OCHRONA DANYCH OSOBOWYCH

Przepisy prawa o ochronie danych osobowych

- ROZPORZĄDZENIE Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (ogólne rozporządzenie o ochronie danych)
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

Wewnętrzne regulacje prawne PANS w Jarosławiu:

- **Zarządzenie Rektora nr 97/2024** w sprawie procedur dotyczących ochrony danych osobowych *(załącznik do kursu)*
- **Zarządzenie Rektora nr 76/2025** w sprawie Polityki zarządzania incydentami w zakresie cyberbezpieczeństwa *(załącznik do kursu)*

Przepisy prawa o ochronie danych osobowych

Nowa ustawa powołała **Urząd Ochrony Danych Osobowych** (UODO), który może kontrolować, czy nasza uczelnia przestrzega zasad ochrony danych osobowych

Kontrole mogą mieć miejsce:

- planowo
- z powodu skargi pracownika
- z powodu skargi klienta, studenta, kontrahenta itp.

Definicje - RODO

Dane osobowe - informacje, które pozwalają bezpośrednio lub pośrednio zidentyfikować osobę.

Przykłady:

- imię i nazwisko,
- *PESEL*
- *adres e-mail*

Szczególne kategorie danych *(dawniej dane wrażliwe)*

- Dane dotyczące zdrowia fizycznego i psychicznego (*ZFŚS, dane medyczne, stopień niepełnosprawności, dysleksja studenta*)
- Dane genetyczne (*DNA, RNA, próbki biologiczne*)
- Dane biometryczne (*wizerunek lub dane daktyloskopijne*)
- Wyroki skazujące i naruszenia prawa
- Przynależność związkowa, polityczna, religijna, rasowa

Formy występowania danych osobowych

Forma papierowa: akta osobowe, segregatory, archiwa, umowy z klientami, umowy-zlecenia, umowy o dzieło, faktury

Forma elektroniczna: programy kadrowo-płacowe, bazy klientów, dane na serwerze i na dyskach komputerów, pliki na pendrive

Forma głosowa: centrala telefoniczna

Forma wizyjna: monitoring wizyjny

Definicje - RODO

Administrator - organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych (w przypadku naszej uczelni jest to Rektor)

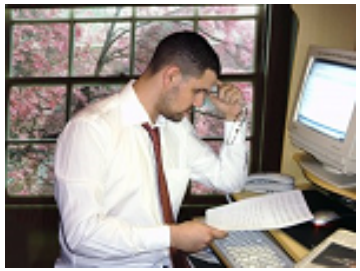
Inspektor Ochrony Danych (IOD) – koordynator wszelkich spraw związanych z danymi osobowymi w organizacji. Nadzoruje, czy Administrator, wszyscy pracownicy i współpracownicy chronią dane w należyty sposób (wszelkie sprawy związane z RODO należy zgłaszać pod adresem iod@pansjar.edu.pl)

Administrator Systemu Informatycznego (ASI) – informatyk lub firma informatyczna odpowiedzialni za prawidłowe działanie i bezpieczeństwo infrastruktury IT (Dział Bezpieczeństwa i Utrzymania Systemów Informatycznych)

Co to jest przetwarzanie danych osobowych?

Operacje na danych osobowych np.:

- wgląd
- wprowadzanie
- modyfikacja
- usuwanie, niszczenie, anonimizacja, archiwizacja



Przetwarzanie danych

- przetwarzanie w systemach informatycznych i wersjach papierowych
- archiwizacja, kopie bezpieczeństwa
- udostępnianie, powierzanie, przesyłanie

Dane podlegające ochronie – kategorie osób

Kategorie osób: Pracownicy	
Wersja papierowa	Wersja elektroniczna
• akta osobowe • umowy o dzieło, zlecenia • umowy, faktury z osobami prowadzącymi własną działalność gospodarczą • dokumentacja BHP	• System EOD • System RCP • Serwer pocztowy • USOSweb

Dane podlegające ochronie – kategorie osób

Kategorie osób: Kontrahenci	
Wersja papierowa	Wersja elektroniczna
• Faktury, umowy, zamówienia	• EOD • Serwer pocztowy

Kategorie osób: Monitoring	
Wersja papierowa	Wersja elektroniczna
	• rejestrator

Kategorie osób: Studenci	
Wersja papierowa	Wersja elektroniczna
• Akta osobowe	• USOSweb • IRK 2 • EOD

