich osób zatrudnionych (pracowników i osób pozostających w niepracowniczym zatrudnieniu).
- Podmiot zatrudniający, przetwarzający dane osobowe tych osób: w aktach osobowych, różnego rodzaju wykazach, skorowidzach lub w systemach informatycznych - staje się administratorem tych danych – stosownie do art. 7 ust. 4 ustawy.
- Administrator danych jest zwolniony z obowiązku z obowiązku rejestracji zbiorów danych dotyczących osób u niego zatrudnionych, świadczących mu usługi na podstawie umów cywilnoprawnych, a także dotyczących osób u niego zrzeszonych lub uczących się (art. 43 ust. 1 pkt. 4 ustawy)

27

POJĘCIA

I

DEFINICJE

DOTYCZĄCE

OCHRONY DANYCH OSOBOWYCH

28

DANE OSOBOWE

- **wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.**
- **PYTANIA:**
- **Jak rozumieć zwrot „wszelkie informacje”?**
- **Jak rozumieć zwrot „osoba możliwa do zidentyfikowania”?**
- **W jakich sytuacjach informacja o osobie fizycznej nie będzie daną osobową w rozumieniu art.6?**

29

DANE OSOBOWE

- Użycie zwrotu "wszelkie informacje" służy podkreśleniu, iż w grę wchodzi informacje odnoszące się do każdego aspektu osoby, jej stosunków osobistych i rzeczowych, jej życia zawodowego, prywatnego, wykształcenia, wiedzy czy cech charakteru. Nie ma znaczenia, w jakiej roli występuje w danym przypadku osoba (np. członek rodziny, członek grupy zawodowej czy przedsiębiorcy).
- Danymi osobowymi są zarówno informacje już rozpowszechnione lub opublikowane (zamieszczone w publikowanych materiałach), jak i w ogóle jeszcze nieujawnione.

30

DANE OSOBOWE

- "Informacja" rozumiana jako pewna wiadomość o osobie fizycznej zapisana w każdej postaci, tj. w postaci papierowej, elektronicznej, słownej, dźwiękowej, która jest zbierana w trakcie przetwarzania danych.

S. Booth, R. Jenkins, D. Moxon, N. Sellmens, C. Spencer, M. Taylor, D. Townsend, *What is "Personal Data"? A study conducted for the UK Information Commissioner*, Sheffield 2004, s. 35

31

DANE OSOBOWE

Osoba możliwa do zidentyfikowania

- **której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na:**
- **numer identyfikacyjny,**
- **jedną lub kilka specyficznych czynników określających jej cechy:**
- **fizyczne,**
- **fizjologiczne,**
- **umysłowe,**
- **ekonomiczne,**
- **kulturowe lub**
- **społeczne.**

32

Kiedy „zwykłe dane” mogą stać się „osobowymi”?

- Czy numer rejestracyjny samochodu może być daną osobową?
- Czy numer ubezpieczenia społecznego może być daną osobową?

33

GIODO

- ... dla pracownika wydziału komunikacji urzędu gminy możliwe będzie ustalenie tożsamości osoby fizycznej na podstawie numeru rejestracyjnego pojazdu, a dla pracownika Zakładu Ubezpieczeń Społecznych możliwe będzie ustalenie tożsamości osoby fizycznej na podstawie numeru ubezpieczenia.
- Dlatego też bardzo istotny jest kontekst, w jakim dane osobowe są pobierane i przetwarzane

34

Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli:

- Wymagałoby to nadmiernych kosztów,
- Wymagałoby to nadmiernego czasu
- Wymagałoby to nadmiernych działań

*

35

Kiedy dane „zwykłe” mogą stać się „danymi osobowymi”?

- Informacje zatem, które bez nadzwyczajnego wysiłku, bez nieproporcjonalnie dużych nakładów dają się "powiązać" z określoną osobą, zwłaszcza przy wykorzystaniu łatwo osiągalnych źródeł powszechnie dostępnych, zasługują na zaliczenie ich do kategorii danych osobowych

36

Dane osobowe osoby fizycznej

- Zasadniczo ustawa reguluje ochronę danych osobowych jednej osoby, ale:
- Wyjątkowo danymi osobowymi będą **informacje dotyczące więcej niż jednej osoby** (dane o "podwójnym odniesieniu"), na przykład informacje o połączeniach (rozmowach) telefonicznych, o zatrudnieniu osoby A u osoby B, o korzystaniu osoby X z pomocy medycznej lekarza Y

37

Kiedy dane „zwykłe” mogą stać się „danymi osobowymi”?

- Dane osobowe mogą być niekiedy wyprowadzone z "informacji zbiorczych" (np. z informacji: "wszyscy pracownicy firmy X zarabiają powyżej 3000 zł miesięcznie");
- w tym też nawet z takich, które *prima facie* mają anonimowy charakter (jak np. z informacji: "10 absolwentów, którzy ukończyli wydział X w roku Y, pracuje w zakładzie Z", jeżeli w tym roku wydział ten ukończyło tylko 10 osób).

38

DANE OSOBOWE np.

- Informacje o „niezależnych okolicznościach”: imię, nazwisko, płeć, wzrost, znaki szczególne, obywatelstwo, linie papilarne, miejsce zamieszkania, data urodzenia, cechy dokumentów tożsamości, PESEL,
- Informacje o cechach nabytych: wykształcenie, znajomość języków, posiadane uprawnienia, charakter pisma, stan cywilny
- Informacje o cechach osobowościowych, psychologicznych: o przekonaniach, zainteresowaniach, światopoglądach, upodobaniach, sposobie spędzania wolnego czasu,
- Informacje o sytuacji majątkowej, operacjach finansowych (np. lista zaległości czynszowych)
- Informacje o najróżniejszych przejawach działalności (o podróżach, życiu kulturalnym),
- Informacje dotyczące biernego lub czynnego uczestnictwa w różnego rodzaju wydarzeniach,
- Informacje o przebytych chorobach, o kalectwie, o wynikach badań medycznych,

39

DANE OSOBOWE „ZWYKŁE”

DANE OSOBOWE

DANE OSOBOWE „WRAŻLIWE”

40

DANE WRAŻLIWE

- Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową
- Dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym
- Dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

41

Ćwiczenie

- *Przed rozpoczęciem semestru każdy ze studentów miał możliwość zapisania się, poprzez indywidualne konto internetowe, na przedmiot do wyboru. Czas zapisów był określony. Odkryło się to jeszcze we wrześniu 2008 r. Teraz mamy rok 2009, a przed dziekanatem naszego wydziału zostały wywieszone tablice z prawnie chronionymi danymi, związane właśnie z przypisaniem osób do wybranego przedmiotu. Umieszczono na nich imiona, nazwiska, nr indeksów studentów studiów zaocznych. Uważam, że takie postępowanie jest niezgodne z przepisami „Ustawy o ochronie danych osobowych*

42

Można byłoby powiedzieć, iż:

- Charakteryzując warunek, jakim jest możliwość określenia tożsamości osoby, zaznaczamy od razu, że podanie nazwiska, a nawet imienia i nazwiska osoby, nie zawsze jest okolicznością pozwalającą stwierdzić, iż wymóg ten jest spełniony. Dotyczy to zwłaszcza popularnych imion i nazwisk".

43

Ponadto:

- Naczelny Sąd Administracyjny, stwierdził, że **przetwarzanie danych jest dopuszczalne, jeśli jest niezbędne do realizacji obowiązku wynikającego z przepisu prawa.**
- A na władzach Wydziału, zgodnie z zapisami ustawy Prawo o szkolnictwie wyższym, ciąży obowiązek właściwego zorganizowania toku studiów:
- *Dlatego studenci powinni mieć dostęp do informacji, ułatwiających im studiowanie. Klasyczny sposób ogłaszania niektórych informacji wynika z faktu, że nie wszyscy studenci mają dostęp do internetu, dlatego pozbawieni byłiby możliwości uzyskania informacji o przynależności do odpowiedniej grupy. Podkreślę, że nie publikowano żadnych wrażliwych danych, które by mogły naruszać godność i dobre imię studenta*

44

Jednakże zdaniem GODO

- Wystarczyło podać nr albumu, bo nazwisko i przynależność do uczelni to już dużo informacji - łatwo zidentyfikować taką osobę.
- Należałoby całą sytuację zbadać, aby sprawdzić, czy nie było innych możliwości poinformowania studentów

45

ZBIÓR DANYCH OSOBOWYCH

- **Każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie."**

46

ZBIÓR DANYCH OSOBOWYCH

- Uporządkowanie (struktura) zbioru może odnosić się albo do indywidualnych osób (oznaczonych nazwiskiem, numerem identyfikacyjnym)

Nr indeksu	Nazwisko	Imię
3456	Kowalski	Jan
2345	Nowak	Anna
4567	Tytka	Paweł
9876	Kwiatek	Piotr
6789	Opel	Izabela
4567	Dudek	Marta

Nazwisko	Imię	Nr indeksu
Kowalski	Jan	3456
Nowak	Anna	2345
Tytka	Paweł	4567
Kwiatek	Piotr	9876
Opel	Izabela	6789
Dudek	Marta	4567

47

ZBIÓR DANYCH OSOBOWYCH

- albo do oznaczonych kryteriów łączących pewne grupy osób (np. wiek, wykonywana praca, preferencje co do zakupów, prawo do określonych przywilejów, członkostwo w organizacjach).

	Nazwisko	Imię	Nr indeksu
GRUPA 1	Nowak	Paweł	12324
	Kowalski	Jan	23455
	Tytka	Anna	22333
GRUPA 2	Fiat	Izabela	24455
	Ford	Piotr	667778
	Nissan	Tadeusz	34567
	Opel	Hanna	98765
GRUPA 3	Tulipan	Ewa	45123
	Fiolek	Stanisław	09877
	Smerf	Tomasz	34567
	Miś	Róża	12345

48

ZBIÓR DANYCH OSOBOWYCH

- Zbiór musi wykazywać się strukturą **uporządkowaną**. Nie powinien być zatem luźnym zestawem, samą tylko sumą elementów składowych. Jak podkreśla A. Mednis (*Ustawa o ochronie danych osobowych...*), *tym, co odróżnia zbiór danych od innych zestawów danych, jest istnienie cechy albo cech pozwalających na odnalezienie informacji bez potrzeby przeglądania całego zestawu.*

49

ZBIÓR DANYCH OSOBOWYCH

- Cechę zbioru danych stanowić ma - stosownie do ustawowej definicji - **"dostępność (zawartości danych) według określonych kryteriów"**

50

ZBIÓR DANYCH OSOBOWYCH

- Chodzi o kryteria pozwalające na w miarę szybki i bezpośredni dostęp do oznaczonych danych. W grę wchodzi też kryterium alfabetycznego ułożenia nazwisk. Chodzi tu o sytuację, w której po to, aby znaleźć pewne dane, nie jest potrzebne przeglądanie sukcesywnie wszystkich składników zbioru, lecz **posłużyć się można kryteriami selekcyjnymi; można przyjąć, iż "dostępność według określonych kryteriów zapewnia już indeks (skorowidz) alfabetyczny"**.

51

GIODO

zbiór danych osobowych

- Zdaniem GIODO **nie jest istotna ilość oraz rodzaj kryteriów**.
- "wszelkie materiały gromadzone w formie akt, w tym sądowe, prokuratorskie, policyjne i inne zawierające dane osobowe, są zbiorem danych osobowych w rozumieniu art. 7 pkt 1 ustawy". A zauważmy, że rzadko tak się zdarza, aby akta tego rodzaju były układane (wewnętrznie porządkowane) według dwóch różnych kryteriów.

52

ZBIÓR DANYCH OSOBOWYCH

- Zawartość zbioru tworzyć mogą **dane** (informacje) **wyrażone w różny sposób**:
- słowem, dźwiękiem (np. zbiory nagranych wypowiedzi),
- obrazem (np. zbiory zdjęć używane do identyfikacji sprawców przestępstw) itd.

53

ZBIÓR DANYCH OSOBOWYCH

- **Zbiory zautomatyzowane:**
 - Bazy danych,
 - Pliki zawierające dane,
- **Zbiory niezautomatyzowane :**
 - Ręczne zbiory ewidencyjne,
 - Zgromadzone akta (teczki, kartoteki),
 - Formularze, kwestionariusze – uporządkowane i ułożone w odpowiedni sposób (poza regulacją – akta, które nie posiadają żadnego strukturalnego układu danych osobowych),
- Ewidencje gruntów i budynków prowadzonych na podstawie umowy, akta sądowe, prokuratorskie, policyjne

54

Ćwiczenie:

- Czy jako zbiór danych można zakwalifikować zestaw danych, składający się z aplikacji składanych przez przyszłych pracowników (do celów rekrutacji). Aplikacje są przechowywane w systemie informatycznym, przy czym kryterium dostępu do tych informacji jest numer referencyjny bądź nazwa stanowiska, na które dana osoba aplikację złożyła?

55

Rozwiązanie

- Cechą wyróżniającą zbiór danych od innego zestawienia danych jest jego uporządkowany charakter, co zapewnia możliwość wyszukania konkretnych danych za pomocą określonego kryterium. Aby określony zestaw danych zaklasyfikować jako zbiór w rozumieniu przepisów ustawy, wystarczające jest istnienie jednego kryterium wyszukiwawczego w zestawieniu danych.

56

Rozwiązanie

- Administratorowi danych przysługuje dowolność w wyborze rodzaju kryterium dostępu, które w omawianym przypadku może stanowić również numer referencyjny.

57

Rozwiązanie

- Możliwość wyszukania, według kryterium, którym może być numer referencyjny, bądź nazwa stanowiska, na które dana osoba aplikuje, dokumentu zawierającego dane osobowe, przesądza o uporządkowanym charakterze zestawienia danych i tym samym stanowi o zakwalifikowaniu tegoż zestawienia jako zbioru danych w rozumieniu art. 7 pkt 1 ustawy o ochronie danych osobowych.

