

Ochrona danych osobowych

w oparciu o wymogi

Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w
sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
(RODO)

Zakres tematyczny spotkania

1. Podstawowe pojęcia systemu bezpieczeństwa informacji
 - a) pojęcie danych osobowych
 - b) szczególne rodzaje danych osobowych
 - c) pojęcie zbioru danych – identyfikacja zbiorów danych
 - d) pojęcie przetwarzania danych
 - e) zasada legalności przetwarzania danych osobowych
 - f) zasada merytorycznej poprawności i adekwatności przetwarzanych danych osobowych
 - g) zasada ograniczenia czasu przetwarzania danych
 - h) inne zasady
2. Administrator Danych Osobowych i jego obowiązki, w tym zapewnienie rozliczalności z wdrożonych procedur ochrony danych osobowych klienta/pacjenta
3. Definicja odbiorcy danych w rozumieniu RODO
4. Podmiot przetwarzający – obowiązki po 25 maja 2018 roku
5. Przesłanki przetwarzania danych osobowych – praktyczne przykłady
6. Zgoda osoby, której dane dotyczą jako podstawa do przetwarzania danych – jak prawidłowo odebrać zgodę
7. Zakres przetwarzania danych osobowych adekwatny do celu – dlaczego musimy kontrolować taką zależność ?
8. Realizacja obowiązku informacyjnego po 25 maja 2018 roku (w oparciu o Art. 13 i 14 RODO)
9. Elementy systemu ochrony danych osobowych
 - a) powierzenie przetwarzania danych osobowych po 25 maja 2018 roku – z kim i dlaczego musimy zawrzeć umowę powierzenia przetwarzania danych
 - b) zabezpieczenie danych
 - c) dokumentacja wymagana oraz dokumentacja pomocnicza
 - d) Rejestr czynności przetwarzania danych oraz rejestr kategorii czynności przetwarzania danych (Art. 30 RODO)
10. Audyt - inwentaryzacja zasobów danych osobowych i rozpoznanie stanu ich ochrony
11. Zabezpieczenia organizacyjno – techniczne, w kontekście ich adekwatności do zakresu przetwarzanych danych osobowych.
12. Analiza zagrożeń i ryzyka.
13. Zasady przetwarzania danych osobowych w systemach informatycznych w tym na portalach społecznościowych, komunikatorach internetowych.
14. Jak zabezpieczyć przesyłanie danych osobowych za pomocą poczty elektronicznej.
15. Kodeks dobrych praktyk podmiotu przetwarzającego dane osobowe.
16. Ocena skutków dla ochrony danych osobowych
17. Ocena ryzyka
18. Procedura zarządzania incydentami - przykłady
19. Ważne zmiany w ogólnym rozporządzeniu o ochronie danych (RODO) pod kątem realizacji praw osób fizycznych których dane dotyczą
 - a) prawo do usunięcia danych (prawo do bycia zapomnianym)
 - b) prawo do przenoszenia danych
 - c) privacy by design oraz privacy by default (ochrona danych w fazie projektowania)
 - d) prawo do sprzeciwu
 - e) prawo dostępu do danych oraz ich poprawiania
20. Prawo osoby fizycznej do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych
21. Ocena przez Administratora wagi naruszenia ochrony danych osobowych
22. Notyfikacja naruszeń

23. Zawiadomienie osoby której dane dotyczą o naruszeniu jej praw i wolności (kiedy zobowiązani jesteśmy zawiadomić osobę o naruszeniu)
24. Odpowiedzialność Administratora za naruszenie przepisów o ochronie danych osobowych po 25 maja 2018 roku