Wymiana danych z innymi podmiotami

Ujawnianie, przekazywanie - przekazanie danych pomiędzy administratorami

- „**wymuszone**” przepisem prawa – *jeżeli pracodawca musi przekazać dane pracownika do Urzędu Skarbowego, ZUS lub Komornika*
- „**możliwe**” na podstawie prawa – *kiedy pracodawca przekazuje dane pracownika do ubezpieczyciela (ubezpieczenie grupowe) ale nie musi tego robić*
- **bez przepisu prawa** - na podstawie zgody osoby – *jeżeli pracodawca przekazuje dane do Benefit Systems, kliniki medycznej za zgodą pracownika*

Powierzenie – przekazanie danych osobowych innemu podmiotowi *(firmie, instytucji),* aby ta przetwarzała je na zlecenie właściciela danych w zakresie przez niego wskazanym. np. *dane pracowników przekazywane są do zewnętrznego biura kadrowo – płacowego*

Incydent bezpieczeństwa

Naruszenie bezpieczeństwa danych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia, braku ciągłości lub nieuprawnionego dostępu do danych osobowych

Można wyróżnić trzy zasadnicze grupy incydentów w ochronie danych osobowych:

- **umyślne incydenty** (np. kradzież danych i sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych, włamanie do systemu informatycznego lub pomieszczeń),
- **zdarzenia losowe wewnętrzne** (np. awaria komputera, serwera, dysku twardego, oprogramowania, pomyłki informatyków, utrata danych),
- **zdarzenia losowe zewnętrzne** (np. pożar, zalanie wodą, utrata zasilania, utrata łączności)

Obowiązki i dobre praktyki pracownika:

- jeśli masz dostęp do danych, upewnij się, że posiadasz aktualne upoważnienie podpisane przez Rektora (nowo zatrudnione osoby powinny być zgłoszone przez kierownika jednostki organizacyjnej do Inspektora Ochrony Danych w celu przeszkolenia i wydania stosownego upoważnienia)

- na swoim stanowisku pracy stosuj wszelkie dostępne środki ochrony danych, m.in:
  - polityka czystego biurka
  - monitor ustawiony w sposób uniemożliwiający podejrzenie ekranu
  - zamykanie szafek, w których przechowywane są ważne dokumenty, nośniki danych
  - zamykanie pomieszczenia w przypadku dłuższej nieobecności

- wszelkie czynności na komputerze wykonuj na swoim koncie i nikomu go nie udostępniaj

- zablokuj ekran lub wyloguj się przed opuszczeniem stanowiska

Obowiązki i dobre praktyki pracownika:

- stosuj silne hasła (co najmniej 12 znaków, w tym małe i wielkie litery oraz znaki specjalne typu $, &, @, %) i często je zmieniaj, nawet jeśli nie wymusza tego system informatyczny

- zachowaj szczególną ostrożność w przypadku podejrzanie wyglądających wiadomości mailowych, nie klikaj w nieznane linki, nie ułatwiaj zadania cyberprzestępcom

- jeśli przesyłasz pocztą elektroniczną dane osobowe, spakuj je do archiwum zabezpieczonego hasłem, a hasło podaj adresatowi inną drogą (np. telefonicznie lub SMSem) - instrukcję znajdziesz w załączniku do Regulaminu Ochrony danych osobowych PANS w Jarosławiu (Zarządzenie Rektora nr 97/2024, zał. nr 5) (link)

- używaj Internetu rozsądnie, odwiedzaj jedynie zaufane strony, aby nie narazić komputera i sieci uczelni na atak wirusów lub hakerów

Obowiązki i dobre praktyki pracownika:

Wszelkie wątpliwości, problemy i zauważone niewłaściwe działania zgłaszaj kierownikowi jednostki lub bezpośrednio inspektorowi ochrony danych pod adresem

iod@pansjar.edu.pl

Zabezpieczenia danych studentów

Nauczyciele akademiccy **nie mogą udostępniać zbiorczych informacji**, w szczególności wykazów ocen z danymi osobowymi studentów na stronach internetowych uczelni, na własnych stronach internetowych lub w wiadomościach e-mail kierowanych do grupy studentów.

Nauczyciel akademicki odpowiada za bezpieczeństwo danych osobowych studentów, przez cały czas ich posiadania, zawartych w:

- pracach tworzonych podczas zajęć, pracach przekazywanych prowadzącemu w toku kształcenia i pracach zaliczeniowych,
- protokołach egzaminacyjnych,
- listach obecności od momentu otrzymania tych dokumentów lub ich wydrukowania z systemu do momentu ich zniszczenia,
- kartach okresowych osiągnięć studenta.

Pamiętaj!

Niedopełnienie czynności dotyczących ochrony danych może być uznane przez pracodawcę za ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy, co skutkuje postępowaniem dyscyplinarnym

(Zarządzenie Rektora nr 97/2024, zał. nr 5, pkt 15)