58

Rozpoznanie zbiorów

- Zbiory danych klientów – osób zewnętrznych
- Zbiory danych pracowników
 - Dane kadrowe – kwestionariusz osobowy, dane do ZUS, US
 - Dane socjalne – kredyty, pożyczki
 - Dane służbowe – dane do kontaktów, zbiór identyfikatorów itp.
- Zbiory kandydatów do pracy
- Zbiory współpracowników – umowy zlecenia
- Zbiory powierzone do przetwarzania przez inne podmioty

59

Przykładowe zbiory na uczelni:

- studentów,
- pracowników,
- osób, z którymi zawierane są umowy cywilnoprawne,
- kontrahentów,
- osób korzystających z Biblioteki Głównej,
- osób spoza Uczelni, które przeprowadzają postępowania o uzyskanie w Uczelni stopnia naukowego doktora lub doktora habilitowanego,
- osób spoza Uczelni, które przeprowadzają w Uczelni postępowanie o nadanie tytułu naukowego profesora,
- uczestników studiów podyplomowych, kursów i szkoleń,
- byłych pracowników Uczelni,
- osób, którym Uczelnia nadała tytuł doktora honoris causa lub inne odznaczenia oraz tytuły honorowe.

60

Proszę pamiętać

- Jeżeli na Uczelni będą tworzone zbiorów danych osobowych innych osób niż wymienione powyżej, zbiory te poddawane są rejestracji zgodnie z rozdziałem 6 ustawy.
Kierownik jednostki organizacyjnej, w której utworzono taki zbiór, zapewnia przetwarzanie danych z tych zbiorów zgodnie z przepisami ustawy.

61

PRZETWARZANIE DANYCH OSOBOWYCH

Wszelkie operacje wykonywane na danych osobowych, takie jak:

- zbieranie,
- utrwalanie,
- przechowywanie,
- opracowywanie,
- zmienianie,
- udostępnianie,
- usuwanie.

- Zwłaszcza - ale nie tylko - te, które wykonuje się w systemach informatycznych.

62

PRZETWARZANIE DANYCH OSOBOWYCH

- a) zbieranie danych (art. 24 i 25)
- b) udostępnianie danych (art. 29 i 30)
- c) usuwanie: zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą = anonimizacja

63

PRZETWARZANIE DANYCH OSOBOWYCH

Przetwarzanie danych może przebiegać
w sposób niezautomatyzowany
albo zautomatyzowany, całkowicie
lub częściowo

64

Jeżeli przetwarzamy dane osobowe – co to oznacza?

- Oznacza to konieczność stosowania regulacji zawartej w omawianej ustawie!

65

Jeżeli przetwarzamy dane osobowe – co to oznacza?

- Przetwarzanie danych osobowych może odbywać się zarówno w systemie informatycznym, jak i w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych

67

Jeżeli przetwarzamy dane osobowe – co to oznacza?

- Przetwarzanie danych osobowych pracowników oraz studentów wyższej uczelni służy realizacji zadań wynikających z art. 13 ust. 1 ustawy Prawo o szkolnictwie wyższym

66

Jeżeli przetwarzamy dane osobowe – co to oznacza?

- W zakresie danych osobowych przetwarzanych w innych systemach niż informatyczne, obowiązują wszystkie przepisy o tajemnicy służbowej, obiegu i zabezpieczeniu dokumentów służbowych

68

Jeżeli przetwarzamy dane osobowe – co to oznacza?

- Pracownicy i studenci oraz inne osoby, których dane są przetwarzane w jednostkach Uczelni mają prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualnienia lub poprawiania jak również do uzyskiwania wszystkich informacji o przysługujących im prawach

69

Jeżeli przetwarzamy dane osobowe – co to oznacza?

- Osoby zatrudnione w Uczelni przetwarzające dane osobowe każdego rodzaju, niezależnie od systemu przetwarzania, są zobowiązane do zachowania tych danych w tajemnicy również po ustaniu zatrudnienia

70

Zgoda osoby, której dane dotyczą

- 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

71

Zgoda osoby, której dane dotyczą

- **zgoda udzielona** może być **nie tylko "osobiście", ale**
- również przez osobę upoważnioną, **przez przedstawiciela.**
- Potrzeba taka pojawić się może na przykład w zakresie zbierania niektórych danych osobowych dotyczących pracowników.
- Mogą oni w tym względzie udzielić upoważnienia organizacjom reprezentującym zatrudnionych.

72

Zgoda osoby, której dane dotyczą

- Jeżeli działanie przedstawiciela mieści się w granicach udzielonego mu upoważnienia, zaś sama zgoda ma charakter wyraźny, wywołuje ona takie same skutki, jak zgoda osoby, której dane są przedmiotem przetwarzania.

73

Zgoda osoby, której dane dotyczą

Komu zgoda powinna być złożona?

Zgoda – oświadczenie woli, należy przyjąć, iż powinno być złożone temu kto decyduje o przetwarzaniu danych osobowych, czyli administratorowi danych.

Ale nic nie stoi jednak na przeszkodzie, aby administrator upoważnił określoną osobę do przyjmowania takich oświadczeń

74

Zgoda osoby, której dane dotyczą

- **Wykluczenie możliwości wyrażenia zgody w sposób domniemany lub dorozumiany** służy istotnemu wzmocnieniu pozycji i ochrony interesów osób, których dane osobowe są przetwarzane

75

Zgoda osoby, której dane dotyczą

- W orzeczeniu z dnia 4 kwietnia 2003 r. (II SA 2135/02, omówienie Mon. Pr. 2003, nr 10, s. 435) Naczelny Sąd Administracyjny podkreślił, że zgoda musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażenia.

76

Zgoda osoby, której dane dotyczą

- Zastrzeżenie, iż zgoda nie może być dorozumiana, nie jest równoznaczne z obowiązkiem wyrażenia zgody w **formie pisemnej**.
- Tego rodzaju "podwyższone" wymaganie odnosi się do przetwarzania szczególnej kategorii danych osobowych - tzw. danych wrażliwych
- Więc można uznać, iż w pozostałych przypadkach dostateczna jest zgoda ustna. Musi być ona jednak wyrażona ze świadomością wynikających z niej tak korzystnych, jak i niekorzystnych konsekwencji.

77

Zgoda osoby, której dane dotyczą

- Zgoda nie powinna mieć charakteru ABSTRAKCYJNEGO – to znaczy, że nie może dotyczyć przetwarzania danych osobowych w ogóle.
- Chodzi zatem o to, by odnosiła się do skonkretyzowanego stanu faktycznego

78

Zgoda osoby, której dane dotyczą

- Zgoda powinna obejmować określone dane oraz sprecyzowany sposób i cel ich przetwarzania.
- Zgoda może mieć bądź charakter bezterminowy, bądź zezwalać na przetwarzanie danych jedynie przez oznaczony okres.

79

Klauzula zgody

- „wyrażam zgodę na przetwarzanie, w tym przekazywanie moich następujących danych osobowych: imienia, nazwiska, daty i miejsca urodzenia, numeru PESEL, adresu zamieszkania, numeru telefonu, w celach marketingu produktów i usług podmiotów powiązanych kapitałowo z ADB Sp. z o.o., tj ABC Investment GmbH z siedzibą w Hamburgu, adres: Leopoldstr. 5, 00-111 Hamburg, Niemcy (...)

80

SYSTEM INFORMATYCZNY

- Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych

81

Zabezpieczanie danych w systemie informatycznym

- To wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem

82

Środki techniczne i organizacyjne zapewniające ochronę danych osobowych

- **Służą zabezpieczeniu danych przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem**
- POLITYKA BEZPIECZEŃSTWA
- INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

83

ODBIORCA DANYCH

każdy, 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 (przedstawiciel administratora z państwa trzeciego),
- d) podmiotu, o którym mowa w art. 31 (podmiot, któremu powierzono przetwarzanie danych),
- e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Zasadniczo dane przekazuje się odbiorcom.

84

Konsekwencją wprowadzenia tych wyłączeń jest wyłączenie obowiązków dotyczących informowania osoby, której dane dotyczą, o podmiotach, którym udostępnianie są dane, jeśli podmioty nie są odbiorcami danych.

- Art. 24 ust. 1 pkt 2
 - *W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o: celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych*
- Art. 25 ust. 1 pkt 2
 - *W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o: celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych*
- Art. 32 ust. 1 pkt 5
 - *Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do: uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane*

85

Konsekwencje wyłączeń:

- Innymi słowy: administrator danych nie musi informować osoby, której dane dotyczą, o udostępnianiu jej danych podmiotom, które nie zostały zaliczone do kategorii odbiorców danych, ani
- odnotowywać faktu udostępnienia danych tym podmiotom.
- Administrator nie ma także obowiązku wskazywania objętych wyłączeniem podmiotów, którym udostępnia dane, w zgłoszeniu zbioru danych osobowych do rejestracji zgodnie z art. 41 ust. 1

86

Ćwiczenie:

- Student wyraził zgodę na umieszczenie jego wyniku na stronie internetowej uczelni. Strona internetowa jest powszechnie dostępna. Czy osoby, które przez przypadek zapoznały się z tą oceną są odbiorcami danych w rozumieniu ustawy o ochronie danych osobowych art. 7 pkt. 6?

87

Za odbiorcę danych uważa się każdego, komu udostępnia się dane osobowe, z wyłączeniem:

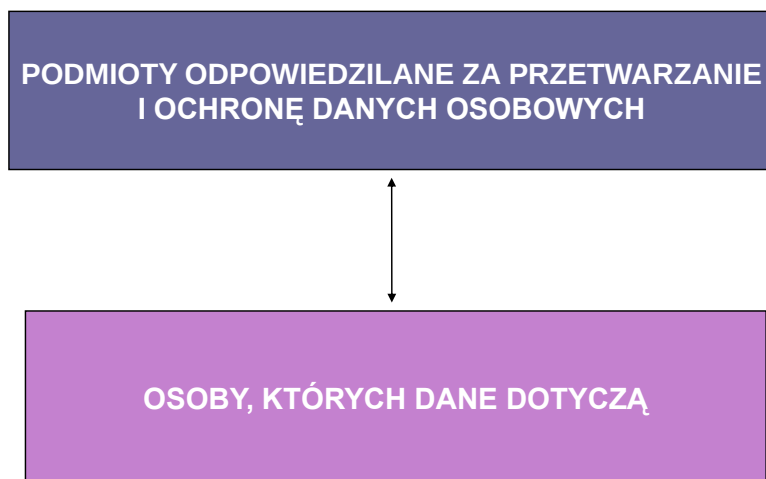
- osoby, której dane dotyczą,
- osoby upoważnionej do przetwarzania danych,
- przedstawiciela, o którym mowa w art. 31a,
- podmiotu, o którym mowa w art. 31,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

88

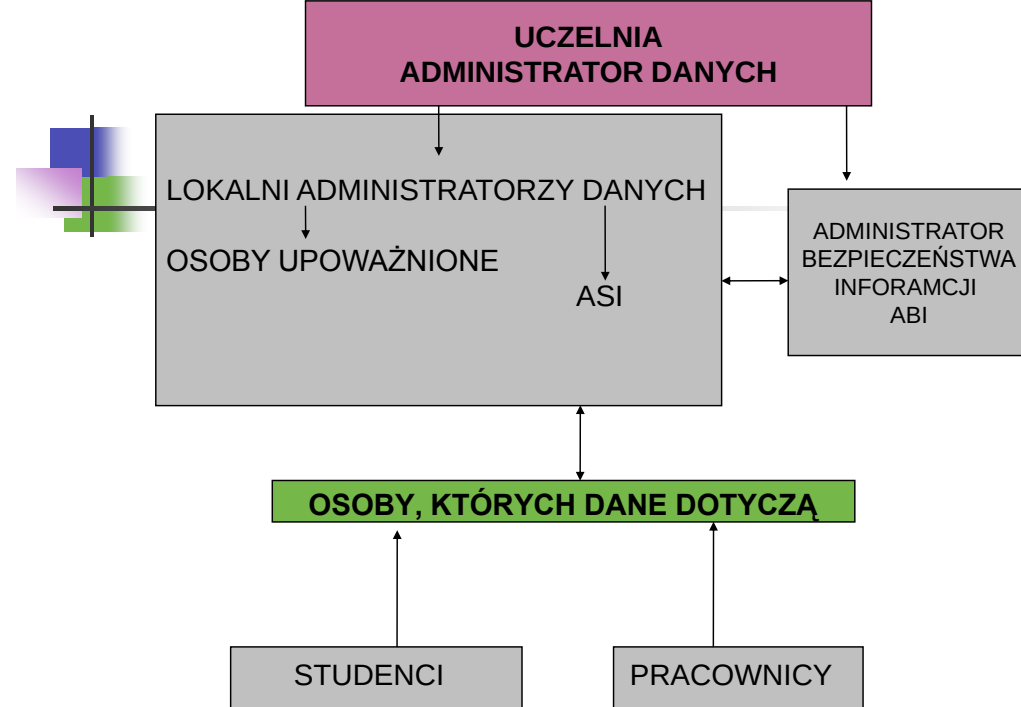
- Z brzmienia przepisu wynika, że odbiorcą jest każda osoba, która otwiera stronę www, na której znajdują się te dane.

