OFERTA SZKOLENIA ZAMKNIĘTEGO

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

RODO - PODSTAWOWE ZASADY. CO TRZEBA WIEDZIEĆ ABY PRAWIDŁOWO CHRONIĆ DANE OSOBOWE?

CELE I KORZYŚCI:

Przypomnienie uczestnikom podstawowych obowiązków nałożonych na Administratorów Danych, omówienie najczęściej występujących problemów z wdrożeniem w jednostkach przepisów RODO oraz stosowaniem ich w praktyce, w bieżącej działalności podmiotu. Prezentacja dotychczasowych interpretacji i zaleceń wydanych przez Urząd Ochrony Danych Osobowych.

Przedstawienie podstawowych wymagań związanych z organizacją skutecznego systemu ochrony danych osobowych.

Omówienie typowych błędów popełnianych przez Administratorów Danych, które skutkują skargami składanymi przez klientów i interesantów do Urzędu Ochrony Danych Osobowych lub jako naruszenia ochrony danych wymagają zgłoszenia do Prezesa UODO.

Wymiana doświadczeń pomiędzy uczestnikami szkolenia, możliwość konsultacji i uzyskania eksperckich porad w zakresie wątpliwości związanych z ochroną danych osobowych.

PROGRAM:

1. System prawa ochrony danych osobowych po wejściu w życie rozporządzenia RODO.
2. Zakres podmiotowy i przedmiotowy RODO.
3. Podstawowe pojęcia z zakresu ochrony danych osobowych:
   a) Dane osobowe.
   b) Przetwarzanie danych.
   c) Profilowanie danych.
   d) Pseudonimizacja i anonimizacja danych.
   e) Zbiór danych.
   f) Administrator danych osobowych (ADO).
   g) Inspektor ochrony danych (DPO/IOD).
   h) Osoba upoważniona do przetwarzania danych.
4. Ogólne zasady przetwarzania danych na gruncie RODO.
   a) Legalności i Przejrzystości.
   b) Celowości.
   c) Adekwatności.
   d) Merytorycznej poprawności.
   e) Ograniczenia czasowego.
   f) Poufności i integralności danych.
   g) Rozliczalności.
5. Prawa osób, których dane dotyczą - zasady realizacji uprawnień, obowiązki i procedury.
   a) Prawo do przejrzystości danych.
   b) Prawo dostępu do danych.
   c) Prawo do sprostowania i usunięcia danych.
   d) Prawo do ograniczenia przetwarzania.
   e) Prawo do przenoszenia danych.
   f) Prawo do sprzeciwu.
   g) Prawa związane z profilowaniem danych.
   h) Prawo skargi do organu nadzorczego.
6. Organizacja systemu ochrony danych – podstawowe obowiązki Administratora Danych:
   a) Powołanie Inspektora Ochrony Danych,
   b) Stosowanie mechanizmów ochrony danych (privacy by design, privacy by default).
   c) Rejestrowanie czynności przetwarzania danych.
   d) Zgłaszanie naruszeń ochrony danych do organu nadzorczego.
   e) Zawiadamianie osób, których dane dotyczą o naruszeniach.
   f) Zabezpieczenie danych osobowych (wewnętrzne polityki, techniczne i organizacyjne środki ochrony danych, zapewnienie poufności, integralności, dostępności).
   g) Zapewnienie ciągłości działania.
   h) Testowanie, mierzenie i ocena skuteczności ochrony danych.
   i) Ocena skutków dla ochrony danych.
   j) Szacowanie ryzyka.
   k) Obowiązki związane z powierzeniem danych.
7. Podstawy prawne legalizujące przetwarzanie danych osobowych w procesach kadrowych:
   a) Przesłanki prawne legalizujące przetwarzanie danych osobowych zwykłych, szczególnych kategorii danych oraz danych na temat karalności (art. 6, 9 i 10 RODO).
   b) Warunki korzystania ze zgody pracownika przez pracodawcę.
8. Procesy rekrutacji i naboru:

