Projekt jest realizowany w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027
współfinansowanego ze środków Europejskiego Funduszu Społecznego
„Wspieranie transformacji energetycznej w Wielkopolsce Wschodniej”
FERS.01.05-IP.08-0490/23

Kwalifikacja:

Ochrona danych osobowych

Manual dla słuchacza

Realizator Projektu: Wyższa Szkoła Kadr Menedżerskich , ul. Zagórowska 3a, 62-500 Konin
Tel 632491262
www.wskm.edu.pl

Manual dla słuchaczy nr 1

Kwalifikacja rynkowa: OCHRONA DANYCH OSOBOWYCH.

Temat zajęć: Dokumentacja przetwarzania danych osobowych zgodnie z RODO

Czas zajęć: 3 godziny

Warunki realizacji:

Praca zbiorowa i w grupach – realizacja nowego materiału

Metody nauczania:

Wykład, pogadanka, burza mózgów, case study, dyskusja.

Cele ogólne:

1. **Zrozumienie wymagań prawnych RODO**:
    - Uczestnicy zdobędą wiedzę na temat kluczowych zasad i wymagań RODO dotyczących dokumentacji przetwarzania danych osobowych.
2. **Rozwinięcie umiejętności tworzenia i zarządzania dokumentacją**:
    - Szkolenie dostarczy praktycznych wskazówek dotyczących tworzenia, utrzymania oraz aktualizacji rejestrów i polityk związanych z przetwarzaniem danych.
3. **Podniesienie świadomości na temat znaczenia rozliczalności**:
    - Uczestnicy zrozumieją, jak dokumentacja pomaga wykazać zgodność z RODO i wspiera zasadę rozliczalności w organizacji.
4. **Zapewnienie narzędzi do identyfikacji i zarządzania ryzykiem**:
    - Szkolenie nauczy uczestników, jak przeprowadzać analizę ryzyka i ocenę skutków dla ochrony danych, co jest kluczowe dla zapewnienia bezpieczeństwa danych osobowych.
5. **Wzmocnienie zdolności do reagowania na incydenty i naruszenia danych**:
    - Uczestnicy dowiedzą się, jak dokumentować i reagować na naruszenia ochrony danych osobowych, co pozwoli na lepsze zarządzanie incydentami i minimalizację ich skutków.

Środki dydaktyczne:

1. **Prezentacje multimedialne**:
    - Wykorzystanie prezentacji multimedialnych do przedstawienia kluczowych pojęć, zasad i wymagań RODO w sposób wizualny i przystępny.

2. **Studia przypadków**:
    - Analiza rzeczywistych przypadków naruszeń ochrony danych i ich konsekwencji, co pozwoli uczestnikom lepiej zrozumieć praktyczne aspekty dokumentacji i zgodności z RODO.
3. **Warsztaty praktyczne**:
    - Organizacja interaktywnych warsztatów, w których uczestnicy będą mogli ćwiczyć tworzenie i ocenę dokumentacji, a także przeprowadzać symulacje analizy ryzyka i reakcji na incydenty.

Przebieg zajęć:

- Część organizacyjna
- Część wprowadzająca
- Część właściwa

KONSPEKT

konspekt szkolenia na temat "Dokumentacja przetwarzania danych osobowych zgodnie z RODO"

Konspekt szkolenia:

1. Wprowadzenie do RODO

- **Historia i tło regulacji RODO**
    - Geneza RODO.
    - Cele i założenia regulacji.
- **Podstawowe zasady RODO**
    - Zasada zgodności z prawem, rzetelności i przejrzystości.
    - Zasada ograniczenia celu.
    - Zasada minimalizacji danych.
    - Zasada prawidłowości.
    - Zasada poufności i integralności.
    - Zasada ograniczenia przechowywania.
- **Znaczenie dokumentacji w kontekście zasady rozliczalności**
    - Definicja zasady rozliczalności.
    - Przykłady zastosowania zasady w praktyce.

- Rola dokumentacji w wykazywaniu zgodności.

2. Obowiązkowa dokumentacja według RODO

- **Rejestr czynności przetwarzania danych**
  - Wymagane elementy rejestru.
  - Przykłady danych do uwzględnienia.
  - Częstotliwość aktualizacji rejestru.
- **Rejestr kategorii czynności przetwarzania**
  - Specyfika dla podmiotów przetwarzających.
  - Wymagania dotyczące zawartości.
  - Różnice w stosunku do rejestru czynności przetwarzania.
- **Polityka retencji danych**
  - Określenie okresów przechowywania danych.
  - Procedury usuwania danych.
  - Wpływ retencji na bezpieczeństwo danych.
- **Procedura weryfikacji podmiotu przetwarzającego**
  - Kryteria wyboru podmiotu przetwarzającego.
  - Metody audytowania i monitorowania.
  - Dokumentacja wyników weryfikacji.
- **Dokumentacja naruszeń ochrony danych osobowych**
  - Zasady prowadzenia rejestru naruszeń.
  - Proces zgłaszania naruszeń organowi nadzorczemu.
  - Wnioski wyciągane z analizy naruszeń.

3. Polityki ochrony danych

- **Znaczenie i cel polityk ochrony danych**
  - Wpływ polityk na zgodność z RODO.
  - Polityki jako narzędzie zarządzania ryzykiem.
- **Elementy polityki ochrony danych**
  - Kluczowe komponenty polityki.
  - Przykłady polityk w różnych organizacjach.
- **Zasady tworzenia i wdrażania polityk**
  - Proces konsultacji i akceptacji polityk.
  - Rola zarządu w implementacji.
  - Monitorowanie i przegląd polityk.

- **Uwzględnianie zasad data protection by design i by default**
    - Definicja i znaczenie zasad.
    - Przykłady zastosowania w praktyce.
- **Rola inspektora ochrony danych (IOD)**
    - Obowiązki i odpowiedzialność IOD.
    - Współpraca IOD z innymi działami.

4. Rejestry dotyczące przetwarzania

- **Rejestr czynności przetwarzania: znaczenie, zawartość, praktyczne wskazówki**
    - Przykłady wpisów do rejestru.
    - Rola rejestru w audytach i kontrolach.
- **Rejestr kategorii czynności przetwarzania: funkcje i wymagania**
    - Jakie dane są przetwarzane w imieniu administratora.
    - Dokumentacja zabezpieczeń technicznych i organizacyjnych.
- **Praktyczne aspekty prowadzenia dokumentacji**
    - Wybór formy prowadzenia rejestru (papierowa vs elektroniczna).
    - Przykłady dobrych praktyk w zakresie dokumentacji.
    - Wskazówki dotyczące audytów i przeglądów dokumentacji.

5. Dodatkowe dokumenty i procedury

- **Standardowe klauzule umowne**
    - Znaczenie klauzul w transferze danych.
    - Przykłady klauzul stosowanych w praktyce.
- **Procedury realizacji żądań podmiotów danych**
    - Proces obsługi żądań dostępu, sprostowania, usunięcia.
    - Weryfikacja tożsamości wnioskodawcy.
- **Dokumenty regulujące bezpieczeństwo danych osobowych**
    - Polityka bezpieczeństwa IT.
    - Zasady powierzania sprzętu służbowego i pracy zdalnej.
- **Postępowanie w przypadku transferów do krajów trzecich**
    - Zasady i procedury transferu danych.
    - Dokumentacja zabezpieczeń transferowych.
- **Analiza ryzyka i ocena skutków dla ochrony danych**
    - Metodyka przeprowadzania analizy ryzyka.

