

WARSZAWA, 18 KWIETNIA 2019 R.



Ministerstwo
Cyfryzacji

AUDYT OCHRONY DANYCH OSOBOWYCH W JEDNOSTCE SEKTORA FINANSÓW PUBLICZNYCH - NA CO ZWRACAĆ UWAGĘ

Dr Maciej Kawecki

Radca prawny Joanna Noga-Bogomilska



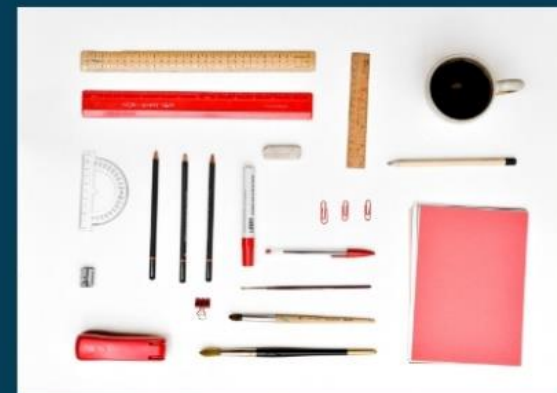
AGENDA

- PRZYGOTOWANIE DO AUDYTU
- DOKUMENTACJA W ZAKRESIE DANYCH OSOBOWYCH
- RAPORT Z AUDYTU – ROLA I BUDOWA
- AUDYTOWANIE PODMIOTU PRZETWARZAJĄCEGO
- PODSUMOWANIE



PRZYGOTOWANIE DO AUDYTU W ZAKRESIE OCHRONY DANYCH

- Podstawa prawna
- Okres objęty audytem
- Opracowanie listy kontrolnej
- Określenie przedmiotu audytu / Zakres audytu
- Plan audytu
- Sposób i zakres audytowania
- Formy technik audytowych



DOKUMENTACJA W ZAKRESIE DANYCH OSOBOWYCH



- Polityka ochrony danych → zaleca się aby był to dokument w ramach szerszej polityki bezpieczeństwa informacji
- Instrukcja postępowania w przypadku naruszenia ochrony danych
- Instrukcja realizacji praw osób, których dane dotyczą
- Dokumentacja związana z powołaniem IOD/ZIOD
- Rejestr czynności przetwarzania
- Rejestr naruszeń
- Rejestr umów powierzenia przetwarzania
- Analiza ryzyka
- Ocena skutków dla ochrony danych

Inne elementy zgodności warte sprawdzenia

- Sprawdzenie sposobu realizowania zasad z art. 5 RODO:
 - ➔ Zgodność z prawem, rzetelność i przejrzystość
 - ➔ Ograniczenie celu przetwarzania
 - ➔ Minimalizacja danych
 - ➔ Prawidłowość danych
 - ➔ Retencja danych
 - ➔ Integralność i poufność danych
- *Privacy by default / privacy by design*
- Realizacja praw osób, których dane są przetwarzane





INNE ELEMENTY ZGODNOŚCI WARTY SPRAWDZENIA

- Realizacja obowiązków związanych z ujawnianiem danych podmiotom trzecim (odbiorcom danych)
 - ➔ Umowy o powierzeniu przetwarzania bądź inne instrumenty prawne, na mocy których dochodzi do powierzenia
 - ➔ Umowy o współadministrowanie (inne instrumenty prawne)
- Zapewnienie zabezpieczenia danych osobowych – *risk based approach*

RAPORT Z AUDYTU W ZAKRESIE OCHRONY DANYCH

- Oznaczenie administratora
- Data rozpoczęcia i zakończenia audytu
- Wykaz podjętych czynności
- Określenie przedmiotu i zakresu audytu
- Opis stanu faktycznego
- Stwierdzone przypadki niezgodności i sposób ich opisywania, ocena istotności
- Zalecenia dotyczące podjęcia działań w celu naprawy



DOKUMENTACJA W ZAKRESIE DANYCH OSOBOWYCH



- Art. 28 ust. 3 lit. h RODO – obowiązki podmiotu przetwarzającego
- Zasady przeprowadzania audytu w umowie powierzenia
 - ➔ Zapis o zasadach audytu
 - ➔ Tryb zawiadamiania
 - ➔ Zakres dokumentowania
 - ➔ Przedstawianie wniosków
 - ➔ Harmonogram działań naprawczych i ich egzekwowanie

PODSUMOWANIE

- Znaczenie dobrego przygotowania audytu dla jego powodzenia
- Audyt i co dalej – Harmonogram wdrożenia rekomendacji i jego egzekwowanie





Ministerstwo
Cyfryzacji

Dziękujemy

Dr Maciej Kawecki
Radca prawny Joanna Noga-Bogomilska