XI Konferencja Naukowa
Bezpieczeństwo w Internecie. Analityka danych
Warszawa 6-7.06.2019

# Analiza ryzyka przy przetwarzaniu danych osobowych

dr hab. Bogdan Fischer

Uniwersytet Jagielloński

Urząd Ochrony Danych Osobowych

Naukowe Centrum Prawno-informatyczne

UKE

- Obowiązek prowadzenia systematycznej analizy ryzyka m.in. w przepisach prawa w zakresie kontroli zarządczej, ochrony danych osobowych (RODO), cyberbezpieczeństwa
- Uwzględniane w międzynarodowych standardach zarządzania m.in. systemie zarządzania jakością (ISO 9001), bezpieczeństwem informacji (ISO 27001), ciągłością działania (ISO 22301) czy systemie antykorupcyjnym (ISO 37001).

# Ryzyko ITIL

- Ryzyko - możliwe zdarzenie, które mogłoby spowodować szkody lub straty, albo wpływać na zdolność do osiągnięcia zamierzonych celów.
- Ryzyko jest mierzone przez: prawdopodobieństwo zagrożenia, podatność zasobów na to zagrożenie oraz wpływ, jaki dane zagrożenie mogłoby mieć, gdyby wystąpiło.
- Ryzyko - niepewność wyników. Może być używane do pomiaru prawdopodobieństwa rezultatów, zarówno tych pozytywnych, jak i negatywnych

- Ryzyko nie stanowi zagrożenia, ale oznacza że może się ono  pojawić
- Norma PN-I-13335-1 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych, definiuje **ryzyko jako prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów aby spowodować stra**ty
- Podatność – słabości zasobu które mogą być wykorzystane przez zagrożenie i ich analiza

# Analiza ryzyka

- Pojęcie ryzyka w zakresie bezpieczeństwa informacji oraz w zakresie ryzyka naruszenia praw i wolności osób fizycznych

- Identyfikacja ryzyka
- Szacowanie i ewaluacja ryzyka
- Planowanie reakcji na ryzyko

# Metodyka szacowania ryzyka

- Jakościowe – bazujące na wartościach opisowych, niepoliczalnych ‚poziom ryzyka definiują np. jako „niski”, „średni”, „wysoki”
- Ilościowe – bazujące na konkretnych danych liczbowych, np. wysokości potencjalnych strat - poziom ryzyka przedstawiany jako konkretna wartość liczbowa
- Mieszane

Elementy analizy ilościowej

- Plan zarządzania ryzykiem,
- Listy ryzyk: zidentyfikowanych, ich hierarchii, przeznaczonych do dalszej analizy, historycznych,
- Opinie ekspertów oraz rezultaty innych planowanych procesów.
- Określenie dwóch podstawowych parametrów : wartości skutku i prawdopodobieństwa wystąpienia danego ryzyka.

- Jakościowe szacowanie ryzyka jest subiektywną oceną, opartą na różnych elementach dobrych praktyk i doświadczenia
- Uwzględnienie przyjętej w organizacji skali prawdopodobieństwa i mierników skutków wystąpień zagrożeń
- Uwzględnienie przyjętych założeń w procesie identyfikacji i oceny źródeł ryzyka.
- Inne

- Metodyka statycznej i dynamicznej analizy ryzyka
- Inne metodyki

- Analiza ryzyka jako podstawowe narzędzie dla Oceny Skutków dla Ochrony Danych
- Dokumentacja

- Dziękuję za uwagę