Program zajęć

Część M: <u>Ochrona danych osobowych w Uczelni</u>

Prowadzący: Piotr Chałaszczyk

Adres: Kampus Uniwersytetu Śląskiego Katowice Centrum – ul. Bankowa

Liczba godzin: 8 h

<u>PROGRAM</u>

1. Wstęp i źródła prawa
    - Rozporządzenie 2016/679
    - Ustawa o ochronie danych osobowych
2. Podstawowe pojęcia i informacje
    - Kto i kiedy ma obowiązek stosować przepisy RODO
    - Administrator danych, procesor i osoba upoważniona do przetwarzania danych – role w procesie przetwarzania danych osobowych, a zmiany z RODO.
    - Dane osobowe – tzw. zwykłe, tzw. sensytywne, w tym biometryczne
    - Zbiory danych osobowych – jak je rozróżniać, jak kwalifikować w kontekście RODO
    - W jakich sytuacjach „przetwarzamy dane osobowe”?
    - Kiedy możemy je przetwarzać?
3. Zasady przetwarzania danych osobowych
    - Zasada legalności – praktyczne aspekty kryteriów prawnych
    - Zasada celowości w przetwarzaniu danych osobowych
    - Zasada adekwatności zbieranych danych
    - Zasada poprawności merytorycznej i jej oceny
    - Zasada ograniczonego czasu – i możliwe optymalizacje
    - Zasada poufności i integralności danych
4. Obowiązki administratora danych
    - Obowiązek informacyjny przy przetwarzaniu danych osobowych – ustawa krajowa oraz RODO
    - Przesłanki przetwarzania danych osobowych – art. 6 i 9 RODO
    - Obowiązek zgłaszania Naruszeń, wynikający z RODO (zasada 72 godzin)
    - Obowiązek uwzględniania ochrony danych już w fazie projektowania tj. nowe zasady RODO: „privacy by design” oraz „privacy by default”
    - Anonimizacja i pseudonimizacja danych osobowych
5. Tworzenie i aktualizowanie dokumentacji przetwarzania i ochrony danych osobowych
    - Jak dostosować Politykę bezpieczeństwa do RODO?
    - Instrukcja zarządzania systemem Informatycznym po wejściu w życie RODO
    - Umowa powierzenia przetwarzania danych osobowych
    - Upoważnienie do przetwarzania danych osobowych w kontekście RODO
    - Rejestr czynności przetwarzania
    - Ewidencja osób upoważnionych do przetwarzania danych
    - Obecna dokumentacja w perspektywie aktualnych wymogów RODO
6. Inspektor Ochrony Danych (Data Protection Officer)
    - Kiedy będziemy mieli obowiązek powołania Inspektora Ochrony Danych?
    - Zadania, status i kompetencje Inspektora Ochrony Danych w RODO oraz w opinii Grupy Roboczej art. 29.

7. Prawa jednostki w RODO
    - Prawo do dostępu do danych
    - Prawo do sprzeciwu i przeniesienia danych
    - Prawo do ograniczenia przetwarzania
    - Prawo do bycia zapomnianym
    - Wnoszenie skarg
    - Prawo do odszkodowania
    - Profilowanie
8. Bezpieczeństwo przetwarzania danych osobowych – przykładowe aspekty praktyczne w kontekście RODO
    - Analiza ryzyka przy przetwarzaniu danych
    - Identyfikacja naruszeń bezpieczeństwa danych osobowych
    - Zabezpieczenie danych – aspekt organizacyjny
    - Zabezpieczenie danych – fizyczne i informatyczne
9. Prawo do ochrony prywatności w Polsce i w Unii Europejskiej. Odpowiedzialność (administracyjna, cywilna, karna, dyscyplinarna) związana z przetwarzaniem danych osobowych – zmiany po RODO
    - Kary do 20 000 EUR dla podmiotów prywatnych
    - Alternatywnie do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego • Sankcje dla podmiotów publicznych

EFEKTY KSZTAŁCENIA

Uczestnicy szkolenia

poznają podstawowe pojęcia związane z bezpieczeństwem informacji i ochroną danych osobowych:

- będą potrafili identyfikować współczesne zagrożenia bezpieczeństwa informacji,
- poznają środki zabezpieczeń informacji (elektroniczne, fizyczne, środki zabezpieczenia danych przetwarzanych w wersji papierowej i w systemach informatycznych),
- będą świadomi jakie obowiązki wynikają z prawidłowo prowadzonej dokumentacji ochrony danych osobowych,
- będą świadomi jakie obowiązki wynikają z Rozporządzenia RODO oraz aktów prawa krajowego,
- będą potrafili zidentyfikować ryzyka i zagrożenia w zakresie ochrony danych osobowych,
- będą świadomi skutków naruszenia bezpieczeństwa aktywów informacyjnych i danych osobowych.

WIEDZA:

- zdobycie i usystematyzowanie wiedzy z zakresu podstaw przepisów prawa z ochrony danych osobowych, ukierunkowanie działań na właściwe działania osób przetwarzających dane we wdrożonym systemie bezpieczeństwa informacji w Uczelni,

UMIEJĘTNOŚCI:

- umiejętność praktycznej interpretacji przepisów prawa pozwalające na prawidłowe wykonywanie czynności wynikających z kompetencyjnego zakresu obowiązków,
- umiejętność dostrzegania i postrzegania zagrożeń dla bezpieczeństwa informacji,
- umiejętność racjonalnego wykorzystania przepisów prawa zależnie od kontekstu sytuacji przetwarzania,
- umiejętność zastosowania katalogu dobrych praktyk przy przetwarzaniu danych