89

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH w tym OBOWIĄZKI I PRAWA



90



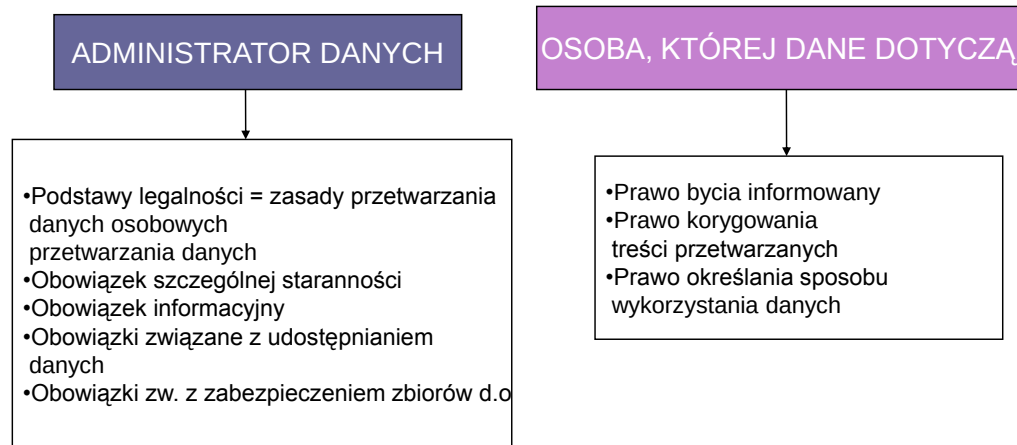
91

„AKTORZY”

- **ADMINISTRATOR DANYCH = UCZELNIA ---- REKTOR**
- **LOKALNI ADMINISTRATORZY DANYCH**
 - prorektor – w zakresie podległych im jednostek organizacyjnych,
 - dziekan – w zakresie pracowników i studentów poszczególnych wydziałów,
 - kanclerz – w zakresie podległych mu jednostek organizacyjnych,
 - kustosz – w zakresie podległych mu jednostek organizacyjnych,
 - dyrektor Biblioteki Głównej – w zakresie zbioru danych osobowych osób korzystających z Biblioteki Głównej Uczelni.
- **ABI** --- podmiot wyznaczony przez Administratora danych
- **OSOBY UPOWAŻNIONE** --- osoby, którym zostało nadane upoważnienie do przetwarzania danych osobowych przez administratora danych/lokalnych administratorów danych
- **ASI** --- administrator systemów informatycznych wyznaczony przez a.d. lub l.a.d.

92

OBOWIĄZKI I PRAWA



93

ADMINISTRATOR DANYCH

- Podstawy legalności = zasady przetwarzania danych osobowych przetwarzania danych**
- Obowiązek szczególnej staranności
- Obowiązek informacyjny
- Obowiązki związane z udostępnianiem danych
- Obowiązki zw. z zabezpieczeniem zbiorów d.o

94

Kiedy można przetwarzać dane?

ZASADY PRZETAWRZANIA DANYCH OSOBOWYCH „ZWYKŁYCH”

oraz

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH „WRAŻLIWYCH”

95

ZASADY PRZETAWRZANIA DANYCH OSOBOWYCH „ZWYKŁYCH”

- Co do zasady prawo przetwarzania danych osobowych opiera się na zgodzie zainteresowanego (art. 23 ust.1 pkt 1), chyba, że na przetwarzanie danych zezwala wyraźny przepis prawa lub zachodzą inne ustawowo określone przesłanki.
- Zgoda musi być oświadczeniem woli, wyraźnym, świadomym, wyrażonym np. w formie pisemnej

96

ZASADY PRZETAWRZANIA DANYCH OSOBWYCH „ZWYKŁYCH”

- Zgoda nie jest wymagana, gdy dochodzi o przetwarzania danych w zbiorach doraźnych – czyli takich, które zostały stworzone **doraźnie , wyłącznie** dla celów technicznych, szkoleniowych oraz dydaktyki w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuniętych/poddanych anonimizacji.

97 Anonimizacja – taka modyfikacja danych osobowych, która nie pozwala na określenie tożsamości osoby

Kiedy można przetwarzać dane zwykłe? Art. 23 ust. 1 ustawy

- osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
- 1. jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- 2. 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,
- 3. jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- 4. jest to niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Kiedy można przetwarzać dane zwykłe?

- Za prawnie usprawiedliwiony cel, o którym mowa w ust. 1 pkt 5, uważa się w szczególności:
 - marketing bezpośredni własnych produktów lub usług administratora danych,
 - dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

99

Przykład

- Czy za usprawiedliwiony cel można uznać przetwarzanie przez podmiot zatrudniający informacji, które są pomocne przy ocenie, czy kandydat na pracownika jest odpowiedni do wykonywania pracy określonego rodzaju?

Odpowiedź

- Tak, jeżeli zatrudnienie jest środkiem do realizacji celów wyznaczonych przez akt założycielski, to za usprawiedliwione należy uznać przetwarzanie przez zatrudniającego wszystkich danych, które wskazują, że ubiegający się o zatrudnienie jest odpowiednim kandydatem na stanowisko pracy określone ze względu na zarobkowe lub zawodowe zadania podmiotu zatrudniającego wynikające z tego aktu.

101

Pamiętać jednak należy:

- **O ocenie wyważenia interesu stron!**
- Z jednej strony: osoby, której dane dotyczą, mającej interes prawny, aby jej dane nie były przetwarzane bez jej zgody,
- Z drugiej strony: interes podmiotu zatrudniającego, którego to interes prawny polega na tym, iż ma on prawo realizować prawnie usprawiedliwione cele i uprawnienia.

102

Kiedy można przetwarzać dane zwykle?

- Zgodnie w tą przesłanką dane osobowe dotyczące zatrudnienia/dotyczące studentów – zatrudniający=administrator danych, **powinien przetwarzać wyłącznie informacje niezbędne do wypełnienia jego prawnie usprawiedliwionych celów, pozostających w związku z jego działalnością zarobkową, zawodową, statutową** – a przetwarzanie danych nie będzie naruszać praw i wolności osoby, której dane dotyczą

103

Kiedy można przetwarzać dane zwykle?

- Zgoda, osoby, której dane dotyczą, może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.
- ZGODA NA PRZYSZŁOŚĆ

104

Przykład

- Zgoda na przetwarzanie danych osobowych może być udzielona tylko konkretnemu podmiotowi np. zatrudniającemu jako administratorowi danych.
- Pytanie: Co jeżeli dochodzi do następstwa prawnego, a dane były przetwarzane na podstawie zgody osoby zatrudnionej, a nie na podstawie innych ustawowych przesłanek?

105

Odpowiedź

- Mianowicie: nowy podmiot zatrudniający jako następca powinien ponownie uzyskać zgodę osoby, której dane dotyczą, chyba że osoba wyraziła zgodę na przetwarzanie danych w przyszłości.

106

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH „WRAŻLIWYCH”

107

Kiedy można przetwarzać „dane wrażliwe”?

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,**

108

Kiedy można przetwarzać „dane wrażliwe”?

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

109

Kiedy można przetwarzać „dane wrażliwe”?

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

110

Kiedy można przetwarzać „dane wrażliwe”?

5. 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

111

Kiedy można przetwarzać „dane wrażliwe”?

6. przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,
7. przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,

112

Kiedy można przetwarzać „dane wrażliwe”?

8. 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

113

Kiedy można przetwarzać „dane wrażliwe”?

9. 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

114

Kiedy można przetwarzać „dane wrażliwe”?

10. 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

115

- Szczególne wątpliwości w tej mierze pojawiają się, gdy chodzi o podstawy prawne oraz zakres dopuszczalności **przetwarzania danych pracowników oraz kandydatów do pracy**

116

Kodeks pracy a uodo

- Z dniem 1 stycznia 2004 r., wprowadzono do kodeksu pracy nowy przepis art. 22¹, który uprawnia pracodawców do żądania od osób ubiegających się o zatrudnienie oraz od pracodawców określonych danych osobowych. W myśl art. 22¹ § 1 k.p.
- **od kandydata do pracy** pracodawca może żądać podania: imienia (imion) i nazwiska; imion rodziców; daty urodzenia; miejsca zamieszkania (adresu do korespondencji); wykształcenia oraz przebiegu dotychczasowego zatrudnienia

117

Kodeks pracy a uodo

- **natomiast od pracownika:**
- Pracodawca może (na podstawie 22¹ § 2 k.p.) domagać się również innych danych osobowych, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, a ponadto numeru ewidencyjnego PESEL

118

Kodeks pracy a uodo

- W art. 22¹ k.p. mowa jedynie o żądaniu przez pracodawcę od kandydata i pracownika podania danych.
- Podstawę uprawniającą do przetwarzania przez pracodawcę danych o pracownikach odnajdujemy w art. 94 pkt 9a k.p., który nakłada na pracodawcę obowiązek prowadzenia dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników. Niedopełnienie tego obowiązku skutkować może odpowiedzialnością w postaci grzywny, zgodnie z art. 281 pkt 6 k.p.

119

Kodeks pracy a uodo

- Zagadnienia dotyczące prowadzenia dokumentacji pracowniczej zostały szczegółowo uregulowane w wydanym na podstawie art. 298¹ k.p. rozporządzeniu Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz. U. Nr 62, poz. 286 z późn. zm.).

120

Kodeks pracy a uodo

- Porównując zakres danych, jakich pracodawca może żądać w oparciu o art. 22 i § 1 k.p., z zakresem określonym w rozporządzeniu należy stwierdzić, iż w dokumentacji osobowej pracowników prowadzonej w oparciu o przepisy art. 94 pkt 9a k.p. oraz przepisy rozporządzenia mieści się znacznie więcej danych osobowych (m.in. zawarte w kwestionariuszu osobowym informacje dotyczące obywatelstwa, numeru NIP, dodatkowych uprawnień, umiejętności i zainteresowań, stosunku do służby wojskowej)

121

- W ramach stosunku pracy, zgodnie z art. 22¹kp pracodawca może żądać od kandydata na pracownika wyłącznie danych innych niż wrażliwe.

122

Zasady przetwarzania danych wrażliwych np. w kadrach:

- Dopuszczalność przetwarzania danych wrażliwych uzależniona jest do łącznego spełnienia dwóch przesłanek:
- 1. dane te są niezbędne do wykonywania zadań odnoszących się do zatrudnienia pracowników i innych osób,
- 2. akt rangi ustawowej powinien określić granice, w jakich przetwarzanie tych danych jest możliwe

123

Kodeks pracy a dane wrażliwe

- Na podstawie art. 22¹par 4 kp, pracodawca może żądać podania innych danych, o ile obowiązek ich podania wynika z odrębnych przepisów:

124

Przykład

- Prawo żądania od kandydata na pracownika, jak również od osoby zatrudnionej **informacji o stanie zdrowia** przewidują pragmatyki pracownicze np.:
- Ustawa z dnia 22 marca 1990 r. o pracownikach samorządowych
- Ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych

125

Przykład

- art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym – pracodawca ma prawo uzyskania danych wrażliwych z KRK w zakresie niezbędnym do zatrudnienia pracownika wyłącznie wtedy, gdy przepisy ustanawiają wymagania kwalifikacyjne **niekaralności**, korzystania z pełni praw publicznych, a także ustalenia uprawnienia do zajmowania określonego stanowiska, wykonywania określonego zawodu lub prowadzenia określonej działalności gospodarczej

126

Przykład

- Dopuszczalne jest przetwarzanie danych wrażliwych jako niezbędne do przyznawania ulgowych usług i świadczeń oraz opłat z zakładowego funduszu świadczeń socjalnych.
- Pracodawca nie narusza dóbr osobistych pracownika zobowiązując go zgodnie z postanowieniami regulaminu przyznawania zapomóg z zakładowego funduszu świadczeń socjalnych do złożenia zaświadczenia o zarobkach uzyskiwanych u drugiego pracodawcy

Wyrok SN z dnia 8 maja 2002 r. I PKN 267/01, OSNAPiUS 2004, nr 6, poz. 99

127

Konkludując:

- Przetwarzanie danych: ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa, 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 - **dopuszczalne jest tylko w związku z realizacją celów statutowych Uczelni i w granicach wynikających z przepisów art. 27 ust. 2 ustawy.**

128

- Jakie dane osobowe są w posiadaniu Uczelni?
- Przykłady ich prawidłowego przetwarzania:

129

Pytanie?

- Czy zatrudnienie na podstawie umowy o dzieło wymaga prowadzenia akt osobowych?

130

- Osoba, z którą zawiera się umowę o dzieło, nie jest pracownikiem.
 - W związku z tym nie jest pracodawcą zobowiązany do prowadzenia akt osobowych takiej osoby.

Zgodnie z art. 94 pkt 9a ustawy z 26 czerwca 1974 r. - Kodeks pracy (Dz.U. z 1998 r. nr 21, poz. 94 ze zm.)
pracodawca ma obowiązek prowadzić dokumentację związaną ze stosunkiem pracy oraz akta osobowe pracowników.

131

Akt osobowych nie ma obowiązku zakładać –
Ale najlepiej trzymać gdzieś osobno komplety dokumentów

- należy zbierać rachunki wystawione przez zleceniodawców, umowy, oświadczenie z danymi osobowymi tzn. czy są na emeryturze, czy są zarejestrowani w PUP, czy są studentami itp.
- zleceniobiorcy muszą mieć szkolenia bhp i zaświadczenia lekarskie, oprócz oświadczeń ds. ZUS i US, które należy mieć

132

- Należy więc, do celów ewentualnej kontroli ze strony urzędu skarbowego, przechowywać zarówno samą umowę, jak i wszelką dokumentację związaną z przekazywaniem zaliczek na podatek dochodowy do urzędu skarbowego, jak również kopie druków PIT przekazywanych do urzędu skarbowego oraz do osoby wykonującej umowę o dzieło.

133

Dane osobowe pracowników

- Przetwarzane są np. w Dziale Kadr i Spraw Socjalnych:
- udostępnia dane przełożonym pracownika oraz właściwym organom Uczelni,
- a także – po zatwierdzeniu rektora lub innej upoważnionej przez niego osoby – innym uprawnionym instytucjom (w szczególności sądom, policji, prokuraturze i organom kontrolującym).
- Dane osobowe pracowników korzystających z Biblioteki – przetwarza Biblioteka Główna.