- Przykłady ocen skutków dla ochrony danych.

6. Case Study i Dyskusja

- **Analiza przykładowych naruszeń i ich dokumentacja**
  - Przykłady rzeczywistych incydentów.
  - Lekcje wyniesione z analizy przypadków.
- **Dyskusja na temat wyzwań w zarządzaniu dokumentacją**
  - Omówienie trudności i rozwiązań.
  - Wymiana doświadczeń między uczestnikami.

7. Podsumowanie i Q&A

- **Kluczowe wnioski**
  - Podsumowanie najważniejszych zagadnień.
  - Wskazówki na przyszłość.
- **Sesja pytań i odpowiedzi**
  - Odpowiedzi na pytania uczestników.
  - Dyskusja na temat indywidualnych wyzwań i rozwiązań.

Ten konspekt ma na celu szczegółowe omówienie kluczowych aspektów dokumentacji przetwarzania danych osobowych, zgodnie z wymaganiami RODO, oraz dostarczenie uczestnikom praktycznej wiedzy i narzędzi do wdrożenia w ich organizacjach.

SCENARIUSZE ĆWICZEŃ

1. **Scenariusz ćwiczenia: Analiza ryzyka przetwarzania danych osobowych**
   - **Cel ćwiczenia**: Uczestnicy nauczą się identyfikować i oceniać ryzyka związane z przetwarzaniem danych osobowych oraz opracowywać strategie ich minimalizacji.
   - **Opis**: Grupa uczestników zostaje podzielona na zespoły. Każdy zespół otrzymuje opis hipotetycznej organizacji, która przetwarza różne rodzaje danych osobowych. Zadaniem zespołów jest zidentyfikowanie potencjalnych zagrożeń związanych z przetwarzaniem tych danych, ocena ryzyka oraz zaproponowanie środków zaradczych. Na zakończenie zespoły prezentują swoje analizy i rozwiązania na forum grupy, co pozwala na wymianę pomysłów i dyskusję.
2. **Scenariusz ćwiczenia: Reakcja na incydent naruszenia danych**

- **Cel ćwiczenia**: Uczestnicy nauczą się, jak szybko i skutecznie reagować na incydenty naruszenia ochrony danych osobowych, w tym jak dokumentować proces reakcji.
- **Opis**: Uczestnicy zostają podzieleni na zespoły i otrzymują scenariusz, w którym dochodzi do naruszenia danych osobowych w organizacji (np. wyciek danych klientów). Zadaniem zespołów jest opracowanie planu działań, który obejmuje natychmiastowe kroki do podjęcia, komunikację z zainteresowanymi stronami, oraz sposób dokumentowania całego incydentu. Po zakończeniu ćwiczenia zespoły przedstawiają swoje plany, a trener omawia najlepsze praktyki i potencjalne poprawki.

Te scenariusze ćwiczeń mają na celu rozwijanie praktycznych umiejętności uczestników w zakresie zarządzania ryzykiem i reagowania na incydenty związane z ochroną danych osobowych.

PRZEZENTACJA 01

Manual dla słuchaczy nr 2

Kwalifikacja rynkowa: OCHRONA DANYCH OSOBOWYCH.

Temat zajęć: Zabezpieczenie danych osobowych

Czas zajęć: 3 godziny

Warunki realizacji:

Praca zbiorowa i w grupach – realizacja nowego materiału

Metody nauczania:

Wykład, pogadanka, burza mózgów, case study, dyskusja.

Cele ogólne:

1. **Identyfikacja i ocena ryzyka**: Ocena skutków dla ochrony danych ma na celu identyfikację potencjalnych zagrożeń związanych z przetwarzaniem danych osobowych oraz ocenę ryzyka naruszenia praw i wolności osób fizycznych.
2. **Zgodność z RODO**: DPIA pomaga w zapewnieniu zgodności operacji przetwarzania danych z przepisami RODO, w tym w szczególności z zasadą rozliczalności i ochrony danych w fazie projektowania.
3. **Ochrona praw i wolności osób fizycznych**: Celem DPIA jest ochrona praw i wolności osób, których dane dotyczą, poprzez wdrażanie odpowiednich środków zaradczych i mechanizmów bezpieczeństwa.

4. **Przejrzystość i odpowiedzialność**: DPIA wspiera przejrzystość działań administratora danych oraz przypisuje odpowiedzialność za ochronę danych osobowych, co zwiększa zaufanie użytkowników.
5. **Poprawa procesów przetwarzania danych**: Ocena skutków umożliwia administratorom danych optymalizację procesów przetwarzania danych, poprzez identyfikację obszarów wymagających poprawy i wdrażanie lepszych praktyk ochrony danych.

Środki dydaktyczne:

1. **Warsztaty i szkolenia**: Organizowanie warsztatów i szkoleń dla pracowników i administratorów danych, które koncentrują się na praktycznych aspektach przeprowadzania DPIA, w tym na identyfikacji ryzyka i wdrażaniu środków zaradczych.
2. **Studia przypadków**: Analiza rzeczywistych przypadków przeprowadzania DPIA, które ilustrują proces oceny skutków i decyzje podejmowane na różnych etapach, co pomaga w lepszym zrozumieniu praktycznych wyzwań i rozwiązań.
3. **Materiały edukacyjne**: Opracowanie i udostępnienie materiałów edukacyjnych, takich jak przewodniki, broszury czy infografiki, które wyjaśniają kluczowe koncepcje DPIA i dostarczają wskazówek dotyczących zgodności z RODO.

Przebieg zajęć:

- Część organizacyjna
- Część wprowadzająca
- Część właściwa

KONSPEKT

1. Wprowadzenie do oceny skutków dla ochrony danych (DPIA)

- **Definicja i cel DPIA**: Ocena skutków dla ochrony danych (DPIA) to proces, który ma na celu identyfikację i ocenę ryzyka związanego z przetwarzaniem danych osobowych. Jej celem jest ochrona praw i wolności osób fizycznych oraz zapewnienie zgodności z przepisami RODO.
- **Historia regulacji ochrony danych w UE**: Historia ochrony danych w Unii Europejskiej sięga lat 90., kiedy to wprowadzono Dyrektywę 95/46/WE, która ustanowiła podstawowe zasady ochrony danych. Wraz z rozwojem technologii

i rosnącym znaczeniem danych osobowych, konieczne stało się wprowadzenie bardziej kompleksowego podejścia, co doprowadziło do uchwalenia RODO w 2016 roku.

