Szkolenie **„Bezpieczeństwo danych osobowych (RODO) w przedsiębiorstwach turystycznych”**

Szkolenie spełnia wymogi okresowego szkolenia pracowników z obszaru ochrony danych (RODO) i bezpieczeństwa informacji wymaganego podczas kontroli UODO.
Dofinasowanie dla pracowników firm z obszaru Turystyki, Hotelarstwa, gastronomii – 80%.
Czas szkolenia -16 h. Dostępna forma stacjonarna, jak i zdalna (OnLine). Termin do ustalenia.
Szkolenie prowadzą certyfikowani praktycy i eksperci z tego Obszaru. Obejmuje ono kluczowe obszary ochrony danych, które były weryfikowane w kontrolach UODO w ostatnich dwu latach.
W ramach szkolenia, w szczególności zostaną:

- omówione zagadnienia wymogów RODO,
- omówione wymogi bezpieczeństwa danych osobowych,
- omówione wyniki i decyzje kontroli (i kar) UODO,
- udzielone odpowiedzi na stawiane pytania oraz
- przekazane materiały informacyjne,

Ramowy program usługi

1. **Pre-test**
   - **Informacje wprowadzające na temat Bezpieczeństwa danych**
   - Podstawowe regulacje prawne i normatywne dotyczące bezpieczeństwa danych osobowych w sektorze turystycznym
   - Wybrane definicje i pojęcia ochrony danych
2. **Podstawy i zasady przetwarzania danych osobowych na gruncie RODO**
   - Zasada legalności
   - Zasada ograniczenia celu
   - Zasada minimalizacji danych
   - Zasada prawidłowości
   - Zasada ograniczenia przechowywania
   - Zasada integralności i poufności
   - Zasada rozliczalności
   - Podstawy prawne przetwarzania danych osobowych
3. **Podstawa przetwarzania,**
   - umowy jako podstawa przetwarzania
   - inne prawa jako podstawa przetwarzania
   - interes administratora jako podstawa przetwarzania
4. **Obowiązek informacyjny – prawo do informacji**
   - Jak wypełnić obowiązek informacyjny - krok po kroku
   - Gdy dane zbieramy od osoby, której dane dotyczą,
   - Gdy dane zbieramy od innej osoby, której dane dotyczą
   - Zasady informowania o przetwarzaniu danych osobowych,
   - Obowiązki informacyjne – miejsca i sposoby ich realizacji
5. **Praktyczne tworzenie klauzul informacyjnych**
6. **Prawa osób, których dane dotyczą**
   - Żądanie usunięcia danych lub żądanie zaprzestania przetwarzania danych osobowych,
   - Prawo do bycia zapomnianych,
   - realizacja sprzeciwu na działania marketingowe,
   - Otrzymanie kopii danych,
   - Żądanie sprostowania, uaktualnienia, zmiany danych osobowych
7. **Retencja danych**
   - Zasady retencji danych
   - Okres przechowywania dokumentacji w postaci papierowej i elektronicznej
8. **Obsługa naruszeń ochrony danych osobowych**
   - Ocena stopnia naruszenia

Projekt został opracowany w Polskiej Agencji Rozwoju Przedsiębiorczości. Realizacja projektu została sfinansowana przez Unię Europejską ze środków Programu Operacyjnego Wiedza Edukacja Rozwój

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
PARP Grupa PFR
Unia Europejska Europejski Fundusz Społeczny

- Dokumentowanie naruszeń
- Zgłoszenie naruszenia do UODO
- Zawiadomienie osoby, której dane zostały naruszone

9. Zlecanie (powierzanie) przetwarzania danych osobowych

- Jakie kwalifikacje musi spełniać podmiot, któremu powierza się przetwarzanie danych
- Jakie postanowienia musi zawierać umowa powierzenia
- Na jakich zasada odpowiada podmiot, któremu powierzono przetwarzanie danych

10. Środki Techniczne i organizacyjne

- Rodzaje środków,
- Mierzenie ocenianie,
- Wyciąganie wniosków , działania optymalizacyjne,
- Ocena skutków dla ochrony danych osobowych – DPIA

11. Dokumentacja ochrony danych

- Rejestr czynności przetwarzania danych
- Rejestr Kategorii przetwarzania danych
- Polityki, metodyki, procedury, instrukcje itp.

12. Obowiązki Administratora danych – na co zwracać uwagę, czego pilnować

13. Kary i wnioski z ostatnich kontroli UODO

- Uprawnienia urzędu,
- Przebieg kontroli,
- Przesłanki nałożenia kary
- Wnioski płynące z ostatnich kontroli.
- Dokumenty regulujące i normatywne ochrony danych osobowych.
- Kto jest osobą nieuprawnioną do dostępu do danych osobowych.

14. Największe zagrożenia – statystyki

- konsekwencje braku zaangażowania i wsparcia kierownictwa.
- Świadomość i zaangażowanie osób uprawnionych - czynniki motywacji
- Wnioskowanie, nadawanie i dokumentowanie nadania uprawnień.
- Dane osobowe, a uprawnienia administracyjne.

15. Największe zagrożenia – cd…

- Hasła domyślne i inne błędy instalacji systemów wpływające na bezpieczeństwo danych osobowych.
- Obowiązek weryfikacji uprawnień.
- Przeglądy i testy zabezpieczeń, pomiary, monitorowanie
- Bezpieczeństwo prawne,
- Czas przetwarzania..

16. Przed kim zabezpieczamy dane i w jaki sposób.

- Dane osobowe w korzystaniu z e-mall - bezpieczeństwo przesyłanych danych,
- Dane osobowe w smartfonach – zagadnienia bezpieczeństwa
- Dane osobowe w monitoringu wizyjnym. Zasady dostępu do nagrań. Czas przetwarzania.
- Dane osobowe w turystyce. Hotel, restauracja, wycieczki, samoloty.

17. Przekazywanie danych do państwa trzeciego

- Dane osobowe przy opuszczaniu Europejskiego obszaru Gospodarczego. Wizy, Hotele poza EOG. Publikowanie
- wizerunku i danych klientów,
- Dane przekazywane i powierzane w celu realizacji umowy,
- Międzynarodowe (i Europejskie) normy ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 29134 oraz ISO/IEC 29151 jako
- standard utrzymania bezpieczeństwa danych osobowych

18. Post- test

Projekt został opracowany w Polskiej Agencji Rozwoju Przedsiębiorczości. Realizacja projektu została sfinansowana przez Unię Europejską ze środków Programu Operacyjnego Wiedza Edukacja Rozwój

Fundusze Europejskie Wiedza Edukacja Rozwój | Rzeczpospolita Polska | PARP Grupa PFR | Unia Europejska Europejski Fundusz Społeczny