Realizacja audytów przez IOD w kontekście specyfiki przetwarzania danych w podmiotach publicznych

Agnieszka Gębicka

Sławomir Wichrowski

ORGANIZATOR:
ABI EXPERT

odo.abi-expert.pl

Audyt IOD – uwarunkowania prawne

Zadania IOD (Art. 39 RODO):

- Informowanie i doradzanie,
- Monitorowanie, audyty DPIA,
- Szkolenia,
- Współpraca z PUODO,
- Punkt kontaktowy.

Rola aktów wewnętrznych:

- Regulamin organizacyjny,
- Polityka Ochrony Danych Osobowych,
- procedury wewnętrzne, np. określające zasady realizacji projektów

- ADO jest odpowiedzialny za przestrzeganie przepisów oraz wykazanie zgodności.
- Audyt IOD stanowi weryfikację zgodności z wymaganiami przepisów prawa.
- IOD wspiera ADO wskazując obszary wymagające podjęcia działań.

IOD – status w kontekście relacji z audytem wewnętrznym i kontrolą wewnętrzną

Niezależność i komplementarność działań

Ministerstwo Finansów i Urząd Ochrony Danych Osobowych we wspólnym stanowisku określili zasady współpracy audytora wewnętrznego i IOD przy realizacji zadań w jednostkach sektora finansów publicznych.

Ich działania powinny być komplementarne, jednak obydwie funkcje powinny posiadać gwarancje niezależności kształtujące ich status.

Konieczność bieżącej współpracy i wymiany informacji

IOD – audyt wewnętrzny – kontrola wewnętrzna

Audyty IOD – cel i zakres

Audyt IOD

zaplanowana, obiektywna i usystematyzowana analiza stanu faktycznego czynności przetwarzania danych osobowych.

Cel Audytu:

- **monitorowanie** przestrzegania przez ADO i Procesora przepisów z zakresu ochrony danych osobowych
- **zapobieganie** lub **minimalizację** ryzyka wystąpienia NODO
- **identyfikację** rozwiązań technicznych i organizacyjnych, które są adekwatne do czynności przetwarzania realizowanych przez ADO i Procesora
- **wsparcie** ADO w zapewnieniu zgodności z przepisami z zakresu ochrony danych osobowych

Roczny plan audytów IOD

Kryteria planowania audytów IOD:

- Wyniki analizy ryzyka w organizacji
- Wyniki audytów IOD w organizacji
- Wyniki analizy naruszeń ochrony danych osobowych
- Wyniki przeprowadzonej oceny skutków dla ochrony danych (DPIA)
- Monitorowanie Rejestru czynności przetwarzania (RCP)
- Decyzje Prezesa UODO
- Roczny Plan kontroli sektorowych UODO
- Orzecznictwo

Wyzwania w praktyce audytowej

- Privacy by design, privacy by default
- Zasady przetwarzania danych osobowych w systemach IT
- Cykliczne testowanie skuteczności zabezpieczeń technicznych
- Zarządzanie uprawnieniami dostępu do aplikacji
- Rozliczalność w systemach IT
- Realizacja praw osób
- Retencja danych

Wyzwania audytu związane z rozwojem technologicznym

Automatyzacja

- Profilowanie,
- Zautomatyzowane podejmowanie decyzji (ZPD),
- ZPD oparte na profilowaniu.

Usługi chmurowe

AI (sztuczna inteligencja)

…?

Dylematy i wyzwania związane z wykorzystaniem nowoczesnych technologii

- Podstawa przetwarzania
- Adekwatne zabezpieczenia
- DPIA
- Autentyczność danych
- Transfer danych
- Dyskryminacja związana ze stronniczym działaniem algorytmu
- Realizacja praw osób

Co wiemy o SI?

Metody uczenia algorytmów SI:

Uczenie maszynowe - Uczenie nadzorowane - Uczenie głębokie - Federated Learning – Generatywna sztuczna inteligencja

Wdrożenie oprogramowania wykorzystującego SI:

Testowanie i walidacja - Produkcyjne wykorzystanie

Jakie dane można wykorzystać do trenowania modelu:

Dane spseudonimizowane – dane zanonimizowane – dane statystyczne

Wykorzystanie generatywnej sztucznej inteligencji

1. **Modele wykorzystania**

   open source – open source + własne dane – własny R&D

2. **Problemy związane z działaniem**

   Halucynacje – black box

3. **Analiza obszarów wykorzystania (back office/front office/wsparcie IT)**
4. **Polityki określające zasady wykorzystania AI**
5. **Monitorowanie i rozliczalność.**

Dziękujemy za uwagę