SZKOLNIE Z OCHRONY DANYCH OSOBOWYCH

Chcąc spełnić wymagania przepisów o ochronie danych osobowych zapraszamy Państwa do wzięcia udziału w krótkim szkoleniu, które przybliży podstawowe zagadnienia z tego zakresu.

Szkolenie składa się z 33 slajdów oraz testu wiedzy składającego się z 10 sprawdzających pytań.

Szkolenie ma na celu zapoznanie uczestników z informacjami niezbędnymi do prawidłowego przetwarzania danych osobowych w trakcie wykonywania swoich obowiązków i prac zleconych.

Podstawa prawna:

- Konstytucja Rzeczypospolitej Polskiej art. 47, 51

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

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

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

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

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

Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.”

- Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych
- Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO)

Podstawowe pojęcia:

Administrator danych osobowych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydującą o celach i środkach przetwarzania danych osobowych (ADO).

Przykłady **ADO:**

Instytucja	ADO
Biblioteka Publiczna miasta X	Biblioteka Publiczna miasta x
Bank Y	Bank Y
Szkoła Podstawowa nr xx	Szkoła Podstawowa nr xx
Sklep internetowy Z	Sklep internetowy Z
Biblioteka szkolna w Szkole Podstawowej	Szkoła Podstawowa
Ośrodek kultury	Ośrodek kultury

Podstawowe pojęcia:

- **Administrator Bezpieczeństwa Informacji (ABI)** - osoba powołana przez administratora danych osobowych odpowiedzialna za nadzorowanie stanu wdrożenia oraz przestrzegania zasad ochrony przetwarzania danych.

Administratorem Bezpieczeństwa Informacji może być osoba, która:

- Ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych
- Posiada odpowiednią wiedzę w zakresie ochrony danych osobowych
- Nie była karana za umyślne przestępstwa.

Podstawowe pojęcia:

- **Administrator Systemu Informatycznego (ASI)** - powołany do sprawowania nadzoru nad systemem służącym do przetwarzania danych, w szczególności nad kontrolą uprawnień użytkowników, zabezpieczeń systemów oraz tworzenia kopii zapasowych danych. Najczęściej jest to jeden z informatyków w Instytucji.

- Czy w Państwa Instytucji został powołany ABI oraz ASI?

Podstawowe pojęcia:

- **Generalny Inspektor Ochrony Danych Osobowych (GIODO)** – organ do spraw ochrony danych osobowych, ma uprawnienia kontrolne w zakresie zgodności przetwarzania danych z przepisami. Prowadzi rejestr zbiorów danych osobowych oraz rejestr administratorów bezpieczeństwa informacji.

- GIODO jest to organ, który ma również na celu edukacje społeczeństwa. Radzi co zrobić w określonych sytuacjach, jak dbać o bezpieczeństwo danych osobowych.

- Do GIODO każdy może zgłosić skargę na nieodpowiednie przetwarzanie danych.

Podstawowe pojęcia:

- **Dokumentacja przetwarzania danych osobowych** – składają się na nią polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym. Dokumentacja stanowi reguły poprawnej i bezpiecznej pracy z danymi, w szczególności obowiązki w zakresie ich zabezpieczenia

- **Polityka Bezpieczeństwa Danych Osobowych** – dokument określający zasady ochrony danych osobowych przez ADO oraz upoważnione przez niego osoby.

- **Instrukcja Zarządzania Systemami Informatycznymi** – określa zasady bezpiecznego przetwarzania danych osobowych w systemach informatycznych.

Podstawowe pojęcia:

- **Przetwarzanie danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

- Przetwarzanie to każda czynność na danych, czyli m.in..:
  - Zbieranie
  - Czytanie
  - Przechowywanie
  - Opracowywanie
  - Zapisywanie
  - Usuwanie

Podstawowe pojęcia:

- **Osoba upoważniona do przetwarzania danych osobowych** – rozumie się przez to osobę, która została przez ADO na piśmie upoważniona do przetwarzania danych osobowych. **Np.:**

Stanowisko	Upoważnienie dotyczy
Bibliotekarz / Bibliotekarka	Przetwarzanie danych czytelników
Kadrowiec	Przetwarzanie danych pracowników
Lekarz	Przetwarzanie danych pacjentów
Księgowy	Przetwarzanie danych kontrahentów, współpracowników, klientów
Pracownik biurowy	Przetwarzanie danych klientów

Podstawowe pojęcia:

- **Osoba uprawniona** – osoba posiadająca uprawnienie wydane przez ADO na mocy którego wykonuje w jego imieniu określone czynności. **Np.:**

Stanowisko	Wyjaśnienie
Sprzątaczka	Nie przetwarza danych osobowych, zostaje uprawniona przez ADO do przebywania w strefie przetwarzania danych osobowych. Nie zawsze jest pracownikiem danej Instytucji.
Serwisant	Nie przetwarza danych osobowych, zostaje uprawniony przez ADO do przebywania w strefie przetwarzania danych osobowych. Nie jest pracownikiem Instytucji.