134

Dane osobowe byłych pracowników

- W okresie do jednego roku po ustaniu stosunku pracy powinny być przetwarzane – w Dziale Kadr i Spraw Socjalnych, a po upływie tego okresu – w Archiwum Uczelni zgodnie z odrębnymi przepisami o działalności archiwalnej (ustawa z dnia 14 lipca 1983 r., Dz. U. Nr 38, poz. 173 ze zmianami).
- Dane osobowe żyjących byłych pracowników są udostępniane organom Uczelni, a także uprawnionym instytucjom na pisemny, umotywowany wniosek, chyba że przepis ustawy stanowi inaczej
- Dane osobowe byłych pracowników mogą być udostępniane także historykom i biografom za zgodą rektora lub innej, upoważnionej przez niego osoby.

135

Dane osobowe byłych pracowników

- **będących emerytami lub rencistami** przetwarzane są w Dziale Kadr i Spraw Socjalnych w celach realizacji uprawnień do korzystania z funduszu socjalnego – na ich imienny wniosek – corocznie, do końca życia

136

Co więcej:

- Dział Kadr i Spraw Socjalnych przetwarza również **dane osobowe dzieci** pozostających na utrzymaniu (do 25. roku życia – jeżeli się uczą) pracowników, oraz byłych pracowników Uczelni będących emerytami lub rencistami, zgodnie z uprawnieniami wynikającymi z regulaminu zakładowego funduszu świadczeń socjalnych

137

Co więcej:

- Dane osobowe dotyczące finansów są przetwarzane w kwesturze
- Dane osobowe dotyczące planowania i rozliczania zajęć dydaktycznych przetwarzane są m.in. w jednostkach, w których realizowane są te zajęcia
- Jednostki organizacyjne Uczelni przetwarzają dane osobowe swych pracowników w zakresie niezbędnym do zapewnienia prawidłowej działalności jednostki.

138

Zasady

Prawo dostępu do akt personalnych ze względu na charakter świadczonej pracy mają pracownicy kadr. Jednak muszą mieć oni imienne upoważnienia uprawniające do wglądu do przechowywanej dokumentacji, wydane przez pracodawcę, jako osobę zarządzającą danymi osobowymi (art. 37 u.o.d.o.). Pracownicy kadr zobowiązani są do zachowania tych informacji w tajemnicy, również po ustaniu zatrudnienia.

139

Zasady

- Upoważnienie do wglądu w dokumentację pracowniczą mogą otrzymać także inne osoby z uwagi na zajmowane przez nie stanowiska, m.in.:
- osoby zarządzające w imieniu pracodawcy zakładem pracy,
 - kierownicy poszczególnych jednostek organizacyjnych - w odniesieniu do danych dotyczących podległych im pracowników,
 - osoby dokonujące przeglądów serwisowych oprogramowania czy też
 - praktykanci, jeżeli wykonują prace związane z przetwarzaniem danych osobowych.

140

Dane osobowe studentów

- W jednostkach organizacyjnych Uczelni prowadzących działalność dydaktyczną przetwarza się dane osobowe studentów w zakresie niezbędnym do zapewnienia prawidłowego toku studiów

141

Dane osobowe studentów

- W jednostkach organizacyjnych Uczelni prowadzących działalność dydaktyczną przetwarza się dane osobowe studentów w zakresie niezbędnym do zapewnienia prawidłowego toku studiów

142

Dane osobowe studentów

- Przetwarzane są przez np. w:
- Dziekanatach poszczególnych wydziałów;
- Dziale Spraw Studenckich,
- Dziale Nauki,
- Kwesturze,
- Bibliotece Głównej.

143

Dane osobowe studentów

- Informacji o danych osobowych studentów udziela się w dziekanacie lub w ww. przykładowych działach, tylko w odpowiedzi na pisemny wniosek organów Uczelni,
- a po zatwierdzeniu dziekana lub kierownika działu, także innym uprawnionym instytucjom (w szczególności sądom, policji, prokuraturze i organom kontrolnym)

144

Dane osobowe studentów

- Wszyscy pracownicy mający dostęp do indeksów i protokołów egzaminacyjnych (w szczególności nauczyciele akademicki oraz personel dziekanatów i działów) są zobowiązani do odpowiedniego zabezpieczenia tych dokumentów przed osobami trzecimi

145

Dane osobowe studentów

- Dziekan wydziału lub inna osoba upoważniona przez ADO Uczelni informuje studentów o przysługujących im prawach „osoby, której dane dotyczą” : prawach do kontroli przetwarzania ich danych osobowych
- - realizacja obowiązku informacyjnego administratora danych osobowych

146

Dane osobowe studentów

- Do słuchaczy studiów podyplomowych i kursów specjalistycznych organizowanych przez Uczelnię
- stosuje się odpowiednio przyjęte zasady przetwarzania danych

147

Dane osobowe kandydatów na studia

- W kwestionariuszu-podaniu, składanym przez kandydata ubiegającego się o przyjęcie na studia umieszcza się informację o celu zbierania danych osobowych i o ich późniejszym przetwarzaniu,
- o sposobie podaniu wyników rekrutacji np. w postaci umieszczenia numeru PESEL na liście zawierającej wyniki rekrutacji.

148

Dane osobowe kandydatów na studia

- Kandydat podpisuje odpowiednie oświadczenie zawierające jego zgodę na przetwarzanie w Uczelni jego danych osobowych w zakresie niezbędnym do realizacji toku studiów oraz w celu wydania legitymacji studenckiej /elektronicznej legitymacji studenckiej

149

Dane osobowe kandydatów na studia

- Informację o prawach osoby, której dane dotyczą – zgodnie z rozdziałem 4 ustawy – można np. wywiesić w widocznym miejscu na tablicach informacyjnych dotyczących rekrutacji.

150

Dane osobowe kandydatów na studia

- Wyniki rekrutacji ogłasza się na listach zawierających numery PESEL kandydatów.
- W Polityce bezpieczeństwa można wskazać sposób udzielania informacji telefonicznej lub pocztą mailową o wynikach rekrutacji np.
- po podaniu nazwiska i numeru PESEL kandydata

151

Dane osobowe kandydatów na studia

- Dane osobowe kandydatów na studia, **którzy nie zostali przyjęci**,
 - **usuwa się** po zakończeniu procesu rekrutacji, a pozostałe przekazuje się do bazy danych systemu dziekanatowego

152

Dane osobowe absolwentów

- Czasowe określenie przetwarzania danych absolwentów, a po upływie tego okresu przekazane do Archiwum, w którym są przetwarzane zgodnie z przepisami o działalności archiwalnej (ustawa z dnia 14 lipca 1983 r., Dz. U. Nr 38, poz. 173 ze zmianami).
- Zasada ma zastosowanie do danych osobowych słuchaczy studiów podyplomowych, kursów lub szkoleń przetwarzane w jednostkach organizacyjnych Uczelni prowadzących działalność dydaktyczną

153

Dane osobowe absolwentów

- W jednostkach organizacyjnych Uczelni prowadzących działalność dydaktyczną mogą być przechowywane wykazy wyników nauczania studentów.
- Studenci są tutaj identyfikowani jedynie imieniem, nazwiskiem i numerem albumu

154

Dane osobowe absolwentów

- Zasady mają zastosowanie odpowiednio do osób, które przerwały studia, kursy lub szkolenia przed uzyskaniem dyplomu lub zaświadczenia o ukończeniu studiów (kursów, szkoleń).

155

ADMINISTRATOR DANYCH

- Podstawy legalności = zasady przetwarzania danych osobowych przetwarzania danych
- **Obowiązek szczególnej staranności**
- Obowiązek informacyjny
- Obowiązki związane z udostępnianiem danych
- Obowiązki zw. z zabezpieczeniem zbiorów d.o

156

Obowiązek szczególnej staranności

- - **legalności (pkt 1),**
- - **celowości (pkt 2),**
- - **merytorycznej poprawności (pkt 3),**
- - **adekwatności (pkt 3) oraz**
- - **ograniczenia czasowego (pkt 4).**

157

Zasada adekwatności

- Swym rodzajem i swą treścią dane nie powinny wykraczać poza potrzeby wynikające z celu ich zbierania.
- Omawiany wymóg sprzeciwia się też zbieraniu wszelkich danych dla tego celu nieistotnych, niemających znaczenia, jak i danych o "większym - niż uzasadniony z tego względu - stopniu szczegółowości".

158

Zasada adekwatności

- W ocenie Generalnego Inspektora Ochrony Danych Osobowych żądanie od osoby przystępującej do ubezpieczenia grupowego takich informacji, jak rodzaj wykonywanej pracy, wykształcenie czy stan cywilny narusza zasadę adekwatności, wykracza poza potrzeby związane z zawarciem i realizacją umowy ubezpieczenia.

E. Kulesza, *Ankieta, która budzi poważne wątpliwości*, Rzeczpospolita z 3 listopada 1999

159

Zasada adekwatności

- W ubezpieczeniach grupowych nie prowadzi się oceny ryzyka ubezpieczeniowego, a ubezpieczający się nie podaje przed zawarciem umowy informacji o swoim stanie zdrowia; nie zachodzi więc nawet ewentualna konieczność weryfikacji informacji udzielanych przez ubezpieczonego.

E. Kulesza, *Ankieta, która budzi poważne wątpliwości*, Rzeczpospolita z 3 listopada 1999

160

Zasada adekwatności

- Z nadmiernym, nieuzasadnionym zbieraniem danych osobowych zetknąć się można - zdaniem Generalnego Inspektora - **na przykład w działalności bibliotek**; trudno usprawiedliwić zbieranie przez nie takich danych, jak miejsce pracy, imię ojca, numer dowodu osobistego.
- Z podobnych powodów zakwestionowane zostało szerokie zbieranie danych osobowych ponad uzasadnione potrzeby związane ze świadczeniem usług przez agentów funduszy emerytalnych i przez firmy ubezpieczeniowe od osób ubezpieczających się na życie.

161

Zasada adekwatności

- Z naruszeniem zasady adekwatności mamy do czynienia - zdaniem NSA, które zostało wyrażone w wyroku z dnia 5 lutego 2003 r. (II SA 3505/01, Mon. Pr. 2003, nr 7, s. 291) - w przypadku zbierania danych o wykształceniu i stanie cywilnym przy zawieraniu umów odpowiedzialności cywilnej posiadacza pojazdu mechanicznego.

162

ADMINISTRATOR DANYCH

- Podstawy legalności = zasady przetwarzania danych osobowych
- Obowiązek szczególnej staranności
- **Obowiązek informacyjny**
- Obowiązki związane z udostępnianiem danych
- Obowiązki zw. z zabezpieczeniem zbiorów d.o

163

Obowiązek informacyjny

Administrator danych pozyskując dane osobowe, od osoby, której one dotyczą powinien poinformować o:

- adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o 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, o jego podstawie prawnej.

164

Twoja osobista!

Warszawska Karta Miejska

Co to jest "Twoja osobista Warszawska Karta Miejska"?

"Twoja osobista Warszawska Karta Miejska" to nie bilet, jest Warszawska Karta Miejska, która jest rodzajem biletu doposażonym (dla 1-30 dniowych) posiadającym jednocześnie na reverse swojej ramki zdjęcie osoby oraz jego danych - imię i nazwisko.

W ten sposób "Twoja" Karta staje się Twoją osobistą WKM.

Nieopłacone datki na kartę jest możliwe od 2 czerwca 2008 r., wraz z wprowadzeniem nowej taryfy biletowej. Pracownicy jest określony jako **personalizacja karty**.

Nieopłacone razowe oferty w postaci personalizacji WKM są dostępne również dla posiadaczy kart z datą ważności użytkownika. Personalizacja kart dokonuje się w datowniku biletu. Imię i nazwisko, tryb kodowania na kartach jest daty i danych - to jednak osoba podpisująca imię, nazwisko i warunki dokumentu jest zgodna.

Podczas personalizacji każdy użytkownik może wybrać jeden z pięciu wzorów spersonalizowanej karty. W przypadku wyboru wzoru będzie wybrany.

Pierwsza Karta jest wydawana bezpłatnie

Ważność, której wartość się dane osobie umożliwia za darmo nie dopłaca, również za jej duplikat. Duplikat biletu kosztuje 10 zł, w przypadku gdy bilet uległ uszkodzeniu lub został zgubiony. Także za 10 zł można uzyskać nową wersję karty. Wniosek o wydanie pierwszej karty można też uzyskać przez Internet. W przypadku zgubienia, kiedy to biletu, biletu i biletu, to koszt biletu duplikatu biletu będzie musiał zapłacić 10 zł.

Za datowanie spersonalizowanej WKM płaci jeden bilet korzyści. Przedstawia o korzyści z personalizacji Warszawskej Karty Miejskiej.

Bezpieczeństwo danych

Proces datowania danych osobowych odbywa się pod ścisłą kontrolą, dlatego też dane datowane przez ZTM są bezpieczne. Zgodnie z Ustawą o ochronie danych osobowych (Dz. U. z 2002 r. 101, poz. 926 ze zm.) ZTM może gromadzić i przetwarzać dane osobowe niezbędne w trakcie procesu personalizacji karty. Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne do przetwarzania danych osobowych (Dz. U. z 2002 r. 101, poz. 1024), dane gromadzone przez ZTM mają charakter danych osobowych. Za ich ochronę odpowiada ZTM przed osobami przetwarzającymi.

165

PERSONALIZACJA

W nowej taryfie wprowadzono nowy rodzaj Warszawskiej Karty Miejskiej (WKM) w postaci karty spersonalizowanej, wydawanej w Punktach Obsługi Pasażerów ZTM lub w innym autoryzowanym przez ZTM punkcie.

Personalizacja WKM nie jest obowiązkowa - równolegle funkcjonuje WKM w dotychczasowej formie, tak więc pasażer ma prawo wyboru rodzaju używanej Karty. Z posiadaniem spersonalizowanej Karty wiążą się jednak korzyści, których nie daje "zwykła" WKM.

Za wydanie pierwszej Karty opłata nie jest pobierana, natomiast za wydanie kolejnej nowej Karty pobierana jest opłata w wysokości 10 zł. Personalizacja WKM, w przypadku zagubienia Karty, zniszczenia lub kradzieży, umożliwia, na wniosek zainteresowanej osoby, wydanie duplikatu Karty z niewykorzystaną częścią biletu i okresem ważności zgodnym z okresem zakodowanym na utraconej Karcie.

