Wojciech Grenda
GDPR Risk Tracker

Dzień Dobry!

https://gdprrisktracker.pl/webinar-pytania-i-odpowiedzi

O czym dzisiaj?

1. Jakie elementy wpływają na ryzyko związane z przetwarzaniem danych?
2. Na co zwrócić uwagę przy ocenie tych czynników?
3. Jak wykonać analizę ryzyka przykładowej czynności przetwarzania?
4. Jak wykonać DPIA (ocenę skutków dla ochrony danych)?
5. Jak tworzyć i prowadzić rejestr czynności przetwarzania w GDPR Risk Tracker?
6. Jak wykorzystać GDPR Risk Tracker w pracy IOD?

Wojciech Grenda
GDPR Risk Tracker

Jakie elementy wpływają na ryzyko związane z przetwarzaniem danych?

Zasoby

Waga danych

Skutki

Aktywa

Prawdopodobieństwo

Zabezpieczenia

Zagrożenia

Ryzyko

Podatność

Jakie ryzyko analizujemy

Patrzymy na ryzyko z perspektywy **podmiotów danych** ALE także

Przetwarzamy dane jako **Administrator** lub **Procesor** ZATEM

Analizujemy **ryzyko** związane z **przetwarzaniem danych**

A jest to ryzyko:

- **zniszczenia,**
- **utraty,**
- **modyfikacji,**
- **ujawnienia,**
- **nieuprawnionego dostępu**

Jakie ryzyko analizujemy

- Można te ryzyka zmapować na znane właściwości bezpiecznego przetwarzania:
  - **Poufność**
  - **Integralność**
  - **Dostępność**

Poufność - nieuprawniony dostęp, ujawnienie

Integralność - zniszczenie, utrata, modyfikacja

Dostępność - zniszczenie, utrata

Co będzie potrzebne, żeby takie ryzyka wyznaczyć

Waga

Prawdopodobieństwo

Skutek

Zabezpieczenia

Zagrożenia

Zasoby

Podatności

Na co zwrócić uwagę przy ocenie tych czynników?

Waga danych

Warto wybrać obiektywne czynniki, które uwzględniają **ilościowy** i **jakościowy** charakter przetwarzanych danych. Dzięki temu można łatwiej i precyzyjniej określić wagę danych, która zależy zarówno od:

- Kategorii (dane „zwykłe”, dane specjalnych kategorii, dane dotyczące wyroków)
- Zakresu danych (np. tylko imię i nazwisko vs. dziesiątki lub setki typów danych)
- Ale także od skali przetwarzania, na którą może wpływać:
  - Liczba rekordów w „bazie danych”
  - Liczba podmiotów biorących udział w przetwarzaniu danych
  - Skomplikowanie samego procesu przetwarzania (czynności), w ramach którego dane są przetwarzane

Na co zwrócić uwagę przy ocenie tych czynników?

Zagrożenia

Dlaczego warto od nich zacząć analizę ryzyka?

- Jest to **pierwotna** i najbardziej **wpływająca** na ryzyko kategoria czynników
- Nie daje złudnego poczucia, że wdrożone dotychczas zabezpieczenia chronią przed **wszystkimi** mogącymi wystąpić zagrożeniami
- Dużo łatwiej określić **prawdopodobieństwo** wystąpienia zagrożenia, niż prawdopodobieństwo materializacji ryzyka jako takiego
- Rozpatrzenie reprezentatywnego, powtarzalnego zbioru zagrożeń, gwarantuje **obiektywizm**.

Na co zwrócić uwagę przy ocenie tych czynników?

Zabezpieczenia

Jak dobrać zabezpieczenia?

- Traktujemy je szeroko, bardziej jako wszelkie **środki** (techniczne, organizacyjne, formalne)
- Powinny być „wtórne” – zabezpieczać **występujące** zagrożenia
- Zabezpieczenia nieistniejących zagrożeń są bezsensowne
- Powinny być skoncentrowane na ryzykach związanych z bezpieczeństwem przetwarzania danych podmiotów danych (modyfikacja, zniszczenie, itd…)
- Dobór zabezpieczeń powinien uwzględniać **wszystkie** zidentyfikowane wcześniej zagrożenia
- Jakość zabezpieczeń może być wyrażona poprzez ich faktyczną **skuteczność** albo **skalę** zastosowania

Na co zwrócić uwagę przy ocenie tych czynników?

Zasoby, podatność…

Dyskusja nad tym, czy oceniać zagrożenia, czy podatności i jak osadzić je w zasobach (i jakich zasobach) powoduje, że:

- Jest to zbyt **skomplikowane** dla osób „nietechnicznych” – a na ogół takie osoby, a nie specjaliści, mają wiedzę na temat procesów, które poddawane są analizie
- Tworzy się chaos pojęciowy i nachodzenie na siebie definicji
- Trudno odróżnić przyczyny od skutków albo pojęcia pierwotne od wtórnych

Zatem

- Warto by to uprościć nie zmieniając zasady działania

Zatem jak to ryzyko wyznaczyć?

1. Wydziel czynności przetwarzania
2. Określ wagę przetwarzanych danych
3. Zidentyfikuj **zagrożenia**
4. Określ **prawdopodobieństwo** wystąpienia każdego z nich
5. Zmapuj zagrożenia na **ryzyka** (utrata, ujawnienie…)
6. Zmapuj zagrożenia na **zasoby**
7. Dla wszystkich zagrożeń dotyczących danego zasobu i wpływających na dane ryzyko określ **zabezpieczenie** i jego jakość
8. Określ **skutek** materializacji danego ryzyka
9. **Gotowe!**

Zapraszam do GDPR Risk Tracker

Dziękujemy za uwagę

Zapraszamy za miesiąc na kolejny webinar

Wojciech Grenda – GDPR Risk Tracker
wojciech.grenda@gdprrisktracker.pl | 501-431-767 | https://gdprrisktracker.pl