Metody zabezpieczeń danych osobowych oraz miejsca ich przetwarzania w Uniwersytecie Zielonogórskim

Zgodnie z art. 32 RODO, administrator danych uwzględniając stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst, cele przetwarzania i ryzyko naruszenia praw lub wolności osób fizycznych, których dane przetwarza jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić odpowiedni stopień bezpieczeństwa, w tym między innymi:

- pseudonimizację i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich
  w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

ADO oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób.
ADO podejmuje działania w celu zapewnienia, by każda osoba działająca z jego upoważnienia, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

Miejsca przetwarzania danych osobowych w Uniwersytecie Zielonogórskim

- system informatyczny – są to między innymi: serwery, macierze, komputery, laptopy, pliki w aplikacjach biurowych, dane zgromadzone w systemach QuatraMax, Dziekanat, Prolib, PERS,
- **dokumentacja papierowa** – zalicza się do niej między innymi: teczki studentów, akta osobowe pracowników, dokumenty wydrukowane zawierające dane osobowe.

Zabezpieczenia techniczne i organizacyjne danych osobowych w Uniwersytecie Zielonogórskim

Budynki Uniwersytetu, w których przetwarzane są dane osobowe powinny być wyposażone w następujące zabezpieczenia:

- alarm PPOŻ,
- monitoring wizyjny połączony ze stacją monitoringu firmy ochraniającej budynek/alarm antywłamaniowy,
- bramę wejściową do budynku zamykaną na klucze,
- drzwi do pomieszczeń wewnątrz budynku zamykane na klucze,
- procedurę wydawania kluczy do pomieszczeń osobom uprawnionym,
- portiernię monitorującą osoby wychodzące i wychodzące z budynku.

Do zabezpieczeń technicznych i organizacyjnych danych osobowych w pomieszczeniach, w których są one przetwarzane (strefa/obszar przetwarzania danych osobowych) należą:

- szafy, w których przechowuje się dokumenty papierowe zawierające dane osobowe obligatoryjnie mają być wyposażone w zamki i być zamykane na klucz po zakończonej pracy lub podczas nieobecności osób upoważnionych do przetwarzania danych osobowych,
- procedura wydawania kluczy do drzwi i szaf oraz sposób ich wydawania,
- dostęp do danych osobowych tylko dla osób upoważnionych,

- osoby trzecie w strefie przetwarzania danych osobowych muszą przebywać zawsze w towarzystwie osób upoważnionych,
- polityka „czystego biurka” – należy pracować tylko na tych dokumentach zawierających dane osobowe, które są niezbędne w danym momencie, a po zakończonej pracy wszystkie dokumenty zawierające dane osobowe należy zamykać w szafach.

Zabezpieczenia danych osobowych przez użytkownika w systemie informatycznym:

Aby dane osobowe przetwarzane w uniwersyteckim systemie informatycznym były zabezpieczone prawidłowo każdy użytkownik systemu informatycznego ma obowiązek stosować się do poniższych zasad:

- zakazu udostępniania powierzonego Identyfikatora i Hasła,
- zakazu pracowania w systemie na koncie innego użytkownika,
- zakazu udostępniania przydzielonego Identyfikatora i Hasła innym użytkownikom, a także osobom nieupoważnionym,
- obowiązku ochrony wprowadzanych danych przez zabezpieczenie ekranu monitora przed wzrokiem nieupoważnionych osób (odpowiednie ustawienie monitora lub założenie filtru prywatyzującego),
- obowiązku zmiany hasła co 30 dni do komputera i wszystkich systemów, w których przetwarzane są dane osobowe,
- aktywizacji wygaszacza ekranu - w przypadku dłuższego opuszczenia stanowiska pracy, należy zaktywizować wygaszasz ekranu z opcją ponownego „logowania się" do systemu lub wylogować się z systemu przed opuszczeniem stanowiska pracy,
- zabezpieczenia systemu po zakończonej pracy - po zakończeniu pracy w systemie należy wylogować się z systemu, zabezpieczyć swoje stanowisko pracy przed dostępem osób nieupoważnionych;
- ochrony antywirusowej - stacja robacza ma być obligatoryjnie wyposażona w system antywirusowy,
- korzystanie z poczty uniwersyteckiej – prowadząc mailową korespondencję służbową należy obligatoryjnie korzystać z poczty uniwersyteckiej, szczególnie przesyłając dane osobowe. ,
- zakazu korzystania w celach służbowych z zewnętrznych skrzynek pocztowych (gmail, onet, wp i innych), w szczególności do przesyłania danych osobowych,
- nie należy przekierowywać poczty służbowej na zewnętrzne skrzynki prywatne, takie postępowanie grozi wyciekiem danych (brak szyfrowania),
- w przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania („logowania się" w systemie), niezwłocznie należy powiadomić o nich swojego przełożonego lub IOD,
- w przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych, niezwłocznie należy powiadomić swojego przełożonego lub IOD.

Zabezpieczenia danych osobowych na urządzeniach przenośnych w Uniwersytecie

Urządzenia przenośne, na których mogą znajdować się dane osobowe to m. in.:

- laptopy,
- tablety,
- telefony komórkowe,
- nośniki USB.

Urządzeń przenośnych zwierających dane osobowe nie powinno wynosić się z terenu Uniwersytetu Zielonogórskiego.

Jeśli zachodzi taka sytuacja należy pamiętać, że urządzenia te powinny być szyfrowane (np. zaszyfrowane nośniki USB, dyski w laptopach).