

Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych dla członków DOIIB

§ 1. Cel i zakres stosowania

1. Niniejsza Instrukcja określa zasady postępowania członków DOIIB w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych w rozumieniu przepisów RODO.
2. Instrukcja ma zastosowanie do wszystkich członków DOIIB, w tym pełniących funkcje w organach oraz wykonujących czynności związane z przetwarzaniem danych osobowych w ramach działalności Izby.

§ 2. Definicja naruszenia

1. Naruszeniem ochrony danych osobowych jest każde zdarzenie prowadzące lub mogące prowadzić do naruszenia poufności, integralności lub dostępności danych osobowych, w szczególności:
 1. nieuprawnione ujawnienie danych osobowych,
 2. przekazanie danych niewłaściwemu adresatowi,
 3. utrata, zniszczenie lub nieuprawniona modyfikacja danych,
 4. utrata dokumentów, nośników danych lub sprzętu zawierającego dane osobowe,
 5. naruszenie bezpieczeństwa systemów teleinformatycznych (awaria, błąd oprogramowania, atak zewnętrzny).
2. W przypadku wątpliwości co do kwalifikacji zdarzenia jako naruszenia, członek Izby zobowiązany jest przyjąć zasadę ostrożności i dokonać zgłoszenia do Inspektora Ochrony Danych.

§ 3. Obowiązek niezwłocznego zgłoszenia

1. Członek Izby, który stwierdził naruszenie ochrony danych osobowych lub powziął uzasadnione podejrzenie jego wystąpienia, zobowiązany jest do niezwłocznego poinformowania Inspektora Ochrony Danych.
2. Zgłoszenie następuje bez zbędnej zwłoki, nie później niż w dniu stwierdzenia zdarzenia, przy wykorzystaniu kanałów komunikacji wskazanych w dokumentacji RODO, tj. adresu e-mail: iod@dos.piib.org.pl
3. Brak pełnych informacji nie wstrzymuje obowiązku dokonania zgłoszenia.

§ 4. Zakres informacji przekazywanych w zgłoszeniu

1. Zgłoszenie do Inspektora Ochrony Danych powinno zawierać, w miarę dostępnych informacji:
 1. opis zdarzenia oraz okoliczności jego wystąpienia,
 2. datę i czas stwierdzenia naruszenia,
 3. kategorie danych osobowych, których zdarzenie dotyczy,

4. kategorie osób, których dane dotyczą,
5. informacje o podjętych dotychczas działaniach zabezpieczających.
2. Jeżeli na etapie zgłoszenia nie są dostępne wszystkie informacje, członek Izby zobowiązany jest do ich uzupełnienia niezwłocznie po ich ustaleniu.

§ 5. Zasady postępowania po stwierdzeniu naruszenia

1. Członek Izby zobowiązany jest do podjęcia niezbędnych działań ograniczających skutki naruszenia, o ile jest to możliwe i nie zagraża bezpieczeństwu systemów lub integralności dowodów zdarzenia.
2. Członek Izby zobowiązany jest do zabezpieczenia dostępnych informacji i materiałów związanych ze zdarzeniem w sposób umożliwiający ich analizę przez Inspektora Ochrony Danych.
3. Członek Izby nie podejmuje samodzielnych działań naprawczych wykraczających poza działania zabezpieczające, bez uzgodnienia z Inspektorem Ochrony Danych lub właściwymi jednostkami organizacyjnymi.

§ 6. Zakaz samodzielnej komunikacji z podmiotami zewnętrznymi

1. Członek Izby nie jest uprawniony do samodzielnego:
 1. informowania osób, których dane dotyczą,
 2. zgłaszania naruszenia do Prezesa Urzędu Ochrony Danych Osobowych,
 3. przekazywania informacji o naruszeniu podmiotom trzecim, w tym mediom.
2. Działania komunikacyjne podejmowane są wyłącznie przez Administratora danych przy udziale Inspektora Ochrony Danych.

§ 7. Obowiązek współpracy i poufności

1. Członek Izby zobowiązany jest do współpracy z Inspektorem Ochrony Danych w toku analizy naruszenia, w szczególności do udzielania rzetelnych i kompletnych informacji.
2. Informacje dotyczące naruszenia, w tym jego przebiegu, przyczyn oraz skutków, objęte są obowiązkiem poufności i nie mogą być ujawniane osobom nieuprawnionym.

§ 8. Charakter zgłoszenia naruszenia

1. Zgłoszenie naruszenia do Inspektora Ochrony Danych stanowi realizację obowiązku wynikającego z przepisów prawa oraz regulacji wewnętrznych, w szczególności Polityki Ochrony Danych Osobowych obowiązującej w DOIIB.
2. Sam fakt dokonania zgłoszenia nie stanowi przyznania się do winy i nie może być podstawą do negatywnych konsekwencji wobec członka Izby wyłącznie z tytułu dokonania zgłoszenia.

§ 9. Działania naprawcze i zapobiegawcze

Po zakończeniu obsługi naruszenia członek Izby zobowiązany jest do stosowania zaleceń organizacyjnych i technicznych wprowadzonych w celu zapobiegania podobnym zdarzeniom w przyszłości.