TYTUŁ:

„RODO w firmie – praktyczna ochrona danych osobowych”

CEL EDUKACYJNY

Celem szkolenia jest podniesienie kompetencji uczestników w zakresie spełniania wymogów rozporządzenia RODO a w szczególności:

1. pojęć dotyczących danych osobowych i ich ochrony,
2. określania kluczowych zasad RODO, dotyczących zgodnego z prawem przetwarzania danych osobowych,
3. praw osób, których dane dotyczą i sposobu ich zapewniania,
4. polityki i metod działania organizacji, które powinny zawierać zestaw podstawowych środków technicznych i organizacyjnych,
5. reagowania na naruszenia danych i konsekwencje nieprzestrzegania przepisów o ochronie danych,
6. świadomości aktualnych cyberzagrożeń,
7. świadomości wartości i znaczenia posiadanych informacji przez firmę oraz jej pracowników oraz konsekwencji wystąpienia incydentów bezpieczeństwa,
8. sposobów skutecznego zabezpieczania dokumentacji i systemów informatycznych.

Uczestnicy nabędą umiejętności pozwalające im stosować w praktyce wymagania RODO w organizacji oraz poznają konsekwencje niezgodnego z prawem przetwarzania danych osobowych a także zapoznają się – na licznych przykładach – z podstawowymi zasadami bezpiecznego przetwarzania danych osobowych. Uczestnicy zdobędą wiedzę niezbędną do skutecznej ochrony informacji (w tym danych osobowych) i bezpiecznego jej przetwarzania w organizacji.

Szkolenie oprócz wykładu jest prowadzone także w formie warsztatowej z licznymi case studies, co przyczyni się pośrednio także do rozwinięcia kompetencji społecznych w zakresie komunikacji poprzez wspólną analizę przypadków, współpracę w grupie.

RAMOWY PROGRAM USŁUGI

DZIEŃ I

„RODO - praktyczne aspekty europejskiego rozporządzenia o ochronie danych osobowych”

1) RODO – OBOWIĄZKI I KORZYŚCI
   - Obowiązki informacyjne dla osób fizycznych, których dane osobowe przetwarzamy;
   - Przetwarzanie danych osobowych: ogólne zasady przetwarzania danych osobowych, przetwarzanie danych osobowych szczególnych kategorii, warunki i zasady uzyskiwania, przechowywania zgody osoby fizycznej, w tym w zakresie przetwarzanie danych osobowych dzieci.
2) PRAWA I OBOWIĄZKI
   - Prawa przysługujące osobom fizycznym, których dane osobowe przetwarzamy m.in. prawo do bycia zapomnianym, prawo do przenoszenia danych do innych podmiotów,
   - Obowiązki administratorów danych: obowiązek rejestrowania czynności przetwarzania danych osobowych, zgłaszania naruszeń ochrony danych osobowych.
3) KONSEKWENCJE PRAWNE NIESTOSOWANIA ROZPORZĄDZENIA RODO
   - Sankcje za nieprzestrzeganie przepisów rozporządzenia: administracyjne kary pieniężne – warunki ich nakładania i wysokość, odszkodowanie za poniesioną szkodę
   - Organ nadzorczy (Prezes UODO): rola, status, zadania i uprawienia
4) PRAWA I OBOWIĄZKI
   - Obowiązki informacyjne dla pracowników/zleceniobiorców, których dane osobowe przetwarzamy
   - Prawa przysługujące pracownikom/zleceniobiorcom, których dane osobowe przetwarzamy: prawo do bycia zapomnianym, prawo do przenoszenia danych do innych podmiotów, prawo do niepodlegania profilowaniu, zasada przejrzystości i inne wymogi informacyjne dla naszych pracowników i zleceniobiorców.
5) WYMOGI DOTYCZĄCE PRACOWNIKÓW, ZLECENIOBIORCÓW
   - Dostosowanie organizacji do zasad wymaganych RODO w zakresie danych pracowników, zleceniobiorców:
   - ograniczenia przechowywania, bezpieczeństwa danych.
   - Wymogi dotyczące przetwarzania danych w procesie rekrutacji pracowników – przechowywanie danych, klauzule w dokumentach CV, profilowanie danych;
6) WYMOGI DOTYCZĄCE PRACOWNIKÓW, ZLECENIOBIORCÓW cd.
   - Obowiązki informacyjne pracodawcy względem pracowników, zleceniobiorców w aspekcie rekrutacji, zatrudnienia i po zatrudnieniu;
   - Zabezpieczenie danych osobowych pracowników i prawo dostępu do własnych danych osobowych;
   - Dane wrażliwe pracowników, zleceniobiorców, w tym przynależności do związku zawodowego; badania lekarskie, w tym psychologiczne, szkolenia BHP, w tym zasady przetwarzania danych biometrycznych;
7) PYTANIA I OMÓWIENIE PRZYKŁADÓW, DYSKUSJA

Dzień II

„RODO - ochrona danych osobowych i cyberzagrożenia”

8) BEZPIECZEŃSTWO INFORMACJI
   - Bezpieczeństwo informacji w firmie – założenia, dobre praktyki

- Czy pracownik jest najsłabszym ogniwem?
- Jak budować kulturę ochrony informacji?
- Przykłady ataków, kradzieży i wycieku danych. Czy Twoją firmę to też może spotkać?