Podstawowe pojęcia:

- **Użytkownik systemu informatycznego** - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano uprawnienia do przetwarzania danych w systemie informatycznym.
- Użytkownikowi zostaje nadany **identyfikator użytkownika** oraz **hasło.**

  - **Hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

  - **Identyfikator użytkownika (login)** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Podstawowe pojęcia:

- **Dane osobowe** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić **bezpośrednio lub pośrednio**, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne, Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.
- Rozróżniamy dane zwykłe i dane wrażliwe.

NUMER TELEFONU

ZDJĘCIE

PESEL

ADRES

ADRES E-MAIL

IMIĘ I NAZWISKO

Podstawowe pojęcia:

Dane osobowe wrażliwe ujawniają**:**

- pochodzenie rasowe lub etniczne
- poglądy polityczne
- przekonania religijne lub filozoficzne
- przynależność wyznaniowa, partyjna lub związkowa
- informacje o stanie zdrowia, dane genetyczne
- informacje o nałogach, życiu seksualnym
- dane dotyczące skazań, orzeczeń o ukaraniu i mandaty karne
- orzeczenia wydawane w postępowaniu sądowym i administracyjnym
- dane biometryczne

Przetwarzanie danych wrażliwych bez odpowiedniej podstawy prawnej jest zakazane!

Podstawowe pojęcia:

- **Zbiór danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony (jego części znajdują się w różnych miejscach) lub podzielony funkcjonalnie (przetwarzany za pomocą programów realizujących różne funkcje). **Np.:**

Zbiór danych	Opis
Pracownicy	Osoby zatrudnione na podstawie umowy o pracę.
Czytelnicy	Osoby korzystające z zasobów biblioteki: czytelnicy, osoby korzystające z czytelni internetowej
Newsletter	Osoby, które zapisały się na odbiór newslettera

Podstawowe pojęcia:

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, czyli zgoda nie może być zawarta w regulaminie.

Zgoda może być odwołana w każdym czasie.

Jedna zgoda na jeden cel przetwarzania.

Chcąc uzyskać zgodę na przesyłanie newslettera, na marketing produktów własnych oraz na marketing produktów partnerów potrzebne są trzy oddzielne zgody.

Zgoda może być wyrażona w dowolnej formie, ale na ADO spoczywa obowiązek udowodnienia, że ją pozyska.

Zgoda

- Wyrażenie zgody może polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej lub zapisu na usługi.
- Okienko wyrażenia zgody nie może być domyślnie zaznaczone.
- Uzyskanie zgody podczas nagrywania ankiet wideo – nagranie zgody przed lub po udzieleniu odpowiedzi
- Klauzula zgody nie może być umieszczona w regulaminie usługi.
- Zgoda na zrobienie zdjęcia nie jest jednocześnie zgodą na wykorzystanie wizerunku.
- Zgoda na przesyłanie ofert reklamowych firmy x, nie jest jednocześnie zgodą na wysyłanie ofert reklamowych partnerów firmy x.

Przetwarzanie danych dopuszczalne jest gdy zostanie spełniony jeden z poniższych warunków:

- Osoba, której dane dotyczą, wyrazi na to zgodę np.:
  - Wysyłanie newslettera
  - Udział w konkursach
  - Publikowanie wizerunku

  lub
- Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa np.:
  - Dane pracowników – umowa o pracę, umowa zlecenie

  lub

Przetwarzanie danych dopuszczalne jest gdy zostanie spełniony jeden z poniższych warunków:

- Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną np.:
  - Zakup towaru przez internet

lub

- Jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego np.:
  - Monitoring wizyjny w okolicy instytucji publicznej

lub

Przetwarzanie danych dopuszczalne jest gdy zostanie spełniony jeden z poniższych warunków:

- Jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez ADO albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą np.:
  - marketing bezpośredni – listownie
  - dochodzenie roszczeń z tytułu działalności gospodarczej

Obowiązek informacyjny

Administrator Danych Osobowych powinien poinformować osobę, której dane zamierza przetwarzać o:

- adresie swojej siedziby i pełnej nazwie
- celu zbierania danych
- dobrowolności albo obowiązku podania danych, a jeśli taki obowiązek istnieje, o jego podstawie prawnej
- okresie przez, który dane osobowe będą przechowywane bądź kryteria ustalania tego okresu
- informacje o zamiarze przekazywania danych do państwa trzeciego
- prawie wniesienia skargi do organu nadzorczego
- prawach osoby, której dane dotyczą to jest prawie do :
  - usunięcia danych;
  - ograniczenia przetwarzania
  - prawie przenoszenia danych
  - prawie do cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych).
- danych Administratora Bezpieczeństwa Informacji