PROWADZĄCY:

Absolwent UMK w Toruniu oraz studiów podyplomowych WSAiB w Gdyni na kierunku zarządzanie bezpieczeństwem informacji, certyfikowany Inspektor Ochrony Danych, Menedżer Bezpieczeństwa Informacji oraz Auditor wewnętrzny systemu zarządzania bezpieczeństwem informacji. W latach 1992 - 2013 funkcjonariusz UOP/ABW, od 1999 lat zawodowo zajmuje się problematyką ochrony informacji niejawnych i innych danych prawnie chronionych, od 2009 ekspert ABW z zakresu ochrony informacji niejawnych. W latach 2013 - 2017 Pełnomocnik ds. ochrony informacji niejawnych w Kujawsko – Pomorskim Urzędzie Wojewódzkim w Bydgoszczy oraz kilku innych jednostkach organizacyjnych rządowej administracji zespolonej. Od 2017 związany z Biurem Doradczo – Usługowym OIN spółka cywilna w Bydgoszczy, wykonuje obowiązki Pełnomocnika ds. OIN oraz Inspektora Ochrony Danych w kilku instytucjach i przedsiębiorstwach. Od 2016 stale współpracuje z Fundacją Rozwoju Demokracji Lokalnej.

a) Ogłoszenia o naborze, obowiązek informacyjny oraz rekrutacje ukryte.
b) Gromadzenie i udostępnianie CV kandydatów.
c) Testy psychologiczne.
d) Profilowanie kandydatów i weryfikacja informacji z CV w oparciu o dane ogólnodostępne.
e) Zasady postępowania z CV kandydatów po zakończonym naborze.
f) CV otrzymane doraźnie (poza procedurą naboru).
g) Wykorzystywanie otrzymanych CV przy kolejnych rekrutacjach.
h) Wykorzystanie danych kandydatów do działalności marketingowej.

9. Dokumentacja kadrowo – płacowa w trakcie zatrudnienia.
a) Pojęcie „danych służbowych".
b) Dane i dokumenty, jakie pracodawca może żądać od pracownika.
c) Akta osobowe pracowników.
d) Listy obecności i grafiki zmianowe.
e) Outsourcing danych kadrowych na przykładzie badań profilaktycznych.
f) Przetwarzanie danych kadrowych przy okazji ubezpieczeń grupowych oraz benefitów pracowniczych.
g) Wykorzystanie wizerunku pracownika oraz zdjęcia na identyfikatorach.
h) Gromadzenie szczególnych kategorii danych w związku z ZFŚS oraz PKZP.
i) Postępowanie z wnioskami ze strony uprawnionych organów (policja, prokuratura, urzędy) o udostępnienie danych osobowych.
j) Przesyłanie danych osobowych do odbiorców zewnętrznych oraz udzielanie informacji na telefon.
k) Przetwarzanie danych osobowych po ustaniu stosunku pracy.

10. Monitoring w zakładzie pracy:
a) Formy monitoringu i cele ich stosowania.
b) Wymogi formalne związane z wprowadzeniem monitoringu.
c) Wgląd do służbowych e-maili pracowników.
d) Ocena pracownika na podstawie jego aktywności w Internecie.
e) Dopuszczalność śledzenia pracowników w sieciach społecznościowych, monitoring byłych pracowników.
f) Śledzenie mobilnych pracowników (GPS, telefony komórkowe).