- **Przejście od dyrektywy 95/46/WE do RODO**: RODO zastąpiło wcześniejszą dyrektywę, wprowadzając bardziej jednolite i rygorystyczne przepisy dotyczące ochrony danych osobowych w całej UE. Nowe przepisy kładą większy nacisk na odpowiedzialność administratorów danych i prawa osób, których dane dotyczą.
- **Zasada risk-based approach**: RODO wprowadza podejście oparte na ryzyku, które wymaga od administratorów danych oceny potencjalnych zagrożeń związanych z przetwarzaniem danych i podjęcia odpowiednich środków zaradczych w celu ich minimalizacji.
- **Zniesienie obowiązku rejestracji zbiorów danych osobowych**: Jednym z kluczowych zmian wprowadzonych przez RODO było zniesienie obowiązku rejestracji zbiorów danych osobowych w krajowych organach ochrony danych, co zmniejszyło biurokrację, ale zwiększyło odpowiedzialność administratorów danych.
- **Rola Grupy Roboczej Art. 29**: Grupa Robocza Art. 29, działająca do czasu powstania Europejskiej Rady Ochrony Danych, była kluczowym organem doradczym w zakresie ochrony danych, dostarczającym wytycznych i opinii dotyczących interpretacji i stosowania przepisów o ochronie danych.

2. Przesłanki przeprowadzenia DPIA

- **Kiedy DPIA jest konieczne?**: DPIA jest konieczne, gdy przetwarzanie danych może prowadzić do wysokiego ryzyka naruszenia praw i wolności osób fizycznych, zwłaszcza w przypadku nowych technologii, przetwarzania na dużą skalę lub systematycznego monitorowania.
- **Ocena ryzyka naruszenia praw lub wolności osób fizycznych**: Proces ten polega na identyfikacji potencjalnych zagrożeń i ocenie ich wpływu na prywatność osób, których dane dotyczą, co pozwala na podjęcie odpowiednich działań zapobiegawczych.
- **Przykłady sytuacji wymagających DPIA**: Przykłady obejmują wdrażanie nowych technologii monitorujących, profilowanie na dużą skalę, przetwarzanie danych wrażliwych oraz systematyczne i kompleksowe przetwarzanie danych.

- **Rola nowych technologii w ocenie ryzyka**: Nowe technologie, takie jak sztuczna inteligencja czy Internet Rzeczy, mogą zwiększać ryzyko naruszenia prywatności, co wymaga szczególnej uwagi podczas przeprowadzania DPIA.
- **Weryfikacja zgodności z przepisami**: DPIA pomaga w zapewnieniu, że przetwarzanie danych jest zgodne z obowiązującymi przepisami, co jest kluczowe dla uniknięcia sankcji i budowania zaufania.
- **Różnice między DPIA a audytem ochrony danych**: DPIA koncentruje się na ocenie ryzyka i zapobieganiu zagrożeniom, podczas gdy audyt ochrony danych ocenia zgodność z politykami i procedurami ochrony danych po fakcie.
- **Wskazówki Grupy Roboczej Art. 29**: Grupa Robocza Art. 29 dostarczała wytycznych dotyczących przeprowadzania DPIA, które pomagają administratorom danych w interpretacji i stosowaniu przepisów RODO.

3. Proces przeprowadzania DPIA

- **Kto jest odpowiedzialny za przeprowadzenie DPIA?**: Odpowiedzialność za przeprowadzenie DPIA spoczywa na administratorze danych, który powinien współpracować z inspektorem ochrony danych oraz innymi zainteresowanymi stronami.
- **Kroki w procesie oceny skutków**: Proces obejmuje identyfikację operacji przetwarzania, ocenę konieczności i proporcjonalności, identyfikację i ocenę ryzyka oraz określenie środków zaradczych.
- **Systematyczny opis operacji przetwarzania**: Należy dokładnie opisać, jakie dane są przetwarzane, w jakim celu, jakie technologie są używane oraz kto jest odpowiedzialny za poszczególne etapy przetwarzania.
- **Ocena konieczności i proporcjonalności przetwarzania**: Ważne jest, aby ocenić, czy przetwarzanie danych jest niezbędne i proporcjonalne do zamierzonych celów, co pozwala na minimalizację zbieranych danych.
- **Identyfikacja i ocena ryzyka**: Proces ten polega na określeniu potencjalnych zagrożeń dla prywatności i ocenie ich prawdopodobieństwa oraz wpływu, co umożliwia podjęcie odpowiednich działań zapobiegawczych.
- **Środki zaradcze i mechanizmy bezpieczeństwa**: W oparciu o ocenę ryzyka należy wprowadzić środki zaradcze, które zminimalizują ryzyko naruszenia praw i wolności osób fizycznych.

- **Konsultacje z inspektorem ochrony danych**: Inspektor ochrony danych powinien być zaangażowany w proces DPIA, aby zapewnić zgodność z przepisami i doradzić w zakresie najlepszych praktyk ochrony danych.

4. DPIA w sektorze publicznym i prywatnym

- **Różnice w obowiązkach administratorów danych**: W sektorze publicznym i prywatnym mogą istnieć różne wymagania dotyczące ochrony danych, co wpływa na zakres i szczegółowość przeprowadzanych DPIA.
- **Przetwarzanie danych na dużą skalę w sektorze publicznym**: Sektor publiczny często przetwarza dane na dużą skalę, co może wymagać bardziej szczegółowych i regularnych ocen skutków dla ochrony danych.
- **Specyfika przetwarzania danych w sektorze prywatnym**: W sektorze prywatnym przetwarzanie danych może być bardziej zróżnicowane i innowacyjne, co wymaga elastycznego podejścia do DPIA.
- **Przykłady przetwarzania danych w sektorze publicznym**: Przykłady obejmują systemy nadzoru wizyjnego, rejestry publiczne oraz systemy identyfikacji obywateli.
- **Wykazy operacji wymagających i niewymagających DPIA**: Administratorzy danych mogą korzystać z wykazów operacji, które wymagają lub nie wymagają przeprowadzenia DPIA, co ułatwia podejmowanie decyzji.
- **Rola Prezesa Urzędu Ochrony Danych Osobowych**: Prezes UODO pełni kluczową rolę w nadzorowaniu zgodności z przepisami ochrony danych i może wydawać zalecenia dotyczące przeprowadzania DPIA.
- **Przypadki, kiedy DPIA nie jest wymagane**: DPIA nie jest wymagane, gdy przetwarzanie danych nie wiąże się z wysokim ryzykiem naruszenia praw i wolności osób fizycznych.

5. Treść i zawartość DPIA

- **Minimalny zakres informacji w DPIA**: DPIA powinno zawierać informacje dotyczące celów przetwarzania, opis operacji przetwarzania, ocenę ryzyka oraz planowane środki zaradcze.
- **Opis celów i operacji przetwarzania**: Należy szczegółowo opisać cele przetwarzania danych oraz operacje, jakie będą wykonywane na danych osobowych.

- **Ocena proporcjonalności i konieczności**: Ważne jest, aby ocenić, czy przetwarzanie danych jest proporcjonalne do zamierzonych celów i czy można je zrealizować w inny, mniej inwazyjny sposób.
- **Identyfikacja ryzyka naruszenia praw**: Proces ten polega na określeniu potencjalnych zagrożeń dla prywatności i ocenie ich prawdopodobieństwa oraz wpływu.
- **Planowane środki zaradcze**: Należy określić środki zaradcze, które zostaną wprowadzone w celu zminimalizowania ryzyka naruszenia praw i wolności osób fizycznych.
- **Dokumentowanie zgodności z RODO**: DPIA powinno dokumentować zgodność z przepisami RODO oraz zapewniać, że wszystkie wymagania są spełnione.
- **Aktualizacja i ponawianie DPIA w trakcie przetwarzania**: DPIA powinno być regularnie aktualizowane w miarę zmiany okoliczności przetwarzania danych, aby zapewnić ciągłą zgodność z przepisami.