Mając na uwadze, że Karta spersonalizowana jest przypisana do konkretnej osoby, pasażer nie ma obowiązku posiadania przy sobie dokumentu tożsamości (z wyjątkiem dokumentu poświadczającego prawo do ulgi), który w tej chwili jest niezbędny dla uznania ważności imiennej WKM.

Karta powyższa jest wydawana na wniosek pasażera. Dane osobowe pasażerów zbierane w związku z wykonywanymi przez ZTM zadaniami, wynikającymi ze Statutu ZTM, podlegają ochronie zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.).

166

WNIOSEK O WYDANIE SPERSONALIZOWANEJ WARSZAWSKIEJ KARTY MIEJSKIEJ

Pierwsze imię

Nazwisko:

Peset:

Adres zamieszkania/kod pocztowy

Telefon kontaktowy

W związku z obowiązkiem wynikającym z art. 21 ustawy o ochronie danych osobowych z dnia 26 sierpnia 1997 r. (zakt. jedn. z 2002 r. 101, poz. 926 ze zm.) niniejszy wniosek, informację o przetwarzaniu danych osobowych w celu wydania spersonalizowanej Warszawskiej Karty Miejskiej (WKM) w celu wydania kolejnej nowej spersonalizowanej WKM w przypadku jej utraty. Osoba, która dane dotyczące przetwarzania danych osobowych, w tym: adres zamieszkania w art. 13 Ustawy, Podanie danych w celu wydania. Adres zamieszkania danych osobowych, w tym: adres zamieszkania, ul. Warszawa 27, 00-009 Warszawa.

Zapoznałem się z powyższymi postanowieniami oraz wyrażam zgodę na przetwarzanie moich danych osobowych na podstawie Ustawy. Wniosek wypełniony nieczytelnie lub nieprawidłowo nie będzie realizowany.

Podpis wnioskodawcy lub
osoba upoważniona

167

AGENDA cz. 1/2 Zasady przetwarzania danych osobowych – Udostępnianie danych



Pytanie

Zainteresowany przychodzi zapisać się na studia. Zna adres Uczelni, wie w jakim celu są zbierane jego dane. Natomiast Uczelnia musi go jeszcze poinformować o prawie dostępu i poprawianiu danych. W jaki sposób można to zrobić? Słownie, czy pisemnie?

168

Obowiązek informacyjny

Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych.

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, określonych informacji

169

Obowiązek informacyjny

- jakie dane osobowe zawiera zbiór,
- w jaki sposób zebrano dane,
- w jakim celu i zakresie dane są przetwarzane,
- w jakim zakresie oraz komu dane zostały udostępnione.

170

Obowiązek informacyjny

Na wniosek osoby, której dane dotyczą, informacji, o których mowa wyżej, udziela się na piśmie. Jeżeli osoba, której dane dotyczą nie zażąda informacji w formie pisemnej, wystarczająca jest forma ustna.

171

Udostępnianie danych osobowych

Potoczne rozumienie udostępniania – faktyczne przekazanie danych
bądź umożliwienie zapoznania się z treścią danych

Nie jest udostępnianiem przekazywanie danych w ramach struktury organizacyjnej administratora danych
/np. pomiędzy wydziałami w urzędzie lub pracownikami w firmie/
- administrator dopuszcza do przetwarzania osoby upoważnione

Przepisy ustawy dot. udostępniania odnoszą się do udostępniania „na zewnątrz”
– podmiotom spoza struktury administratora

172

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, 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.

Podstawy udostępnienia - TRYB UDOSTĘPNIENIA

- przepis prawa
- wiarygodne uzasadnienie potrzeby posiadania danych (nie dotyczy tzw. danych wrażliwych) a udostępnienie nie naruszy praw i wolności osoby, której dane dotyczą

173

UDOSTĘPNIANIE DANYCH

1. przepis prawa

2. wiarygodne uzasadnienie potrzeby posiadania danych, a udostępnienie nie naruszy praw i wolności osoby, której dane dotyczą
– nie dotyczy udostępniania danych wrażliwych!

174

Udostępnianie na podstawie przepisu prawa

- Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia lub upoważnionej przezeń osoby może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii

175

Udostępnianie na podstawie przepisu prawa

- W szczególności dostęp do danych osobowych na podstawie przepisu prawa mogą mieć:
- Państwowa Inspekcja Pracy, Zakład Ubezpieczeń Społecznych, organy skarbowe, Policja, Agencja Bezpieczeństwa Wewnętrznego, sądy powszechne, Najwyższa Izba Kontroli, Generalny Inspektor Ochrony Danych Osobowych i inne upoważnione przez przepisy prawa podmioty i organy, działające w granicach przyznanych im uprawnień –
- **wszystkie – po okazaniu dokumentów potwierdzających te uprawnienia.**

176

Udostępnianie na podstawie wniosku

- 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 art.29 ust 3

177

Udostępnienie danych osobowych

- Kiedy odmówimy udostępnienia danych?

Gdy udostępnienie spowodowałoby (art. 30 u.o.d.o.)

- ujawnienie wiadomości stanowiących tajemnicę państwową,
- zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
- zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
- istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

178

Udostępnienie danych osobowych

- FORMA UDOSTĘPNIENIA/ODMOWY
UDOSTĘPNIENIA DANYCH OSOBOWYCH:

Udostępnienie co do zasady **nie przybiera formy**:

- decyzji administracyjnej
- postanowienia
- zaświadczenia

Jest to zazwyczaj czynność **faktyczna**, tzw. czynność materialno – techniczna

179

Udostępnienie danych osobowych

ODNOTOWYWANIE FAKTU UDOSTĘPNIENIA DANYCH:

Administrator danych osobowych ma (m.in..) obowiązek zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (art. 38).

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)

§7. 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:
(...)

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;
(...)

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

180

Odpowiedzialność za bezprawne udostępnienie danych

Odpowiedzialność administracyjna

może ją ponosić administrator danych, wynika z decyzji (nakazów GODO)

- np. nakaz zaprzestania udostępniania danych

Odpowiedzialność porządkowa i dyscyplinarna

pracownika wobec pracodawcy

- za naruszenie obowiązków pracowniczych

Typowe sankcje: upomnienie, nagana.

Jeśli naruszenie jest uznawane za ciężkie, sankcją może być rozwiązanie stosunku pracy bez wypowiedzenia.

Odpowiedzialność cywilna

za szkody na zasadach określonych w kodeksie cywilnym – art. 415 i n.

„Kto z winy swej wyrządził drugiemu szkodę obowiązany jest do jej naprawienia”

ewentualnie odpowiedzialność za krzywdy (niemajątkowe)

181

Odpowiedzialność za bezprawne udostępnienie danych

Odpowiedzialność karna za bezprawne udostępnianie danych

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.

182

Udostępnienie danych osobowych

- Czy dane osobowe pracowników można udostępniać publicznie?
- Np. na tablicy ogłoszeń, w Internecie?

183

Udostępnienie danych osobowych

- jedynie w zakresie:
- stopni naukowych i stanowiska, miejsca zatrudnienia i funkcji pełnionych w Uczelni,
- zajęć dydaktycznych (w stosunku do nauczycieli akademickich),
- sprawy kandydowania w wyborach do organów Uczelni, niezbędnych do tego informacji (w szczególności życiorysu w brzmieniu ustalonym przez kandydata) i wyników wyborów,
- odznaczeń, nagród i wyróżnień (bez wskazania kwot pieniężnych).

184

- Czy można udostępniać informacje o wysokości wynagrodzenia pracownika?

185

Udostępnienie danych osobowych

- Tajemnica wynagrodzenia
- Art. 97 par.2 k.p. oraz par.1 Rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 15 maja 1996 r. w sprawie szczegółowej treści świadectwa pracy oraz sposobu i trybu jego wydawania i prostowania Dz. U. nr 60 poz. 282 ze zm.

186

Udostępnienie danych osobowych

Zasada: pracodawca zamieszcza w świadectwie pracy informację o wysokości i składnikach wynagrodzenia tylko na wyraźne żądanie pracownika.

Pracownik z różnych powodów będzie mógł z tego prawa zrezygnować, przy czym rezygnacja będzie musiała być wyrażona w sposób niebudzący wątpliwości - wtedy to pracodawca zgodnie z art. 97 par. 2 k.p. ujawni informacje o wynagrodzeniu

187

Udostępnienie danych osobowych

Przepis par 8 pkt.2 rozporządzenia Ministra Pracy i Polityki Socjalnej z 29 maja 1996 r w sprawie zakresu prowadzenia przez pracodawcę dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika **nakazuje prowadzenia dla każdego zatrudnionego imiennej karty/listy/ wypłacanego wynagrodzenia za pracę i innych świadczeń związanych z pracą.**

188

Udostępnienie danych osobowych

Przy czym realizacja tajemnicy zarobków pracowników wiąże się z zasadą, **iż nikt nie może mieć wglądu do dokumentacji pracownika bez jego zgody lub wyraźnego ustawowego upoważnienia.**

Pracodawca bez zgody pracownika nie może udostępnić akta osobowe oraz dokumentacje w sprawach związanych ze stosunkiem pracy osobom trzecim – z wyłączeniem podmiotów uprawnionych ustawowo: do kontroli i wglądu w tę dokumentację, na przykład inspektorów pracy, pracowników ZUS, kontrolerów NIK sądom,, społecznym inspektorom pracy, pracownikom urzędów pracy itp.

189

Udostępnienie danych osobowych

Kiedy można, bez zgody pracownika, ujawniać dane o wynagrodzeniu?

- Na podstawie przepisów szczególnych:

Art. 8 ustawy z dnia 24 czerwca 1983 r. o społecznej inspekcji pracy – uprawnia pracodawcę, ażeby społecznym inspektorom pracy ujawniać informację oraz okazywać dokumenty w sprawach wchodzących w zakres ich działania, czyli też do danych o warunkach płac konkretnych pracowników

190

Udostępnienie danych osobowych

Przepisy egzekucyjne i podatkowe:

Art. 883 k.p.c. zobowiązuje pracowników do ujawniania komornikowi sądowemu, który zajął wynagrodzenie za pracę w ramach egzekucji sądowej, wysokości i terminu wypłaty wynagrodzenia pracownika oraz informowania komornika o wszelkich związanych z tym zmianach,

Art. 72 par. 3 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji nakłada na pracodawcę obowiązek ujawniania wysokości wynagrodzenia pracownika, którego wynagrodzenie zostało zajęte w toku egzekucji na podstawie ww. ustawy

191

Udostępnienie danych osobowych

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, stanowi, iż informacje o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania tych funkcji nie podlegają ograniczeniu ze względu na sferę prywatności

192



Pytanie

- Czy sąd musi podać podstawę prawną na której opiera swoje żądanie skierowane do uczelni o udostępnienie adresu studenta?

193

- 
- Zgodnie z art. 248 kpc, każdy obowiązany jest przedstawić na zarządzenie sądu w oznaczonym terminie i miejscu dokument znajdujący się w jego posiadaniu i stanowiący dowód faktu istotnego dla rozstrzygnięcia sprawy, chyba że dokument zawiera tajemnicę państwową

194



Pytanie

- Wykonaniu podlegać powinno również zarządzenie sądu, w którym wprost nie wskazano podstawy prawnej żądania. Podstawą w takiej sytuacji są ogóle przepisy procedury. Ponadto, osoba nie stosująca się do zarządzeń sądu może zostać ukarana grzywną.

195

- 
- W jakich przypadkach szkoły wyższe mogą udostępniać rodzicom, w związku z ciążącym na nich obowiązkiem alimentacyjnym bądź mającym się dopiero rozpocząć postępowaniem sądowym o ustalenie obowiązku alimentacyjnego, informacji o tym, czy syn lub córka nadal studiuje.
 - Czy wystarczy, jeśli rodzic przedstawi zaświadczenie postępowania sądowego o ustalenie obowiązku alimentacyjnego? Ale jak ustrzec się przed fałszywym zaświadczeniem? Czy może lepiej, żeby sąd zwrócił się z tym zapytaniem do uczelni?

196

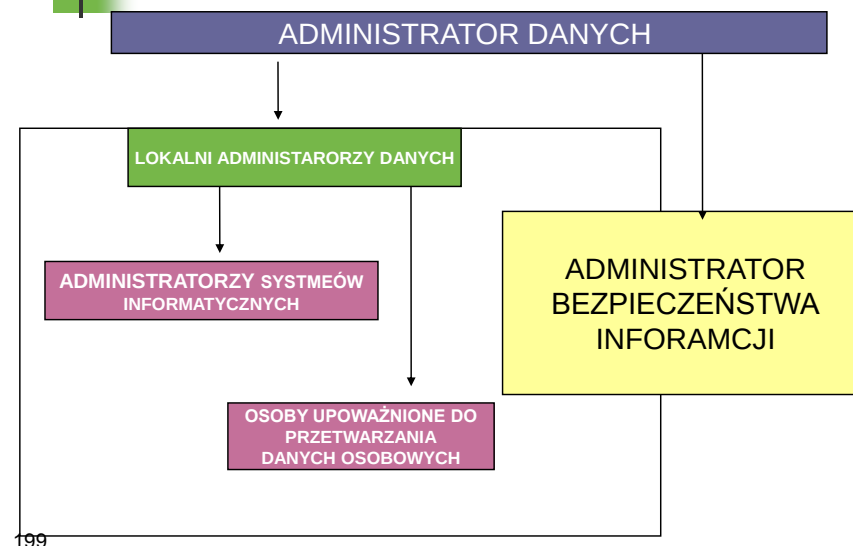
- Trudno w ustawie o ochronie danych osobowych znaleźć podstawę do udostępnienia danych na temat studenta jego rodzicowi. Zgodnie z jej przepisami przetwarzanie danych jest co prawda możliwe, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa

197

- Jednakże przepis ten należy interpretować w ten sposób, że administrator danych może powołać się na omawianą przesłankę tylko wtedy, gdy jest to niezbędne do wykonania **jego** uprawnień lub obowiązków, a nie osoby trzeciej (rodzica). W związku z powyższym należałoby uznać, że uczelnie powinna poczekać, aż sąd skieruje odpowiednie żądanie.

