

1. Prowadzenie audytów bezpieczeństwa

Wstępna oraz cykliczna ocena organizacji na zgodność z wymaganiami U.O.D.O. W przypadku uchybień, do Burmistrza kierowane są odpowiednie wnioski. Aktualizacja polityki bezpieczeństwa informacji i instrukcji zarządzania systemami informatycznymi.

2. Opracowanie wymaganej ustawowo dokumentacji ODO

Tworzenie i aktualizacja Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemami Informatycznymi wraz z niezbędnymi załącznikami i formularzami.

3. Kontrola legalności przetwarzania zbiorów danych

Sprawdzenie legalności przetwarzania wszystkich zbiorów

3.1 Wskazanie podstawy legalizującej przetwarzanie - z art. 23, 27, np.: zgoda osoby, wymaganie prawne, dane niezbędne do realizowania umowy, dla dobra publicznego, jako usprawiedliwiony cel administratora, dane medyczne, w trybie KPA

3.2 Sprawdzenie, czy spełniony jest obowiązek informacyjny (czy istnieją odpowiednie klauzule informacyjne), zgodnie z art. 24, 25, 33 podczas kontaktu z klientami/petentami/zatrudnionymi.

W przypadku stwierdzenia uchybień - pomoc w przywróceniu stanu zgodnego z prawnym.

4. Rejestracja i aktualizacja zgłoszonych zbiorów w GIODO

Tam, gdzie jest to wymagane, zgodnie z art. 41 i 43, przeprowadzanie rejestracji, aktualizacji lub wyrejestrowania zbiorów danych osobowych z bazy GIODO.

5. Szkolenia pracowników i współpracowników

Prowadzenie wewnętrznych szkoleń z zasad przestrzegania ochrony danych osobowych.

6. Zarządzanie upoważnieniami i klauzulami poufności

Gromadzenie pisemnych oświadczeń/klauzul poufności od pracowników i podwykonawców. Nadawanie imiennych upoważnień do przetwarzania zbiorów.

7. Prowadzenie ewidencji osób upoważnionych

Prowadzenie i aktualizacja ewidencji osób upoważnionych do przetwarzania zbiorów.

8. Organizacja formalnych zasad współpracy z podmiotami zewnętrznymi

Tworzenie umów powierzenia / poufności, wsparcie podczas negocjacji i podpisania ich przez podmioty posiadające dostęp do danych osobowych.

9. Pomoc w sytuacjach wystąpienia incydentów bezpieczeństwa i sporach

Wsparcie w opanowaniu kryzysów (np. kradzież, wyciek, upublicznienie danych, skargi). Wsparcie prawidłowej komunikacji w kontaktach z policją, GIODO, prasą, poszkodowanymi i innymi instytucjami zainteresowanymi.

10. Reprezentowanie organizacji w kontaktach z GIODO

Prowadzenie kontaktów i korespondencji z GIODO, zarówno w trybie administracyjnym, jak i podczas kontroli.

11. Opiniowanie dokumentów organizacji pod kątem zgodności z wymogami U.O.D.O.

Opiniowanie i dostosowanie dokumentacji organizacji do wymagań UODO (np. klauzule zgody, poufności, informacyjne).

12. Formułowanie wniosków do Burmistrza, dotyczących poprawy bezpieczeństwa danych osobowych

Tam, gdzie to konieczne sporządzanie wniosków wymagających decyzji Burmistrza, np.: zakupu klimatyzatora do serwerowni, szaf zamykanych na klucz.

13. Współpraca z informatykami w zakresie wdrażania wymaganych zabezpieczeń informatycznych

Wyznaczanie wymaganych ustawowo zabezpieczeń. W przypadku braku, nadzór nad ich wdrożeniem, np.: wprowadzenie polityki haseł, zapewnienie kopii bezpieczeństwa.

14. Kontrola zgodności oprogramowania

Pomoc w dostosowaniu, doborze lub zmianie oprogramowania do przetwarzania danych osobowych, aby spełniało wymagania rozporządzenia MSWiA

Uwaga: Wszystkie artykuły przywołane w Załączniku nr 1 odnoszą się do Ustawy O Ochronie Danych Osobowych.