SCENARIUSZE ĆWICZEŃ

Scenariusz ćwiczenia 1: Wdrożenie nowej technologii monitorującej

Cel ćwiczenia:

Ocena skutków dla ochrony danych (DPIA) w kontekście wdrożenia nowego systemu monitoringu wizyjnego w przestrzeni publicznej.

Opis sytuacji:

Miasto planuje zainstalować nowoczesny system monitoringu wizyjnego w celu poprawy bezpieczeństwa na ulicach. System ten wykorzystuje zaawansowane technologie rozpoznawania twarzy i analizy zachowań.

Kroki do wykonania:

1. **Identyfikacja operacji przetwarzania**:
    - Opisz, jakie dane będą zbierane (np. obrazy twarzy, ruchy osób).
    - Określ cel przetwarzania danych (np. zwiększenie bezpieczeństwa publicznego).
2. **Ocena konieczności i proporcjonalności**:
    - Oceń, czy system monitoringu jest niezbędny do osiągnięcia zamierzonych celów.
    - Rozważ alternatywne rozwiązania, które mogą być mniej inwazyjne.
3. **Identyfikacja i ocena ryzyka**:

- Zidentyfikuj potencjalne zagrożenia dla prywatności, takie jak nieautoryzowany dostęp do danych.
- Oceń prawdopodobieństwo i wpływ tych zagrożeń.

4. **Środki zaradcze i mechanizmy bezpieczeństwa**:
    - Proponuj środki mające na celu ochronę danych, takie jak szyfrowanie i ograniczenie dostępu.
5. **Konsultacje z inspektorem ochrony danych**:
    - Skonsultuj się z inspektorem ochrony danych w celu uzyskania opinii i zaleceń.

Oczekiwane rezultaty:

- Przygotowanie raportu z DPIA, który zawiera wszystkie powyższe elementy.
- Zidentyfikowanie i wdrożenie środków zaradczych.

Scenariusz ćwiczenia 2: Ocena wpływu nowej aplikacji mobilnej

Cel ćwiczenia:

Ocena skutków dla ochrony danych (DPIA) przed wprowadzeniem na rynek nowej aplikacji mobilnej, która zbiera dane lokalizacyjne użytkowników.

Opis sytuacji:

Firma technologiczna planuje wprowadzenie aplikacji mobilnej, która oferuje spersonalizowane rekomendacje miejsc do odwiedzenia na podstawie lokalizacji użytkownika.

Kroki do wykonania:

1. **Identyfikacja operacji przetwarzania**:
    - Opisz, jakie dane będą zbierane (np. dane lokalizacyjne, preferencje użytkowników).
    - Określ cel przetwarzania danych (np. dostarczanie spersonalizowanych rekomendacji).
2. **Ocena konieczności i proporcjonalności**:
    - Oceń, czy zbieranie danych lokalizacyjnych jest niezbędne dla funkcji aplikacji.
    - Rozważ możliwość zbierania mniej szczegółowych danych.
3. **Identyfikacja i ocena ryzyka**:
    - Zidentyfikuj potencjalne zagrożenia, takie jak nieautoryzowane śledzenie użytkowników.
    - Oceń prawdopodobieństwo i wpływ tych zagrożeń.

4. **Środki zaradcze i mechanizmy bezpieczeństwa**:
    - Proponuj środki ochrony danych, takie jak anonimizacja danych i zgoda użytkowników.
5. **Konsultacje z inspektorem ochrony danych**:
    - Skonsultuj się z inspektorem ochrony danych w celu uzyskania opinii i zaleceń.

Oczekiwane rezultaty:

- Przygotowanie raportu z DPIA, który zawiera wszystkie powyższe elementy.
- Zidentyfikowanie i wdrożenie środków zaradczych przed uruchomieniem aplikacji.

PREZENTACJA 02

Manual dla słuchaczy nr 3

Kwalifikacja rynkowa: OCHRONA DANYCH OSOBOWYCH.

Temat zajęć: Skuteczne zarządzanie dokumentacją przetwarzania danych osobowych zgodnie z RODO

Czas zajęć: 3 godziny

Warunki realizacji:

Praca zbiorowa i w grupach – realizacja nowego materiału

Metody nauczania:

Wykład, pogadanka, burza mózgów, case study, dyskusja.

Cele ogólne:

1. **Zrozumienie podstaw dokumentacji RODO**: Uczestnicy będą potrafili zdefiniować dokumentację przetwarzania danych osobowych i wyjaśnić jej znaczenie dla zgodności z RODO.
2. **Znajomość zasad rozliczalności**: Uczestnicy nauczą się, jak zasada rozliczalności wpływa na prowadzenie i aktualizowanie dokumentacji oraz jakie są jej praktyczne implikacje.

3. **Umiejętność prowadzenia rejestrów czynności przetwarzania**: Uczestnicy będą w stanie samodzielnie przygotować i utrzymywać rejestry czynności przetwarzania zgodnie z wymogami art. 30 RODO.
4. **Tworzenie i wdrażanie polityk ochrony danych**: Uczestnicy zdobędą umiejętność tworzenia efektywnych polityk ochrony danych, które wspierają zgodność z RODO, oraz poznają zasady ich wdrażania.
5. **Zarządzanie incydentami ochrony danych**: Uczestnicy nauczą się, jak skutecznie zarządzać incydentami i naruszeniami ochrony danych, w tym jak dokumentować i zgłaszać naruszenia.

Środki dydaktyczne:

1. **Prezentacje multimedialne**: Prezentacje będą wykorzystywane do przedstawienia teoretycznych aspektów RODO oraz przykładów dokumentacji i polityk.
2. **Warsztaty praktyczne**: Uczestnicy wezmą udział w warsztatach, podczas których będą tworzyć przykładowe rejestry i polityki, co pozwoli na zastosowanie zdobytej wiedzy w praktyce.
3. **Studia przypadków**: Analiza rzeczywistych przypadków naruszeń ochrony danych i ich zarządzania, co pomoże uczestnikom lepiej zrozumieć wyzwania i rozwiązania stosowane w praktyce.

Przebieg zajęć:

- Część organizacyjna
- Część wprowadzająca
- Część właściwa

KONSPEKT

1. **Wprowadzenie do dokumentacji przetwarzania danych osobowych**
    - **Definicja i znaczenie dokumentacji w kontekście RODO**: Omówienie, czym jest dokumentacja przetwarzania danych osobowych i dlaczego jest kluczowa dla zgodności z RODO.

- **Zasada rozliczalności i jej wpływ na dokumentację**: Wyjaśnienie zasady rozliczalności i jak wpływa ona na konieczność prowadzenia i aktualizowania dokumentacji.
- **Obowiązki dokumentacyjne wynikające z RODO**: Przegląd głównych obowiązków dokumentacyjnych, takich jak prowadzenie rejestrów czy dokumentacja naruszeń.
- **Rola polityk ochrony danych w organizacji**: Jak polityki ochrony danych wspierają zgodność z RODO i jakie elementy powinny zawierać.
- **Znaczenie rejestrów czynności przetwarzania**: Dlaczego rejestry są ważne i jak pomagają w zarządzaniu procesami przetwarzania danych.
- **Przykłady dokumentów wspierających zgodność z RODO**: Przegląd różnych dokumentów, takich jak polityki bezpieczeństwa, które wspierają zgodność z przepisami.
- **Wpływ dokumentacji na procesy audytowe**: Jak dobrze prowadzona dokumentacja może ułatwić audyty i kontrole zgodności.
- **Aktualizacja dokumentacji w odpowiedzi na zmiany prawne**: Znaczenie regularnej aktualizacji dokumentacji w kontekście zmieniających się przepisów.