198

Kto odpowiada za ochronę danych osobowych?



199

Kto odpowiada za ochronę danych osobowych?

- Administrator danych osobowych
- Administrator bezpieczeństwa informacji ABI
- Lokalni administratorzy danych osobowych
- Administratorzy Systemów Informatycznych
- Osoby upoważnione do przetwarzania danych osobowych

200

ADMINISTRATOR DANYCH OSOBOWYCH

Administrator danych to podmiot uprawniony do **decydowania o celach i środkach przetwarzania danych osobowych**, na który ustawa nakłada wiele obowiązków związanych z przetwarzaniem danych.

Administratorem może być zarówno

- **podmiot publiczny**, jak i
- **podmiot prywatny**.

201

ADMINISTRATOR DANYCH OSOBOWYCH

- **Administratorem danych osobowych, zwanym dalej „ADO”** – w sensie formalno-prawnym jest **Uczelnia**,
- natomiast w sensie praktycznym za realizację podstawowych obowiązków ADO odpowiedzialny jest
 - **REKTOR**

202

ADMINISTRATOR DANYCH OSOBOWYCH

- W zakresie ochrony danych osobowych Uczelnia winna dokłada szczególnej staranności w celu **ochrony interesów osób, których dane dotyczą**, a w szczególności zapewniać, aby dane te były:
 - *przetwarzane zgodnie z prawem,*
 - *zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,*
 - *merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,*
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania

203

ADMINISTRATOR DANYCH OSOBOWYCH

- Rektor wyznacza
- **Administradora Bezpieczeństwa Informacji** zwanego dalej
 - **„ABI”**
- nadzorującego przestrzeganie zasad zabezpieczania danych osobowych w Uczelni

204

ADMINISTRATOR DANYCH OSOBOWYCH

- Wyznaczenie administratora bezpieczeństwa informacji powinno mieć formę pisemną; choć przepisy nic na ten temat nie mówią, warto o to zadbać ze względów dowodowych. Wyznaczenie ABI powinno znaleźć także odzwierciedlenie w indywidualnym zakresie czynności - obowiązków osoby wyznaczonej.

205

ADMINISTRATOR DANYCH OSOBOWYCH

- Obowiązek wyznaczenia administratora bezpieczeństwa informacji dotyczy obecnie nie tylko administratorów, którzy przetwarzają dane w systemach informatycznych (jak było to "pod rządami" poprzedniego rozporządzenia), ale **także administratorów przetwarzających dane w tradycyjnych zbiorach danych ("ręcznie")**.

206

ADMINISTRATOR DANYCH OSOBOWYCH

- Administrator Bezpieczeństwa Informacji może być pracownikiem administratora danych (tak jest zazwyczaj), może jednak być to również osoba zatrudniona na podstawie umowy cywilno-prawnej (np. zlecenia) - przepisy nie rozstrzygają tej kwestii.
- Niewątpliwie jednak bezpieczniejsze dla administratora jest pierwsze z wskazanych powyżej rozwiązań. W praktyce funkcja ABI jest niekiedy łączona ze sprawowaniem innych funkcji.

207

Administrator Bezpieczeństwa Informacji - ABI

- Sprawuje nadzór nad przeciwdziałaniem dostępowi osób nieuprawnionych do zbiorów danych oraz wykrywanie naruszeń w systemie ochrony i prawidłowego wykorzystywania danych osobowych w Uczelni

208

Administrator Bezpieczeństwa Informacji - ABI

- sprawuje nadzór nad wdrażaniem
- instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych we wszystkich systemach informatycznych Uczelni, w których przetwarzane są dane osobowe oraz dba o bieżące jej przystosowanie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych,

209

Administrator Bezpieczeństwa Informacji - ABI

- wytycza strategię zabezpieczania systemów informatycznych Uczelni,
- identyfikuje i aktualizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Uczelni,

210

Administrator Bezpieczeństwa Informacji - ABI

- określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
- monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych oraz ich przetwarzania.

211

Administrator Bezpieczeństwa Informacji - ABI

- ABI w wykonywać swoje zadania mogą przy pomocy np.
- Administratorów sieci teleinformatycznych
- Działu Technicznego – Centrum Sieci Komputerowych?

212

Administrator Bezpieczeństwa Informacji - ABI

- Zobowiązany jest do prowadzenia dokumentacji odzwierciedlającej wykonywanie zadań z zakresu ochrony danych osobowych i baz danych:

213

Administrator Bezpieczeństwa Informacji - ABI

- Dokumenty:
- Polityka bezpieczeństwa
- Instrukcja zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych

214

Administrator Bezpieczeństwa Informacji - ABI

- Dokumenty:
- Instrukcja postępowania w przypadkach naruszenia ochrony danych osobowych
- Wykaz informatycznych baz danych, w których przetwarzane są dane osobowe

215

Administrator Bezpieczeństwa Informacji - ABI

- Dokumenty:
- Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatory
- Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych

216

ADMINISTRATOR DANYCH OSOBOWYCH

- Obowiązki wynikające z ustawy o ochronie danych osobowych REKTOR powierza
- „**LOKALNYM ADMINISTRATOROM DANYCH**”
 - daje
- LOKALNYM ADMINISTRATOROM

217

LOKALNI ADMINISTRATORZY np.

- prorektor – w zakresie podległych im jednostek organizacyjnych,
- dziekan – w zakresie pracowników i studentów poszczególnych wydziałów,
- kanclerz – w zakresie podległych mu jednostek organizacyjnych,
- kwestor – w zakresie podległych mu jednostek organizacyjnych,
- dyrektor Biblioteki Głównej – w zakresie zbioru danych osobowych osób korzystających z Biblioteki Głównej Uczelni.

218

LOKALNI ADMINISTRATORZY

- Określają indywidualne obowiązki i odpowiedzialność osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy

219

LOKALNI ADMINISTRATORZY

- Zapoznają osoby zatrudnione przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie

220

LOKALNI ADMINISTRATORZY

- Wykonują zalecenia ABI w zakresie ochrony danych osobowych i baz danych w systemach informatycznych funkcjonujących w podległych im jednostkach

221

LOKALNI ADMINISTRATORZY

- Przekazują, w przypadku zaistnienia jakichkolwiek zmian, na bieżąco do ABI aktualnych danych w zakresie:
- wykazu informatycznych baz danych, w których przetwarzane są dane osobowe Uczelni

222

LOKALNI ADMINISTRATORZY

- Przekazują, w przypadku zaistnienia jakichkolwiek zmian, na bieżąco do ABI aktualnych danych w zakresie:
- ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych oraz w zbiorach papierowych i identyfikatorów tych osób

223

LOKALNI ADMINISTRATORZY

- Przekazują, w przypadku zaistnienia jakichkolwiek zmian, na bieżąco do ABI aktualnych danych w zakresie:
- wykazu miejsc, w których te dane są przetwarzane

224

LOKALNI ADMINISTRATORZY

- Bez zbędnej zwłoki informuję ABI o stwierdzonych nieprawidłowościach przy przetwarzaniu danych osobowych w Uczelni

225

LOKALNI ADMINISTRATORZY

- Stwarzają warunki techniczne i organizacyjne umożliwiające spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych w podległych im jednostkach

226

LOKALNI ADMINISTRATORZY

- Wdrażają i nadzorują przestrzeganie

instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych



zabezpieczanie danych osobowych

227

LOKALNI ADMINISTRATORZY

- Szczególnym ich zadaniem jest wyznaczanie
- **administratorów systemów informatycznych**
- funkcjonujących w podległych im jednostkach

228

ADMINISTRATORZY SYSTEMÓW INFORMATYCZNYCH - ASI

- Mają za zadanie opracowanie i bieżące uaktualnianie szczegółowych instrukcji dotyczących zarządzania systemami informatycznymi w podległych im systemach informatycznych



zabezpieczanie danych osobowych

229

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

- Osoby mające być dopuszczonymi do pracy na stanowiskach związanych z przetwarzaniem danych osobowych powinny być przez Uczelnię zaznajomione z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony danych stosowanymi w Uczelni – oświadczenie**

230

Do użytku wewnętrznego
w XXX

Załącznik nr 1.2 do Instrukcji określającej sposób zarządzania
systemami informatycznymi w XXX

WZÓR OŚWIADCZENIA O ZAPOZNANIU SIĘ PRACOWNIKA Z PRZEPISAMI USTAWY O OCHRONIE DANYCH OSOBOWYCH

Nazwa miejscowości dnia

OŚWIADCZENIE

Ja niżej podpisany(a) oświadczam, że zapoznałem(lam) się z przepisami ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. t.j. z 2002 r. Nr 101, poz. 926 ze zm.), z przepisami 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) oraz wewnętrznymi zarządzeniami Zarządu XXX dotyczącymi ochrony danych osobowych w tym w szczególności z polityką bezpieczeństwa oraz instrukcją zarządzania systemami informatycznymi eksploatowanymi w XXX.

.....
data, imię i nazwisko pracownika

231

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

- Następnie w trakcie zatrudnienia w przypadku zmian w obowiązujących przepisach prawa, uregulowania wewnętrznych lub technikach i środkach ochrony danych osobowych na uczelni, powinni być z nimi zaznajamiani

232

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

- Do przetwarzania danych osobowych mogą być wyłącznie dopuszczone osoby

UPOWAŻNIONE

- **przez ADO lub przez lokalnych administratorów danych**

233

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

- Osoby upoważnione do przetwarzania danych osobowych zostają zaznajomione z zakresem informacji objętych tajemnicą w związku z wykonywaną przez siebie pracą.
- Informowane są także o **powinności zachowania w tajemnicy danych osobowych** oraz sposobów ich zabezpieczenia stosowanych w Uczelni.

234

Osoba, której prawa dotyczą

1. **Prawo do informacji i kontroli przetwarzanych danych przysługujące osobie, której dane dotyczą (art. 32 ustawy);**

obowiązek udzielenia informacji spoczywający na administratorze (art. 33 ustawy)

235

Osoba, której prawa dotyczą

- **Każda osoba, której dane są przetwarzane w zbiorze, ma prawo, nie częściej niż raz na 6 miesięcy, zwrócić się do administratora danych o wyczerpującą informację na temat dotyczących jej danych.**

236

Osoba, której prawa dotyczą

Podmiot, do którego osoba zwraca się z takim żądaniem, powinien m.in. poinformować o istnieniu zbioru, swojej nazwie i siedzibie, źródle, z którego informacje pochodzą, celu, zakresie i sposobie wykorzystywania danych zawartych w zbiorze, od kiedy wykorzystuje dane osobowe, o sposobie udostępniania danych, a w szczególności o ich odbiorcach. Administrator winien także poinformować osobę o treści posiadanych na jej temat danych.

Nie oznacza to jednak prawa wglądu tej osoby do dokumentów, nie jest też podstawą ich wydania.

237

Osoba, której prawa dotyczą

Odmowa może nastąpić jedynie wtedy, gdy spowodowałoby to

- ujawnienie wiadomości stanowiących tajemnicę państwową, zagrożenie
- obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub
- bezpieczeństwa i porządku publicznego, zagrożenie podstawowego interesu
- gospodarczego lub finansowego państwa, istotne naruszenie dóbr osobistych innych osób.

238

Osoba, której prawa dotyczą

- **Obowiązkiem administratora jest udzielenie żądanych informacji w terminie 30 dni.**
- **Informacja powinna być udzielona w zrozumiałej formie.**
- **Na wniosek osoby, której dane dotyczą, informacji udziela się jej na piśmie.**

239

Osoba, której prawa dotyczą

2. Prawo do poprawiania danych, żądania wstrzymania ich przetwarzania lub ich usunięcia

240

Osoba, której prawa dotyczą

- Osoba, której dane dotyczą, może zwrócić się do administratora danych o uzupełnienie, uaktualnienie, sprostowanie danych, czasowe lub stałe wstrzymanie ich przetwarzania lub o ich usunięcie.
- Musi ona jednak wykazać, że dane są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są już zbędne do realizacji celu, dla którego je zgromadzono

241

Osoba, której prawa dotyczą

- Ustawa nakazuje w takiej sytuacji administratorowi uwzględnienie żądania bez zbędnej zwłoki, chyba że dotyczy to danych, których tryb uzupełniania, uaktualniania lub sprostowania określają odrębne ustawy.
- Administrator danych jest obowiązany poinformować bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanych uaktualnieniach lub sprostowaniach danych (art. 35 ust. 3 ustawy).
- Jeśli natomiast administrator nie uwzględni żądania osoby, której dane dotyczą, to może ona wystąpić do Generalnego Inspektora z wnioskiem o nakazanie dopełnienia tego obowiązku (art. 35 ust. 2 ustawy).

242

Osoba, której prawa dotyczą

3. Prawo do wniesienia sprzeciwu (art. 32 ust. 1 pkt 8 ustawy)

243

Osoba, której prawa dotyczą

- Sprzeciw można wnieść, jeśli administrator twierdzi, że wykorzystuje dane osobowe w oparciu o przesłankę dopuszczalności przetwarzania danych wymienioną w art. 23 ust. 1 pkt 4 ustawy (przetwarzanie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego) i przesłankę wymienioną w art. 23 ust. 1 pkt 5 ustawy (przetwarzanie jest niezbędne dla wypełnienia prawnie usprawiedliwionego celu administratora albo odbiorcy danych i nie narusza praw i wolności osoby, której dotyczy), **tymczasem zaś zamierza je przetwarzać w celach marketingowych lub przekazać je innemu administratorowi danych.**

244

Osoba, której prawa dotyczą

Prawo sprzeciwu nie przysługuje osobie, której dane dotyczą, gdy

- podstawą przetwarzania danych jest zgoda tej osoby,
- realizacja obowiązku lub uprawnienia wynikającego z przepisu prawa albo
- gdy przetwarzanie danych służy zawarciu lub wykonaniu umowy między administratorem a osobą, której dane dotyczą.