11. RODO a dostęp do informacji publicznej (BIP, udostępnianie dokumentacji zawierającej dane osobowe).

12. Jak należy skutecznie zabezpieczyć dane osobowe (w wersji papierowej i elektronicznej)?
a) Zasady:
- Zasada wiedzy uzasadnionej.
- Zasada czystego ekranu.
- Zasada czystego biurka.
- Zasada czystych drukarek.
- Zasada czystej tablicy.
- Zasada czystego kosza.

b) Środki zabezpieczenia danych osobowych:
- Zasady dostępu do pomieszczeń.
- Bezpieczeństwo pasywne.
- Procedura zarządzania kluczami od pomieszczeń.
- Loginy.
- Polityka haseł.
- Wygaszacze ekranów.
- Komputery przenośne i "praca na odległość".
- Komputerowe nośniki danych.
- Kopie bezpieczeństwa.
- Zabezpieczenia przed szkodliwym oprogramowaniem.
- Zabezpieczenia kryptograficzne.
- Procedury reagowania na incydenty.

13. Pytania i konsultacje indywidualne.

Szkolenia zamknięte realizujemy w formie stacjonarnej jak również w formule on-line.

Jak organizujemy szkolenie zamknięte stacjonarne?

W przypadku organizacji szkolenia zamkniętego w formule stacjonarnej Trener i koordynator szkolenie przyjeżdżają do Państwa w ustalonym terminie do siedziby Zamawiającego lub innym ustalonym miejscu.

Cena szkolenia stacjonarnego wynosi dla 15-20 uczestników wynosi 3400 zł netto zw. z VAT w przypadku finansowania szkolenia ze środków publicznych (zwolnienie z art. 43, ust.1, pkt 29C u.p.t.u). Płatność przelewem po szkoleniu w terminie 14 dni.

Cena obejmuje:

- Analizę potrzeb szkoleniowych i dostosowanie programu szkolenia do potrzeb Zamawiającego,
- Przygotowanie i przeprowadzenie dedykowanego programu szkolenia przez 1 trenera,
- Materiały szkoleniowe dla każdego uczestnika dostępne w wersji papierowej i elektronicznej,
- Imienne certyfikaty ukończenia szkolenia,
- Ewaluację szkolenia i przekazanie jej wyników Zamawiającemu,
- Konsultacje poszkoleniowe.

Jak organizujemy szkolenia zamknięte online?

Uczestnicy mogą uczestniczyć w szkoleniu w formule stacjonarnej (w sali urzędu czy dowolnym miejscu wyposażonym w rzutnik i internet), mieszanej tj. część osób w sali urzędu, część przy komputerach lub wszyscy przy komputerach (praca zdalna lub przy swoich stanowiskach pracy). Ekspert będzie prowadził szkolenie z sali multimedialnej (zdalnie) dzięki czemu będą go Państwo widzieli i słyszeli, a materiały, prezentacje, filmy instruktażowe, dokumenty będą wyświetlane przez niego na ekranie Państwa monitora lub w sali urzędu za pośrednictwem rzutnika multimedialnego.
Zarówno przed spotkaniem, jak i w jego trakcie mogą Państwo zadawać pytania poprzez mikrofon lub czat. Trener odpowiada na te pytania na bieżąco lub w drugiej części szkolenia w sesji pytań i odpowiedzi.
Platforma, na której odbywa się webinarium, jest dostępna bezpośrednio przez przeglądarkę internetową, (Google Chrome). Potrzebny jest komputer z dostępem do Internetu. Przydatne mogą być również słuchawki z mikrofonem lub głośniki.

Cena szkolenia online wynosi dla 15-20 uczestników wynosi 2500 zł netto zw. z VAT w przypadku finansowania szkolenia ze środków publicznych (zwolnienie z art. 43, ust.1, pkt 29C u.p.t.u). Płatność przelewem po szkoleniu w terminie 14 dni.

Cena obejmuje:

- Analizę potrzeb szkoleniowych i dostosowanie programu szkolenia do potrzeb Zamawiającego,
- Przygotowanie i przeprowadzenie dedykowanego programu szkolenia przez 1 trenera,
- Materiały szkoleniowe dla każdego uczestnika dostępne w wersji elektronicznej,
- Imienne certyfikaty ukończenia szkolenia w wersji elektronicznej,
- Ewaluację szkolenia i przekazanie jej wyników Zamawiającemu,
- Konsultacje poszkoleniowe.