2. **Rejestry przetwarzania danych osobowych**
    - **Czym jest rejestr czynności przetwarzania i jego znaczenie**: Szczegółowe omówienie funkcji rejestru i jego roli w organizacji.
    - **Kluczowe elementy rejestru czynności przetwarzania**: Jakie informacje muszą być zawarte w rejestrze zgodnie z art. 30 RODO.
    - **Różnice między rejestrem czynności a rejestrem kategorii czynności**: Wyjaśnienie, jakie są różnice i kiedy każdy z tych rejestrów jest wymagany.
    - **Przykłady informacji zawartych w rejestrach**: Omówienie typowych danych, które powinny być rejestrowane.
    - **Praktyczne wyzwania w prowadzeniu rejestrów**: Dyskusja na temat trudności, które mogą się pojawić podczas prowadzenia rejestrów, i jak sobie z nimi radzić.
    - **Kiedy rejestry są obligatoryjne, a kiedy fakultatywne**: Wyjaśnienie sytuacji, w których prowadzenie rejestrów jest obowiązkowe.

- **Rola rejestrów w przypadku kontroli organów nadzorczych**: Jak rejestry mogą pomóc w przypadku kontroli przez organy nadzorcze.
- **Narzędzia wspierające prowadzenie rejestrów**: Przegląd narzędzi i oprogramowania, które mogą ułatwić prowadzenie rejestrów.

3. **Polityki ochrony danych osobowych**
    - **Cel i struktura polityk ochrony danych**: Jakie są cele polityk ochrony danych i jak powinny być one zorganizowane.
    - **Zasady tworzenia i wdrażania polityk**: Proces tworzenia efektywnych polityk ochrony danych oraz ich wdrażanie w organizacji.
    - **Elementy polityki ochrony danych: od zgody po retencję**: Szczegółowe omówienie kluczowych elementów polityki ochrony danych.
    - **Przykłady polityk: bezpieczeństwa IT, czystego biurka**: Przegląd różnych typów polityk i ich zastosowania w praktyce.
    - **Polityki ochrony danych a zasada "privacy by design"**: Jak polityki ochrony danych wspierają zasadę ochrony danych w fazie projektowania.
    - **Weryfikacja i audyt polityk ochrony danych**: Jak regularnie sprawdzać i audytować polityki, aby zapewnić ich skuteczność.
    - **Współpraca z inspektorem ochrony danych przy tworzeniu polityk**: Rola inspektora ochrony danych w tworzeniu i wdrażaniu polityk.
    - **Praktyczne wskazówki dotyczące aktualizacji polityk**: Jak i kiedy aktualizować polityki, aby były zgodne z najnowszymi przepisami.
4. **Zarządzanie incydentami i naruszeniami ochrony danych**
    - **Procedury reagowania na incydenty ochrony danych**: Jakie kroki należy podjąć w przypadku incydentu ochrony danych.
    - **Dokumentacja naruszeń: co i jak dokumentować**: Jak prawidłowo dokumentować naruszenia ochrony danych.
    - **Obowiązek zgłaszania naruszeń organowi nadzorczemu**: Kiedy i jak zgłaszać naruszenia do organu nadzorczego.
    - **Wzory zawiadomień dla osób, których dane dotyczą**: Jak przygotować zawiadomienia dla osób, których dane zostały naruszone.
    - **Analiza ryzyka jako element zarządzania incydentami**: Jak analiza ryzyka wspiera zarządzanie incydentami ochrony danych.

- **Rola inspektora ochrony danych w zarządzaniu incydentami**: Jak inspektor ochrony danych może wspierać zarządzanie incydentami.
- **Przykłady incydentów i ich skuteczne zarządzanie**: Studium przypadków incydentów i jak były one zarządzane.
- **Narzędzia wspierające zarządzanie incydentami**: Przegląd narzędzi, które mogą pomóc w zarządzaniu incydentami ochrony danych.

5. **Praktyczne aspekty wdrażania i utrzymywania dokumentacji**
    - **Metodyka przeprowadzania analizy ryzyka**: Jak przeprowadzać analizę ryzyka w kontekście ochrony danych osobowych.
    - **Wdrażanie zasad "data protection by design" i "by default"**: Jak zasady ochrony danych można wdrożyć w praktyce.
    - **Dokumentacja transferów danych do krajów trzecich**: Jak dokumentować transfery danych i jakie są związane z tym obowiązki.
    - **Wzory umów powierzenia przetwarzania danych**: Jak przygotować i stosować wzory umów powierzenia.
    - **Szkolenia pracowników z zakresu ochrony danych**: Jak skutecznie szkolić pracowników w zakresie ochrony danych osobowych.
    - **Monitorowanie i audytowanie zgodności z RODO**: Jak regularnie monitorować i audytować zgodność z RODO.
    - **Współpraca z podmiotami przetwarzającymi dane**: Jak efektywnie współpracować z podmiotami przetwarzającymi dane.
    - **Przyszłe trendy w dokumentacji ochrony danych**: Jakie są przyszłe kierunki rozwoju dokumentacji ochrony danych osobowych.

To szkolenie ma na celu dostarczenie uczestnikom szczegółowej wiedzy i praktycznych umiejętności, które pomogą w skutecznym zarządzaniu dokumentacją przetwarzania danych osobowych, zapewniając zgodność z przepisami RODO.

KONSPEKTY ĆWICZEŃ

1. **Tworzenie rejestru czynności przetwarzania danych**

Cel ćwiczenia: Uczestnicy nauczą się, jak prawidłowo tworzyć i aktualizować rejestr czynności przetwarzania danych osobowych zgodnie z wymogami RODO.

Opis ćwiczenia:

- Uczestnicy zostaną podzieleni na małe grupy i otrzymają opis hipotetycznej organizacji (np. firma IT, szkoła, szpital).
- Każda grupa zidentyfikuje procesy przetwarzania danych w swojej organizacji.
- Grupy stworzą rejestr czynności przetwarzania, uwzględniając takie elementy jak cel przetwarzania, kategorie danych, odbiorcy danych, oraz środki ochrony danych.
- Na koniec każda grupa zaprezentuje swoje rejestry, a prowadzący omówi najczęstsze błędy i najlepsze praktyki.

2. **Reagowanie na incydent ochrony danych**

Cel ćwiczenia: Uczestnicy nauczą się, jak skutecznie zarządzać incydentem ochrony danych, od wykrycia do zgłoszenia i dokumentacji.

Opis ćwiczenia:

- Uczestnicy zostaną podzieleni na zespoły i otrzymają scenariusz incydentu (np. wyciek danych klientów z powodu błędu pracownika).
- Zespoły opracują plan reakcji, który obejmuje identyfikację incydentu, ocenę ryzyka, działania naprawcze oraz komunikację z organem nadzorczym i osobami, których dane dotyczą.
- Każdy zespół przedstawi swój plan działania, a prowadzący omówi kluczowe elementy skutecznego zarządzania incydentami i odpowie na pytania uczestników.