Obowiązek informacyjny

- W przeciwieństwie do zgody, obowiązek informacyjny może być umieszczony w dowolnym miejscu. **Np.**
  - W regulaminie usługi
  - Pod okienkiem zgody
  - Pod formularzem kontaktowym, ankietą w formie rozwijającej się wiadomości
  - Poprzez wysłanie wiadomości na adres mailowy

Dokumentacja przetwarzania 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
- Wykaz zbiorów danych wraz ze wskazaniem struktury danych i powiązań między nimi
- Sposób przepływu danych pomiędzy poszczególnymi systemami
- Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Dokumentacja przetwarzania danych osobowych

Instrukcja Zarządzania Systemami Informatycznymi zawiera:

- 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
- Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych
- Sposób zabezpieczenia systemu informatycznego
- Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Dokumentacja przetwarzania danych osobowych

- Dokumentacja określa zasady postępowania w przypadku naruszeń bezpieczeństwa informacji
- Zawiera wytyczne w zakresie pozyskiwania zgody na przetwarzanie
- Zawiera wytyczne w zakresie realizowania obowiązków informacyjnych
- Stworzenie dokumentacji to jeden z obowiązków administratora danych oraz wykazanie przez niego należytej staranności dla zapewnienia procedur bezpiecznego przetwarzania danych

Dokumentacja przetwarzania danych osobowych

- Czy w Państwa Instytucji została opracowana dokumentacja przetwarzania danych osobowych?
- Gdzie można się z nią zapoznać?

Zabezpieczenia fizyczne danych osobowych

- Biurka i szafki zamykane na klucz
- Pokoje w których przetwarzane są dane osobowe zamykane na klucz
- Odpowiednie ustawienie monitora, tak aby ekran był widoczny tylko dla osoby z niego korzystającej
- Nie pozostawianie kluczy w drzwiach wejściowych do pokoju oraz w szafkach
- Monitoring
- Ochrona budynku
- Karty dostępu do obszaru przetwarzania danych osobowych
- Polityka czystego biurka
- Polityka czystego ekranu
- Polityka kluczy

Zabezpieczenia techniczne danych osobowych:

- Oprogramowanie antywirusowe
- Włączony firewall
- Zasilacze awaryjne
- Listwy przepięciowe
- Aktualizacja systemów informatycznych
- Nadawanie loginów i haseł do systemów informatycznych

Zobowiązania osoby upoważnionej do przetwarzania danych osobowych

- Zasada prywatności kont w systemach informatycznych oraz poufności haseł i kodów dostępu (zakaz zapisywania haseł na karteczkach i umieszczanie ich w widocznych miejscach)
- Zasada nadzorowania dokumentów, czystych (pustych) drukarek i niszczenia dokumentów w niszczarkach
- Zasada czystego biurka (tylko te dokumenty, które nam są potrzebne aktualnie do pracy)
- Zasada czystego ekranu (konieczność wylogowania się każdorazowo przy opuszczaniu stanowiska pracy) i czystego pulpitu (minimum ikon)

Zobowiązania osoby upoważnionej do przetwarzania danych osobowych

- Każdy pracownik przetwarza dane osobowe zgodnie z zakresem upoważnienia
- Blokowanie komputera przy każdorazowym opuszczeniu stanowiska pracy i/lub zastosowanie wygaszaczy ekranu
- Utworzenie jakiejkolwiek nowej bazy danych należy niezwłocznie zgłosić do ABI lub ADO
- Rozwaga we wszelkich działaniach związanych z przetwarzaniem danych, w szczególności ich właściwym niszczeniem oraz udostępnianiem na zewnątrz

PAMIĘTAJ:

Każdy odpowiada osobiście za powierzone dokumenty, sprzęt i bezpieczeństwo przechowywanych w nim danych.

Jeżeli istnieje podejrzenie naruszenia ochrony danych osobowych należy niezwłocznie powiadomić swojego przełożonego i/lub ABI.

Odpowiedzialność karna

- Za naruszenie przepisów o ochronie danych osobowych ustawodawca przewidział ogromne kary finansowe.
- W zależności od przewninienia kara może sięgać do 20 mln euro lub do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

- Należy pamiętać, iż utrata **wizerunku firmy, instytucji** jest najgorszym następstwem nie przestrzegania przepisów.

Dziękujemy za udział w szkoleniu

Zapraszamy do wypełnienia krótkiego testu pozwalającego na utrwalenie oraz sprawdzenie zdobytej wiedzy.