245

Osoba, której prawa dotyczą

4. Żądanie zaprzestania przetwarzania danych, ze względu na szczególną sytuację osoby (art. 32 ust. 1 pkt 7 ustawy)

246

Osoba, której prawa dotyczą

- **Każda osoba może wystąpić do administratora z żądaniem zaprzestania przetwarzania jej danych osobowych, uzasadniając żądanie swoją szczególną sytuacją**

247

Osoba, której prawa dotyczą

- Umotywowane żądanie powinno być skierowane do administratora danych na piśmie
- Z takim żądaniem można wystąpić, tak jak ze sprzeciwem, jedynie wtedy, **gdy podstawą prawną przetwarzania danych jest art. 23 ust. 1 pkt 4 i 5 ustawy**

248

Osoba, której prawa dotyczą

- **W przypadku wniesienia takiego żądania administrator danych zaprzestaje przetwarzania kwestionowanych danych osobowych albo bez zbędnej zwłoki przekazuje takie żądanie Generalnemu Inspektorowi, celem podjęcia decyzji w tym zakresie**

249

ZABEZPIECZANIE DANYCH OSOBOWYCH

250

Zabezpieczenie danych osobowych

Bezpieczeństwo informacji:

- **Poufność** –zapewnieniu, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
- **Integralność** –zapewnieniu, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- **Dostępność** –zapewnieniu bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
- **Rozliczalność** –zapewnieniu, że działania podmiotu mogą być przy pisane w sposób jednoznaczny tylko temu podmiotowi,

251

Zabezpieczenie danych osobowych

- Bezpieczeństwo informacji:
- **Autentyczność** –zapewnieniu, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
- **Niezaprzeczalność** – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
- **Niezawodność** –zapewnieniu spójności oraz zamierzonych zachowań i skutków

252

Zabezpieczenie danych osobowych

1. Zasady postępowania przy przetwarzaniu danych osobowych
2. Sposób zarządzania systemem informatycznym
3. Sposoby postępowania w sytuacji naruszenia ochrony danych osobowych

253

Zabezpieczenie danych osobowych

1. Zasady postępowania

- Opracowanie dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych – odpowiednią do zagrożeń oraz kategorii danych objętych ochroną

254

Zabezpieczenie danych osobowych

1. Zasady postępowania

POLITYKA BEZPIECZEŃSTWA

255

Zabezpieczenie danych osobowych

Polityka bezpieczeństwa

zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz określonej organizacji

256

Zabezpieczenie danych osobowych

Polityka bezpieczeństwa

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.

Jej celem jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.

257

Zabezpieczenie danych osobowych

Polityka bezpieczeństwa

- **ZAWIERA**
- 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

258

Zabezpieczenie danych osobowych

Polityka bezpieczeństwa

- Dokument określający politykę bezpieczeństwa nie może mieć zbyt abstrakcyjnego charakteru.
- Zasady postępowania w niej wskazane powinny zawierać uzasadnienie wyjaśniające przyjęte standardy i wymagania. Jeżeli ma to miejsce, to rzadziej dochodzi do ich naruszenia!

259

Zabezpieczenie danych osobowych

1. Zasady postępowania

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby upoważnione

260

262

261264

262

- 262

264

- 264

Zabezpieczenie danych osobowych

1. Zasady postępowania

- **Kontroli podlega również dostęp do budynków i pomieszczeń w których przetwarzane są dane osobowe**

265

Zabezpieczenie danych osobowych

1. Zasady postępowania

- Kontrola dostępu polegać może w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do pomieszczeń.
- W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia oraz godzinę pobrania lub zdanienia klucza

266

Zabezpieczenie danych osobowych

1. Zasady postępowania

- Klucze do pomieszczeń, w których przetwarzane są dane osobowe mogą być wydawane wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do pomieszczeń na innych zasadach

267

Zabezpieczenie danych osobowych

1. Zasady postępowania

- Administrator danych/lokalni administratorzy danych prowadzą wykaz baz danych:

268

.....
nazwa jednostki organizacyjnej

**Wykaz informatycznych baz danych,
w których przetwarzane są dane osobowe**

Lp.	Nazwa bazy danych*	Forma bazy danych/ system operacyjny serwera* **	Sposób zabezpieczenia informatycznego* **	Liczba miejsc/stanowisk z prawem przetwarzania bazy danych
1	2	3	4	5

* - nazwa bazy danych - nazwa przyjęta zwyczajowo, np.: dziekanat, kadry, płace itd.

** - np.: plik OFFICE, ORACLE, DBF/Windows 2003, NOVELL itd.

*** "W" - wygaszacz ekranu na hasło,
"S" - wydzielona sieć,
"P" - wydzielony komputer,
"N" - plik lub baza szyfrowana,
"H" - hasło wraz z identyfikatorem logowania,
"B" - hasło na BIOS,
"I" - inne zabezpieczenia

Dane aktualne na dzień:

Sporządził

Zabezpieczenie danych osobowych

Instrukcja określa

- 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

Zabezpieczenie danych osobowych

2. Sposób zarządzania systemem informatycznym

Instrukcja zarządzania systemami informatycznymi używanych do przetwarzania danych osobowych

Dalej „INSTRUKCJA”

Do użytku wewnętrznego		Załącznik nr 11 do Instrukcji o określaniu sposobu zarządzania systemami informatycznymi w XXXX	
WNIOSK O NADANIE/ODBIENIE UPRAWNIEN DO DOSTĘPU DO SIECI I KOMPUTEROWEJ XXXX ORAZ JEJ ZASOBÓW (Dla użytkowników będących administratorami sieci)			
1. Imię, nazwisko oraz zajmowane stanowisko użytkownika:			
2. Proponowany identyfikator (uzgodnić z administratorem sieci):			
3. Nazwa jednostki organizacyjnej			
4. Określenie stacji roboczej (nazwę stacji roboczej, nr pomieszczenia, telefon):			
5. Określenie segmentu sieci (domeny) lub indywidualnej stacji roboczej.			
Nazwa segmentu sieci (domeny):		Specyfikacja nadawanych uprawnień	
A	☐		
B	☐		
C	☐		
D	☐		
6. Określenie wymaganych zasobów stacji roboczej			
Oprogramowanie edycyjne (nazwa i wersja programu)		Uwagi	
MS Word 97+ Excel 97	☐	MS Office 2003 Standard	☐
MS Office 97 Standard	☐	MS Office 2003 Professional	☐
MS Office 97 Professional	☐		
MS Office 2000 Standard	☐		
MS Office 2000 Professional	☐		
Inne oprogramowanie: (wskazać nazwę i wersję programu)			
7. Określenie dostępu do usług sieciowych:			
Internet ☐		Poczta elektroniczna ☐	
Inne (wskazać rodzaj usługi):			
8. Określenie dostępu do aplikacji użytkowych i baz danych			
Nazwa aplikacji		Specyfikacja nadawanych uprawnień	

WNIOSEK O COFNIĘCIE UPRAWNIENI UŻYTKOWNIKA DO SIECI KOMPUTEROWEJ ORAZ JEJ ZASOBÓW/SYSTEMU INFORMATYCZNEGO A

1. Imię, nazwisko oraz zajmowane stanowisko użytkownika:
2. Identyfikator użytkownika:
3. Nazwa jednostki organizacyjnej
4. Określenie stacji roboczej (nazwę stacji roboczej, nr pomieszczenia, telefon):
5. Określenie segmentu sieci (domeny) lub indywidualnej stacji roboczej, wobec której mają być wycofane uprawnienia.

Nazwa segmentu sieci (domeny):	A	☐	Specyfikacja zakresu cofnięcia uprawnień:
	B	☐	
	C	☐	
	D	☐	

7. Określenie usunąć uprawnień dostępu do usług sieciowych:

Internet ☐ Poczta elektroniczna ☐ Poczta elektroniczna szyfrowana ☐
Inne (wskazać rodzaj usługi):

8. Określenie usunąć uprawnień dostępu do aplikacji użytkowych i baz danych

Nazwa aplikacji	Specyfikacja nadawanych uprawnień			
Środki Trwałe	USER ☐	DBA ☐	SA ☐	
System FK	USER ☐	DBA ☐	SA ☐	
System Płace	USER ☐	DBA ☐	SA ☐	
Platnik	USER ☐	DBA ☐	SA ☐	
System A	GOSC ☐	UZYTKOWNIK ☐		
	KOREKTOR ☐	PRACOWNIK DZIAŁU A..... ☐		
	APROBANT ☐	ADMINISTRATOR ☐		
ENBEPE	ADMINISTRATOR ☐	UZYTKOWNIK ☐		
ePPERON	UZYTKOWNIK ☐			

9. Dyspozycja dotycząca indywidualnie użytkowanych zasobów (należy określić co należy zrobić z dokumentami zapisanymi w katalogu danego użytkownika)

273

Zabezpieczenie danych osobowych

2. Sposób zarządzania systemem informatycznym

- ASI:
- sposób rejestrowania i wyrejestrowywania użytkowników z systemu informatycznego oraz wskazanie osoby odpowiedzialnej za te czynności

275

Zabezpieczenie danych osobowych

2. Sposób zarządzania systemem informatycznym

- **ADMINISTRATORZY SYSTEMÓW INFORMATYCZNYCH – ASI – opracowują:**
- **zasady przydziału haseł dla użytkowników poszczególnych systemów informatycznych i częstotliwość ich zmiany oraz wskazanie osoby odpowiedzialnej za te czynności**

274

Zabezpieczenie danych osobowych

2. Sposób zarządzania systemem informatycznym

- ASI:
- procedury rozpoczęcia i zakończenia pracy
- metody i częstotliwość wykonywania kopii awaryjnych,
- metody i częstotliwość sprawdzania systemów informatycznych na obecność wirusów komputerowych oraz metodę ich usuwania,

276

Zabezpieczenie danych osobowych

2. Sposób zarządzania systemem informatycznym

- ASI:
- sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków,
- sposób postępowania w zakresie komunikacji w sieci komputerowej

277

Zabezpieczenie danych osobowych

2. Sposób zarządzania systemem informatycznym

- ASI:
- wykonywania poleceń ABI w zakresie zarządzania podległymi systemami informatycznymi,
- czuwania nad właściwym eksploataowaniem podległych im systemów informatycznych

278

Zabezpieczenie danych osobowych

2. Sposób zarządzania systemem informatycznym

- ASI:
- prowadzenia, uaktualniania na bieżąco oraz przesyłania ABI, danych w zakresie:
 - listy osób uczestniczących w przetwarzaniu danych osobowych,
 - lokalizacji pomieszczeń, w których te dane są przetwarzane, w przypadku zaistnienia jakichkolwiek zmian tych lokalizacji,
 - rodzaju systemów informatycznych funkcjonujących w zakresie ich działalności,

279

.....
Nazwa jednostki organizacyjnej

Wykaz miejsc przetwarzania danych osobowych w systemach informatycznych

Lp.	Nazwa bazy danych *	Lokalizacja (adres) *	Sposób zabezpieczenia * **	Uwagi
1	2	3	4	5

* - nazwa bazy danych: nazwa z

** - „S” - pomieszczenie z serwerem lub z serwerami,
„M” - miejsce przechowywania kopii bezpieczeństwa,
„P” - pomieszczenie, w którym przetwarzane są dane,
„G” - pomieszczenie administratora danych,

*** - „A” - alarm,
„D” - drzwi antywłamaniowe,
„K” - kraty w oknach,
„F” - folia antywłamaniowa w oknach,
„B” - brak dodatkowych zabezpieczeń .

Dane aktualne na dzień:

Sporządził

280

Zabezpieczenie danych osobowych

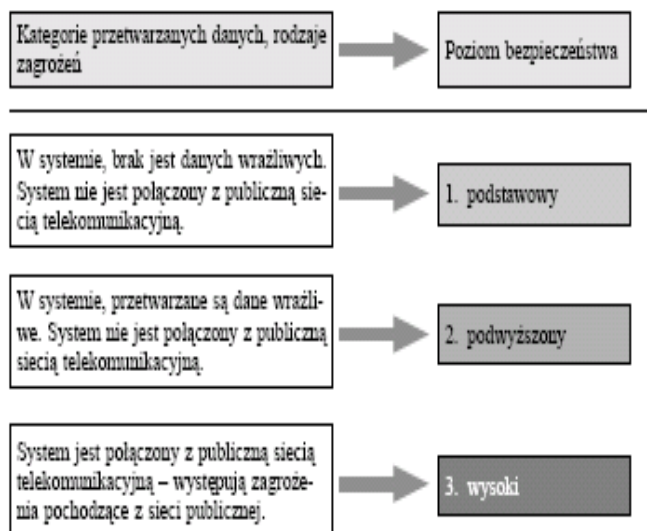
2. Sposób zarządzania systemem informatycznym

- ASI:
- listy identyfikatorów osób uczestniczących w przetwarzaniu danych osobowych w podległych im systemach informatycznych,
 - czynności serwisowych wykonywanych w podległych systemach informatycznych,
 - zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym między innymi:
 - wykrytych wirusów, koni trojańskich itp.,
 - oprogramowania nielegalnego lub zainstalowanego bez upoważnienia,
 - awarii systemu informatycznego lub jego nieprawidłowego działania,
 - stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną,
 - awarii zasilania,

281

Zabezpieczenie danych osobowych

2. Sposób zarządzania systemem informatycznym



282

Zabezpieczenie danych osobowych

POZIOM PODSTAWOWY

1. Zabezpieczenie fizyczne obszaru przetwarzania danych
2. Mechanizm kontroli dostępu do danych (identyfikator i hasło). Wymogi wobec hasła: ilość znaków (6) i okres jego używania(max. 30 dni)
Dopuszczalność stosowania dodatkowych sposobów uwierzytelnienia
1. Ochrona infrastruktury przed zakłóceniami i zagrożeniami wewnętrznymi:
 - ochrona przed awarią zasilania lub zakłóceniami w sieci zasilającej,
 - ochrona przed dostępem do danych przy pomocy oprogramowania wykorzystującego luki i błędy w systemach
- Zabezpieczenie kopii zapasowych
- Użytkowanie komputera przenośnego
- Zasady postępowania z nośnikami przeznaczonymi do likwidacji, naprawy lub przekazania innemu podmiotowi

283

Zabezpieczenie danych osobowych

2. Sposób zarządzania systemem informatycznym

POZIOM PODWYŻSZONY

1. Ilość znaków w hasle (8 znaków, hasło kombinowane)
2. Zabezpieczenie urządzeń i nośników zawierających dane osobowe wynoszone poza obszar przetwarzania danych

POZIOM WYSOKI

1. Zabezpieczenia logiczne i fizyczne przed zagrożeniami pochodzącymi ze strony sieci
2. Zabezpieczenia teletransmisji („Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej”)

284

Zabezpieczenie danych osobowych

Pytanie

- Jeżeli zbiór danych znajduje się na stanowisku komputerowym wydzielonym z sieci, a jedynie proces zbierania danych osobowych odbywa się metodą teletransmisji poprzez sieć Internet, to czy konieczne jest zastosowanie wysokiego poziomu bezpieczeństwa w stosunku do komputera (sieci komputerowej) używanej wyłącznie do zbierania danych? Czy w razie zbierania danych osobowych drogą mailową konieczne jest stosowanie wysokiego poziomu zabezpieczeń?