9) ZAGROŻENIA DLA OCHRONY DANYCH OSOBOWYCH
   - Aktualne zagrożenia np. phishing / ransomware / ataki ukierunkowane …
   - Cyberzagrożenia: poczta e-mail, strony www, serwisy społecznościowe
   - Hasła do systemów informatycznych. Jak je chronić i tworzyć, aby były bezpieczne
   - Etyczny hacking
10) OCHRONA PRZED ATAKAMI
   - Proste i skuteczne sposoby codziennej ochrony informacji
   - Metody ochrony przed phishingiem - przykłady
   - Bezpieczne korzystanie z poczty e-mail
   - Pendrive od znajomego – prezent czy zagrożenie?
11) ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI
   - Polityka Bezpieczeństwa Informacji i Ochrony Danych Osobowych (PBI) – skuteczne narzędzie codziennej ochrony.
   - PBI: Jak skutecznie wdrożyć?
   - PBI: Przykładowe procedury
12) PYTANIA I OMÓWIENIE PRZYKŁADÓW, DYSKUSJA

EFEKTY USŁUGI (PRODUKTY), EFEKTY UCZENIA SIĘ/KSZTAŁCENIA

Uczestnik po zakończeniu kursu:

1. Opisuje podstawowe cele Rozporządzenia RODO.
2. Wyjaśnia pojęcia: prywatność i związane z nim prawa, dane osobowe, przetwarzanie danych, ochrona danych, automatyczne i ręczne przetwarzanie danych, naruszenie danych osobowych.
3. Rozpoznaje zagrożenia dla przetwarzania danych osobowych, takie jak: przypadkowe lub bezprawne zniszczenie, utrata, zmiana, nieautoryzowane ujawnienie, nieautoryzowany dostęp.
4. Określa zasady: legalności, uczciwości i danych osobowych, przejrzystości. ograniczenia celu przetwarzania, minimalizacji danych, rzetelności przetwarzania, integralności, poufności i rozliczalności.
5. Wskazuje warunki, w których przetwarzanie danych osobowych jest zgodne z wymaganiami i prawem.
6. Wskazuje, że administrator danych powinien zgłaszać przypadki naruszenia danych osobowych osób, których dane dotyczą, jeżeli istnieje wysokie ryzyko dla ich praw i wolności.
7. Rozróżnia pseudonimizację i anonimizację danych osobowych
8. Posiada praktyczną wiedzę dotyczącą aktualnych cyberzagrożeń i typów ataków.
9. Ma świadomość wartości i znaczenia posiadanych informacji przez firmę oraz jej pracowników oraz konsekwencji wystąpienia incydentów bezpieczeństwa.
10. Zna podstawowe, skuteczne metody zabezpieczania dokumentacji i systemów informatycznych.
11. Identyfikuje podstawowe zagrożenia dla bezpieczeństwa informacji w cyberprzestrzeni takie jak phishing i ransomware

12. Zna metody poprawy cyberbezpieczeństwa poprzez wprowadzenie lub udoskonalenie standardów ochrony informacji i danych osobowych.

GRUPA DOCELOWA

przedsiębiorcy, pracownicy

HARMONOGRAM

LP	Przedmiot / Temat zajęć	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1.	Dzień 1.	2023-xx-xx	09:00	??:00	??
2.	Dzień 2.	2023-xx-xx	09:00	??:00	??

OSOBY PROWADZĄCE USŁUGĘ

Imię i nazwisko	**Urszula Giercarz**
Obszar specjalizacji	prawnik, specjalistka w ochronie danych osobowych.
Doświadczenie zawodowe	Ponad 8 letnie doświadczenie jako prawnik, specjalizujący się w obsłudze przedsiębiorstw i spółek handlowych. Specjalista z dziedziny ochrony danych osobowych. Inspektor Ochrony Danych Osobowych.
Doświadczenie w świadczeniu tego typu usług	Praktyczna wiedza zebrana w trakcie licznych wdrożeń RODO w firmach z wielu gałęzi gospodarczych. Wiedzę teoretyczną zdobyła w trakcie szkoleń jak również w trakcie pracy w kancelarii prawnej Anny Giercarz. Posiada doświadczenie w prowadzeniu szkoleń z zakresu ochrony danych osobowych.
Wykształcenie	Uniwersytet im. Adama Mickiewicza w Poznaniu, kierunek prawo;

Imię i nazwisko	**Arkadiusz Stawczyk**
Obszar specjalizacji	Bezpieczeństwo informacji i cyberzagrożenia
Doświadczenie zawodowe	- trener, doradca i kierownik projektów. Specjalista w dziedzinie bezpieczeństwa informacji. Audytor wiodący ISO/IEC 27001:2017 oraz egzaminator ECDL. Członek Polskiego Towarzystwa Informatycznego.
Doświadczenie w świadczeniu tego typu usług	Doradza firmom i jednostkom administracji publicznej m.in. z zakresu ochrony informacji (tworzenie polityk bezpieczeństwa i procedur). Jest autorem licznych instrukcji i procedur związanych z ochroną danych osobowych i informacji. W zakresie szkoleń specjalizuje się w tematach związanych z informatyzacją administracji publicznej, cyberzagrożeniami, bezpieczeństwem informacji i ochroną danych osobowych (RODO).
Wykształcenie	Absolwent Wyższej Szkoły Inżynierskiej w Zielonej Górze, kierunek matematyka.