Te scenariusze ćwiczeń mają na celu rozwijanie praktycznych umiejętności uczestników w zakresie zarządzania dokumentacją i incydentami ochrony danych osobowych, co jest kluczowe dla zgodności z RODO.

PREZENTACJA 03

Manual dla słuchaczy nr 4

Kwalifikacja rynkowa: OCHRONA DANYCH OSOBOWYCH.

Temat zajęć: Profilowanie i automatyczne podejmowanie decyzji w kontekście RODO

Czas zajęć: 3 godziny

Warunki realizacji:

Praca zbiorowa i w grupach – realizacja nowego materiału

Metody nauczania:

Wykład, pogadanka, burza mózgów, case study, dyskusja.

Cele ogólne:

1. Zrozumienie RODO i jego znaczenia - Uczestnicy będą potrafili wyjaśnić, czym jest RODO, jakie są jego główne cele oraz jak wpływa na ochronę danych osobowych.
2. Identyfikacja ryzyk związanych z profilowaniem - Uczestnicy będą w stanie zidentyfikować i omówić potencjalne ryzyka i zagrożenia związane z profilowaniem i zautomatyzowanym podejmowaniem decyzji.
3. Praktyczne zastosowanie przepisów RODO - Uczestnicy nauczą się, jak stosować przepisy art. 22 RODO w praktyce oraz jakie są wyjątki od zakazu zautomatyzowanego podejmowania decyzji.
4. Rozpoznawanie środków ochrony danych - Uczestnicy będą potrafili wskazać i opisać środki ochrony danych osobowych, które mogą być stosowane w kontekście profilowania i automatyzacji.
5. Krytyczna analiza przypadków - Uczestnicy nabędą umiejętność krytycznej analizy rzeczywistych przypadków zastosowania profilowania i automatyzacji w różnych sektorach, oceniając ich zgodność z RODO.

Środki dydaktyczne:

1. Prezentacje multimedialne - Wykorzystanie prezentacji multimedialnych do wizualizacji kluczowych pojęć i przepisów związanych z RODO, profilowaniem i automatyzacją.
2. Studia przypadków - Analiza rzeczywistych przypadków i scenariuszy, które pomogą uczestnikom zrozumieć praktyczne zastosowanie przepisów RODO oraz związane z nimi wyzwania.
3. Dyskusje grupowe - Organizowanie dyskusji w małych grupach, które pozwolą uczestnikom wymieniać się poglądami i doświadczeniami, a także wspólnie rozwiązywać problemy związane z ochroną danych osobowych.

Przebieg zajęć:

- Część organizacyjna
- Część wprowadzająca
- Część właściwa

KONSPEKT

1. Wprowadzenie do tematu

1. **Znaczenie RODO** - Omówienie ogólnych celów RODO i jego znaczenia dla ochrony danych osobowych.
2. **Definicja profilowania** - Wyjaśnienie, czym jest profilowanie w kontekście RODO, oraz jak wpływa na przetwarzanie danych osobowych.
3. **Automatyczne podejmowanie decyzji** - Omówienie, co oznacza automatyczne podejmowanie decyzji i jak różni się od profilowania.
4. **Przykłady zastosowań** - Przedstawienie przykładów z życia codziennego, gdzie stosowane jest profilowanie i automatyczne podejmowanie decyzji.
5. **Ryzyka związane z automatyzacją** - Dyskusja na temat potencjalnych zagrożeń związanych z automatycznym podejmowaniem decyzji, takich jak dyskryminacja czy naruszenie prywatności.
6. **Zasady ochrony danych** - Omówienie podstawowych zasad RODO dotyczących ochrony danych osobowych.
7. **Cele zajęć** - Przedstawienie celów edukacyjnych i oczekiwanych rezultatów uczestnictwa w zajęciach.

2. Artykuł 22 RODO: Prawo do niepodlegania zautomatyzowanym decyzjom

1. **Treść artykułu 22** - Szczegółowe omówienie zapisów artykułu 22 RODO.
2. **Warunki zastosowania** - Wyjaśnienie, kiedy można stosować zautomatyzowane podejmowanie decyzji zgodnie z RODO.
3. **Skutki prawne** - Dyskusja na temat skutków prawnych decyzji opartych na automatycznym przetwarzaniu.
4. **Istotny wpływ na osobę** - Analiza, co oznacza istotny wpływ na osobę w kontekście RODO.

5. **Wyjątki od zakazu** - Omówienie sytuacji, w których zautomatyzowane podejmowanie decyzji jest dozwolone.
6. **Środki ochrony prawnej** - Przedstawienie dostępnych środków ochrony dla osób, których dane dotyczą.
7. **Przykłady z praktyki** - Analiza rzeczywistych przypadków zastosowania artykułu 22.

3. Profilowanie a ochrona danych osobowych

1. **Definicja i zakres** - Szczegółowe wyjaśnienie, co obejmuje profilowanie według RODO.
2. **Zastosowanie w praktyce** - Przykłady branż i sytuacji, gdzie profilowanie jest powszechnie stosowane.
3. **Ryzyka związane z profilowaniem** - Dyskusja na temat ryzyk, takich jak utrwalanie stereotypów czy ograniczenie wolności wyboru.
4. **Przepisy RODO dotyczące profilowania** - Omówienie, jakie przepisy RODO regulują profilowanie.
5. **Środki ochrony prawnej** - Jakie środki ochrony przysługują osobom, których dane są profilowane.
6. **Profilowanie dzieci** - Specyfika i ograniczenia dotyczące profilowania dzieci według RODO.
7. **Przykłady profilowania w sektorze publicznym i prywatnym** - Analiza przypadków, gdzie profilowanie jest wykorzystywane w różnych sektorach.

4. Zautomatyzowane podejmowanie decyzji w praktyce

1. **Przykłady zastosowań** - Omówienie, jak zautomatyzowane podejmowanie decyzji jest stosowane w różnych branżach.
2. **Technologie wspierające** - Przegląd technologii, które umożliwiają automatyzację decyzji.
3. **Przypadki naruszeń** - Analiza przypadków, gdzie automatyzacja decyzji prowadziła do naruszeń praw.
4. **Rola sztucznej inteligencji** - Jak AI wpływa na procesy decyzyjne i jakie stwarza wyzwania.
5. **Przykłady dobrych praktyk** - Przedstawienie przykładów, gdzie automatyczne podejmowanie decyzji jest stosowane zgodnie z RODO.
6. **Środki zapobiegawcze** - Jakie środki można wdrożyć, aby zminimalizować ryzyka związane z automatyzacją.

7. **Dyskusja grupowa** - Interaktywna sesja, gdzie uczestnicy omawiają potencjalne zastosowania i wyzwania.