285

Zabezpieczenie danych osobowych

Odpowiedź

- Zgodnie z § 6 ust. 4 rozporządzenia wysoki poziom zabezpieczeń należy stosować w stosunku do komputera bądź sieci, które połączone są z siecią publiczną.
Fakt zbierania danych przy użyciu poczty elektronicznej, która nie jest pocztą wewnętrzną funkcjonującą tylko w obrębie lokalnej sieci komputerowej, świadczy o tym, że sieć ta oraz podłączone do niej komputery, w tym ten, na którym odbierana jest poczta elektroniczna, połączone są z siecią publiczną. Komputer ten należy zatem zabezpieczyć na poziomie wysokim.
Należy również zaznaczyć, że ankiety osobowe, które mają być przesyłane pocztą elektroniczną, powinny być zabezpieczone przed ujawnieniem osobom nieuprawnionym – poprzez zastosowanie odpowiednich środków kryptograficznych.

286

- ***. Uczelnia ma obowiązek zachowania szczególnych zasad bezpieczeństwa systemu wydawania i użytkowania legitymacji studenckiej. Uczelnia ponosi odpowiedzialność za bezpieczeństwo informacji zamieszczonych w legitymacji studenckiej.***

287

Odpowiedzialność administracyjna

może ją ponosić administrator danych, wynika z decyzji (nakazów GIODO)
- np. nakaz zaprzestania udostępniania danych

Odpowiedzialność cywilna

za szkody na zasadach określonych w kodeksie cywilnym – art. 415 i n.
„Kto z winy swej wyrządził drugiemu szkodę obowiązany jest do jej naprawienia”
ewentualnie odpowiedzialność za krzywdy (niemajątkowe)

Odpowiedzialność porządkowa i dyscyplinarna

pracownika wobec pracodawcy
– za naruszenie obowiązków pracowniczych

Typowe sankcje: upomnienie, nagana.
Jeśli naruszenie jest uznawane za ciężkie, sankcją może być rozwiązanie stosunku pracy bez wypowiedzenia.

Odpowiedzialność karna

288

Odpowiedzialność administracyjna

- 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:
 - usunięcie uchybień,
 - uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych,
 - zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe,
 - wstrzymanie przekazywania danych osobowych do państwa trzeciego,
 - zabezpieczenie danych lub przekazanie ich innym podmiotom,
 - usunięcie danych osobowych.

289

Odpowiedzialność administracyjna

- GIODO może żądać wszczęcia **postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania** przeciwko osobom winnym naruszeniom (na podstawie ustaleń w ramach przeprowadzonej kontroli)

290

Odpowiedzialność porządkowa i dyscyplinarna

- Najbardziej dolegliwym środkiem nadzorczego oddziaływania jakim dysponuje pracodawca w przedmiocie niewłaściwego przetwarzania danych osobowych są

kary porządkowe i dyscyplinarne

291

Odpowiedzialność porządkowa i dyscyplinarna

- Są to kary, które mogą być nakładane na osoby, naruszające zasady przetwarzania danych osobowych, biorąc pod uwagę m.in. Zasady prawa pracy oraz inne zasady obowiązujące na uczelni

292

Odpowiedzialność porządkowa i dyscyplinarna

- Odpowiedzialność porządkowa – na gruncie kodeksu pracy
- Odpowiedzialność dyscyplinarna i porządkowa – na gruncie pragmatyk służbowych

293

Odpowiedzialność porządkowa i dyscyplinarna

Art. 108 k.p. i nast.

Reguluje odpowiedzialność porządkową za nieprzestrzeganie przez pracownika ustalonej organizacji i porządku w procesie pracy.

Podstawowe sankcje =

Kara upomnienia i nagany

294

Odpowiedzialność porządkowa i dyscyplinarna

- Kara porządkowa może być zastosowana po wcześniejszym wysłuchaniu pracownika!!!
- Ale nie można zastosować tego rodzaju kary po upływie 2 tygodni od powzięcia wiadomości o naruszeniu obowiązku pracowniczego i po upływie 3 miesięcy od dopuszczenia do tego naruszenia

295

Odpowiedzialność porządkowa i dyscyplinarna

- Pracownik powinien zostać powiadomiony o zastosowaniu kary **na piśmie**.
- **Wskazując:** rodzaj naruszenia obowiązków pracowniczych, datę naruszenia, informację o prawie zgłoszenia sprzeciwu i terminie jego wniesienia.
- Odpis zawiadomienia powinien zostać złożony do akt osobowych pracownika

296

Odpowiedzialność porządkowa i dyscyplinarna

- Przy stosowaniu kary powinno się brać pod uwagę m.in.:
- Rodzaj naruszenia obowiązków pracowniczych
- Stopień winy
- Dotychczasowy stosunek do pracy pracownika

297

Odpowiedzialność porządkowa i dyscyplinarna

- Jeżeli zastosowanie kary nastąpiło z naruszeniem przepisów prawa – pracownikowi przysługuje sprzeciw – może go wnieść w ciągu 7 dni od dnia zawiadomienia go o ukaraniu
- Nieodrzućenie sprzeciwu w ciągu 14 dni od dnia jego wniesienia oznacza uwzględnienie sprzeciwu

298

Odpowiedzialność porządkowa i dyscyplinarna

- Pracownik, który wniósł sprzeciw, może w ciągu 14 dni od dnia zawiadomienia o odrzuceniu jego sprzeciwu – wystąpić do sądu pracy o uchylenie zastosowanej wobec niego kary.
- Karę uznaje się za niebyłą, a odpis zawiadomienia o ukaraniu usuwa się z akt osobowych pracownika po roku nienagannej pracy.

299

Odpowiedzialność porządkowa i dyscyplinarna

- Kodeks pracy przewiduje także
- ODPOWIEDZIALNOŚĆ MATERIALNĄ.
- w tym odpowiedzialność w przypadku, gdy pracownik z własnej winy wyrządził pracodawcy szkodę w skutek niewykonania lub nienależytego wykonania obowiązków pracowniczych

300

Odpowiedzialność porządkowa i dyscyplinarna

- Pracownik ma ponieść szkodę w granicach rzeczywistej straty podniesionej przez pracodawcę i tylko za normalne następstwo działania lub zaniechania, z których powstała szkoda.

301

Odpowiedzialność porządkowa i dyscyplinarna

- ODSZKODOWANIE nie powinno przekroczyć trzymiesięcznego wynagrodzenia przysługującego pracownikowi w dniu wyrządzenia szkody.
- W przypadku wyrządzenia szkody przez pracownika osobie trzeciej – zobowiązanym do jej naprawienia jest wyłącznie pracodawca.

302

Odpowiedzialność porządkowa i dyscyplinarna

- Art. 52 par. 1 pkt 1 k.p.
- SANKCJA W POSTACI ROZWIĄZANIA UMOWY O PRACĘ BEZ WYPOWIEDZENIA Z WINY PRACOWNIKA W RAZIE CIĘŻKIEGO NARUSZENIA PRZEZ PRACOWNIKA PODSTAWOWYCH OBOWIĄZKÓW PRACOWNICZYCH

303

Odpowiedzialność porządkowa i dyscyplinarna

- PRZYKŁADOWO:
- Naruszenie przez pracownika obowiązku zachowania w tajemnicy danych osobowych –
 - W myśl art. 100 par 2 pkt 5 k.p. przestrzeganie tajemnicy określonej w odrębnych przepisach jest jednym z podstawowych obowiązków pracowniczych

304

Odpowiedzialność porządkowa i dyscyplinarna

■ Pragmatyki służbowe

- Ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych:
 - Naruszenie mniejszej wagi = **kara porządkowa** tj. **upomnienie**
- **Kara dyscyplinarna** = **nagana**, nagana z ostrzeżeniem, nagana z pozbawieniem możliwości awansu przez okres do dwóch lat do wyższej grupy szeregowania lub na wyższe stanowisko, przeniesienie na niższe stanowisko, wydalenie z pracy w urzędzie

305

Odpowiedzialność karna

- 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.

306

Odpowiedzialność karna

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.

Naruszenie obowiązku szczególnej staranności

307

Odpowiedzialność karna

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.

Naruszenie obowiązku informacyjnego

308

Odpowiedzialność karna

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.

Naruszenie obowiązku związanego z udostępnianiem danych osobowych

309

Odpowiedzialność karna

I w końcu:

Art. 49.1.

Kto przetwarza w zbiorniku 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

310

Odpowiedzialność karna

Art. 49.2 – przetwarzanie danych wrażliwych
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

311

Ochrona karna

Kodeks Karny z dnia 6 czerwca 1997 r.
(Dz. U. 2004, Nr 93, poz 889).

**Rozdział XXXIII zatytułowany
„Przestępstwa przeciwko
ochronie informacji”**

312

- Art. 265. § 1. **Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje stanowiące tajemnicę państwową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.**
 § 2. Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
 § 3. Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

- Art. 266. § 1. **Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.**
 § 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację stanowiącą tajemnicę służbową lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia w § 1 następuje na wniosek pokrzywdzonego

- Art. 267. § 1. **Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.**
 § 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.
 § 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.
 § 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

- Art. 268. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
 § 2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.
 § 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
 § 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

- Art. 269. § 1. Kto, na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
- § 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji.

317

REASUMUJĄC:



318

Jak Albert Einstein:

**wszystko należy
robić tak prosto
jak to tylko możliwe...
ale nie prościej.**

319

W przygotowaniu prezentacji wykorzystano:

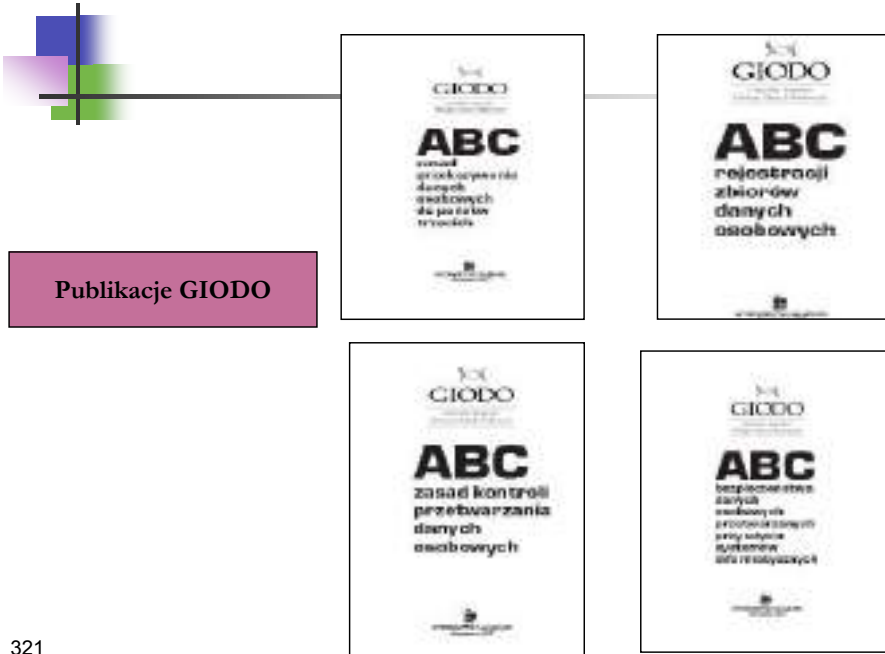
Książki, artykuły i źródła w formacie elektronicznym

J. Barta, P. Fajgielski, R. Markiewicz
OCHRONA DANYCH OSOBOWYCH
Komentarz. Wolters Kluwer 2007



P. Fajgielski
**Kontrola przetwarzania i ochrony
danych osobowych**
KUL 2008

320



321

Informacje dostępne na stronach internetowych

- www.giodo.gov.pl
- www.giodo.gov.pl
- www.kadrowe.pl
- www.twoja-firma.pl
- www.mojafirma.pl
- www.poradaprawna.pl
- <http://bip.ar.wroc.pl>

323

Pozycje:

- Ochrona dóbr osobistych w zatrudnieniu, H. Szewczyk, Wolter business 2007
- Ochrona danych osobowych w stosunkach zatrudnienia, T. Kuczyński, Przegląd Sądowy 1998, nr 11-12, s. 128

322