5. Środki ochrony danych osobowych w kontekście profilowania i automatyzacji

1. **Zasady ochrony danych** - Omówienie kluczowych zasad RODO dotyczących ochrony danych.
2. **Prawo do sprzeciwu** - Wyjaśnienie, jak osoby mogą sprzeciwić się profilowaniu i automatycznym decyzjom.
3. **Interwencja ludzka** - Znaczenie interwencji ludzkiej w procesach automatycznych.
4. **Przejrzystość procesów** - Jak zapewnić przejrzystość w procesach profilowania i automatyzacji.
5. **Zgoda na przetwarzanie danych** - Kiedy i jak należy uzyskać zgodę na zautomatyzowane przetwarzanie.
6. **Ocena skutków dla ochrony danych** - Jak przeprowadzać ocenę skutków dla ochrony danych w kontekście profilowania.
7. **Przykłady implementacji** - Przykłady, jak firmy wdrażają środki ochrony danych w praktyce.

6. Podsumowanie i wnioski

1. **Podsumowanie kluczowych punktów** - Przegląd najważniejszych informacji omówionych podczas zajęć.
2. **Wnioski uczestników** - Zachęcenie uczestników do podzielenia się swoimi wnioskami i przemyśleniami.
3. **Pytania i odpowiedzi** - Sesja pytań i odpowiedzi, aby wyjaśnić wszelkie wątpliwości.
4. **Przyszłość profilowania i automatyzacji** - Dyskusja na temat przyszłych trendów i wyzwań.
5. **Rola regulacji prawnych** - Jak regulacje prawne mogą ewoluować, aby lepiej chronić dane osobowe.
6. **Zasoby i materiały** - Przekazanie uczestnikom dodatkowych materiałów i zasobów do samodzielnej nauki.
7. **Zakończenie** - Podziękowanie uczestnikom za udział i zachęcenie do dalszego zgłębiania tematu.

KONSPKETY ĆWICZEŃ

Scenariusz ćwiczenia 1: Analiza przypadku

Cel ćwiczenia: Uczestnicy nauczą się identyfikować potencjalne naruszenia RODO w kontekście profilowania i automatycznego podejmowania decyzji oraz proponować odpowiednie środki zaradcze.

Opis ćwiczenia:

1. **Podział na grupy:** Uczestnicy zostaną podzieleni na małe grupy (3-5 osób).
2. **Przedstawienie przypadku:** Każda grupa otrzymuje opis rzeczywistego przypadku, w którym firma wykorzystuje profilowanie i automatyczne podejmowanie decyzji w swoich procesach biznesowych (np. przyznawanie kredytów).
3. **Analiza przypadku:** Grupy analizują przypadek, identyfikując:
    - Jakie dane osobowe są zbierane i przetwarzane?
    - Czy i w jaki sposób naruszane są przepisy RODO?
    - Jakie ryzyka dla praw i wolności osób fizycznych mogą wystąpić?
4. **Propozycja rozwiązań:** Grupy opracowują propozycje środków zaradczych lub zmian w procesach, które mogłyby zwiększyć zgodność z RODO.
5. **Prezentacja wyników:** Każda grupa prezentuje swoje wnioski i propozycje na forum, po czym następuje dyskusja moderowana przez prowadzącego.

Scenariusz ćwiczenia 2: Symulacja audytu RODO

Cel ćwiczenia: Uczestnicy zdobędą praktyczne umiejętności w zakresie przeprowadzania audytu zgodności z RODO w kontekście profilowania i automatyzacji.

Opis ćwiczenia:

1. **Podział na role:** Uczestnicy zostają podzieleni na zespoły, gdzie każdy członek zespołu pełni inną rolę (np. audytor, specjalista ds. ochrony danych, przedstawiciel działu IT, przedstawiciel działu marketingu).
2. **Przygotowanie do audytu:** Zespoły przygotowują się do przeprowadzenia audytu w fikcyjnej firmie, która stosuje profilowanie klientów w swoich działaniach marketingowych.

3. **Przeprowadzenie audytu:** Każdy zespół analizuje dostępne dokumenty, procedury i praktyki firmy, identyfikując obszary zgodności i niezgodności z RODO.
4. **Raport z audytu:** Zespoły opracowują raport z audytu, zawierający:
    - Identyfikację niezgodności z RODO.
    - Rekomendacje dotyczące wdrożenia środków poprawiających zgodność z przepisami.
5. **Omówienie wyników:** Zespoły prezentują swoje raporty na forum, a następnie uczestniczą w dyskusji, podczas której mogą wymieniać się spostrzeżeniami i doświadczeniami z ćwiczenia.

PREZENTACJA 04

Manual dla słuchaczy nr 5

Kwalifikacja rynkowa: OCHRONA DANYCH OSOBOWYCH.

Temat zajęć: Ocena skutków dla ochrony danych (DPIA) w praktyce: zasady, proces i wdrożenie

Czas zajęć: 3 godziny

Warunki realizacji:

Praca zbiorowa i w grupach – realizacja nowego materiału

Metody nauczania:

Wykład, pogadanka, burza mózgów, case study, dyskusja.

Cele ogólne:

1. Zrozumienie DPIA - Uczestnicy będą w stanie zdefiniować ocenę skutków dla ochrony danych (DPIA) oraz zrozumieć jej znaczenie i zastosowanie w kontekście RODO.
2. Proces przeprowadzania DPIA - Uczestnicy nauczą się, jak krok po kroku przeprowadzić DPIA, w tym identyfikować ryzyka, oceniać ich prawdopodobieństwo i wpływ oraz wdrażać środki zaradcze.

3. Współpraca i konsultacje - Uczestnicy zdobędą umiejętność efektywnej współpracy z inspektorami ochrony danych, organami nadzorczymi oraz innymi działami w organizacji podczas procesu DPIA.
4. Zarządzanie ryzykiem - Uczestnicy będą potrafili identyfikować zagrożenia związane z przetwarzaniem danych, oceniać ryzyko oraz stosować odpowiednie strategie jego minimalizacji.
5. Adaptacja do nowych technologii - Uczestnicy zdobędą wiedzę na temat wpływu nowych technologii, takich jak AI i IoT, na proces DPIA oraz jak dostosować się do przyszłych regulacji i wyzwań.

Środki dydaktyczne:

1. **Prezentacje multimedialne** - Wykorzystanie prezentacji w celu wizualizacji kluczowych pojęć i procesów związanych z DPIA, co ułatwi uczestnikom przyswajanie wiedzy.
2. **Studia przypadków** - Analiza rzeczywistych przykładów przeprowadzania DPIA, co pomoże uczestnikom zrozumieć praktyczne aspekty i zastosowanie teorii w rzeczywistości.
3. **Warsztaty interaktywne** - Organizacja warsztatów, podczas których uczestnicy będą mogli samodzielnie przećwiczyć proces DPIA, co pozwoli na praktyczne zastosowanie zdobytej wiedzy i umiejętności.

Przebieg zajęć:

- Część organizacyjna
- Część wprowadzająca
- Część właściwa

KONSPEKT

Punkt 1: Wprowadzenie do DPIA

1. **Definicja DPIA** - Omówienie, czym jest ocena skutków dla ochrony danych i jej znaczenie w kontekście RODO.

2. **Podstawy prawne** - Przegląd przepisów RODO dotyczących DPIA, w tym art. 35.
3. **Cel przeprowadzania DPIA** - Dlaczego DPIA jest kluczowym elementem ochrony danych?
4. **Kiedy DPIA jest wymagana?** - Identyfikacja sytuacji, w których przeprowadzenie DPIA jest obligatoryjne.
5. **Rola administratora danych** - Obowiązki administratora w procesie DPIA.
6. **Zasada ochrony danych w fazie projektowania** - Jak DPIA wpisuje się w tę zasadę?
7. **Przykłady zastosowań** - Praktyczne przykłady sytuacji wymagających DPIA.

Punkt 2: Proces przeprowadzania DPIA

1. **Kroki w procesie DPIA** - Szczegółowy opis etapów oceny skutków.
2. **Opis operacji przetwarzania** - Jak dokładnie opisać planowane operacje przetwarzania?
3. **Ocena niezbędności i proporcjonalności** - Jak ocenić te aspekty w kontekście przetwarzania danych?
4. **Identyfikacja ryzyk** - Jakie ryzyka mogą wynikać z przetwarzania danych?
5. **Środki zaradcze** - Jakie środki można wdrożyć, aby zminimalizować ryzyko?
6. **Dokumentowanie wyników** - Znaczenie dokumentacji w procesie DPIA.
7. **Przykłady narzędzi DPIA** - Przegląd dostępnych narzędzi wspierających proces oceny skutków.

Punkt 3: Konsultacje i współpraca

1. **Rola inspektora ochrony danych** - Jak inspektor ochrony danych wspiera proces DPIA?
2. **Konsultacje z organem nadzorczym** - Kiedy i jak konsultować się z organem nadzorczym?

3. **Zasięganie opinii podmiotów danych** - Kiedy i jak zasięgać opinii osób, których dane dotyczą?
4. **Współpraca z procesorami danych** - Jak współpracować z podmiotami przetwarzającymi dane?
5. **Interdyscyplinarne podejście** - Znaczenie współpracy różnych działów w organizacji.
6. **Przykłady dobrych praktyk** - Praktyczne wskazówki dotyczące współpracy.
7. **Rozwiązywanie konfliktów** - Jak radzić sobie z różnicami w opiniach i podejściach?

Punkt 4: Analiza ryzyka i zarządzanie nim

1. **Identyfikacja zagrożeń** - Jakie zagrożenia mogą wystąpić w procesie przetwarzania danych?
2. **Ocena prawdopodobieństwa i wpływu** - Jak ocenić prawdopodobieństwo i wpływ zagrożeń?
3. **Strategie zarządzania ryzykiem** - Jakie strategie można zastosować do zarządzania ryzykiem?
4. **Przykłady ryzyk wysokiego poziomu** - Omówienie typowych ryzyk związanych z przetwarzaniem danych.
5. **Metody minimalizacji ryzyka** - Jakie metody mogą pomóc w zminimalizowaniu ryzyka?
6. **Monitorowanie i przegląd ryzyka** - Jak monitorować i regularnie przeglądać ryzyko?
7. **Case study** - Analiza rzeczywistego przypadku zarządzania ryzykiem.

Punkt 5: Dokumentacja i zgodność z RODO

1. **Zasada rozliczalności** - Jak dokumentacja DPIA wspiera zasadę rozliczalności?
2. **Elementy dokumentacji DPIA** - Co powinno znaleźć się w dokumentacji?

3. **Przechowywanie i dostęp do dokumentacji** - Jak prawidłowo przechowywać dokumentację DPIA?
4. **Audyt i przegląd** - Jak przeprowadzać audyty i przeglądy zgodności DPIA?
5. **Przykłady dokumentacji** - Przegląd przykładowych dokumentów DPIA.
6. **Zarządzanie zmianami** - Jak zarządzać zmianami w procesie przetwarzania danych?
7. **Komunikacja wewnętrzna** - Jak skutecznie komunikować wyniki DPIA w organizacji?

Punkt 6: Przyszłość DPIA i nowe technologie

1. **Wpływ nowych technologii** - Jak nowe technologie wpływają na proces DPIA?
2. **Sztuczna inteligencja i DPIA** - Jak AI zmienia podejście do oceny skutków dla ochrony danych?
3. **Big Data i IoT** - Wyzwania związane z dużymi zbiorami danych i Internetem Rzeczy.
4. **Przetwarzanie transgraniczne** - Jak radzić sobie z wyzwaniami przetwarzania danych poza UE?
5. **Przyszłe regulacje** - Jakie nowe regulacje mogą wpłynąć na proces DPIA?
6. **Innowacyjne podejścia** - Nowe metody i narzędzia wspierające DPIA.
7. **Warsztaty i szkolenia** - Jakie szkolenia mogą pomóc w lepszym zrozumieniu i wdrożeniu DPIA?

SCENARIUSZE ĆWICZEŃ

cenariusz ćwiczenia 1: Analiza ryzyka w kontekście DPIA

Cel ćwiczenia: Uczestnicy nauczą się identyfikować i oceniać ryzyka związane z przetwarzaniem danych osobowych oraz proponować odpowiednie środki zaradcze.

Przebieg ćwiczenia:

1. **Wprowadzenie do scenariusza:**
    - Przedstawienie fikcyjnej firmy, która planuje wdrożyć nowy system CRM do zarządzania danymi klientów.
    - Omówienie podstawowych operacji przetwarzania danych w nowym systemie.
2. **Identyfikacja ryzyk:**
    - Uczestnicy w grupach analizują potencjalne ryzyka związane z przetwarzaniem danych w nowym systemie.
    - Każda grupa sporządza listę zagrożeń, takich jak nieautoryzowany dostęp do danych, błędy w przetwarzaniu danych, czy brak zgodności z RODO.
3. **Ocena prawdopodobieństwa i wpływu:**
    - Grupy oceniają prawdopodobieństwo wystąpienia każdego zidentyfikowanego ryzyka oraz jego potencjalny wpływ na ochronę danych osobowych.
    - Wyniki oceny są przedstawiane na macierzy ryzyka.
4. **Propozycja środków zaradczych:**
    - Uczestnicy opracowują propozycje środków zaradczych, które mogą zminimalizować zidentyfikowane ryzyka.
    - Każda grupa prezentuje swoje propozycje na forum, a wyniki są dyskutowane.

Scenariusz ćwiczenia 2: Opracowanie dokumentacji DPIA

Cel ćwiczenia: Uczestnicy nauczą się tworzyć dokumentację DPIA, uwzględniając wszystkie niezbędne elementy zgodne z RODO.

Przebieg ćwiczenia:

1. **Wprowadzenie do zadania:**

- Uczestnicy otrzymują opis projektu polegającego na wdrożeniu aplikacji mobilnej do zarządzania zdrowiem pacjentów.
- Omówienie kluczowych aspektów przetwarzania danych w aplikacji, w tym typów zbieranych danych i celów przetwarzania.

2. **Opis operacji przetwarzania:**
    - Każda grupa szczegółowo opisuje operacje przetwarzania danych, uwzględniając kategorie danych osobowych, cele przetwarzania i odbiorców danych.
3. **Ocena niezbędności i proporcjonalności:**
    - Uczestnicy oceniają, czy przetwarzanie danych jest niezbędne i proporcjonalne do osiągnięcia zamierzonych celów, oraz jak dane są chronione.
4. **Dokumentowanie wyników:**
    - Grupy przygotowują przykładową dokumentację DPIA, zawierającą opis operacji, ocenę ryzyk, środki zaradcze oraz wnioski.
    - Każda grupa prezentuje swoją dokumentację, a następnie omawiane są mocne strony i obszary do poprawy.

PREZENTACJA 05