Zał. nr 5 do Polityki

PROCEDURA OBSŁUGI NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Procedura opisuje sposób zbierania informacji o incydentach oraz realizację zadań wynikających z art. 33 i 34 RODO.

Informacje o incydentach i zdarzeniach, które mogą mieć wpływ na bezpieczeństwo danych osobowych mogą wpływać do Administratora danych i IOD, jeżeli został powołany, między innymi z następujących źródeł:
- od pracowników (obowiązek określony w Regulaminie ochrony danych osobowych),
- od ASI (Informatyka),
- z urządzeń monitorujących,
- od podmiotu przetwarzającego.

Każdy zgłoszony incydent i zdarzenie Administrator powinien zweryfikować i stwierdzić czy jest to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Naruszenie ochrony danych to incydent bezpieczeństwa pociągający za sobą skutek w postaci zniszczenia, utraty, nieuprawnionego zmodyfikowania, ujawnienia lub dostępu do danych osób nieuprawnionych. Każde naruszenie ochrony danych powinno być udokumentowane i opisane w Raporcie z naruszenia ochrony danych.

Jeżeli jest mało prawdopodobne, by stwierdzone naruszenie ochrony danych skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych Administrator danych nie ma obowiązku zgłaszać naruszenia organowi nadzorczemu.

W przeciwnym wypadku Administrator danych ma obowiązek bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłosić je organowi nadzorczemu. Zgłoszenie do organu nadzorczego powinno zawierać informacje opisane w art. 33 ust. 3 RODO. Zgłoszenie do organu nadzorczego powinno powstać w oparciu o Raport z naruszenia ochrony danych. Jeżeli Administratorowi nie uda się dochować 72-godzinnego terminu zgłoszenia o wystąpieniu naruszenia ochrony danych, to musi wyjaśnić przyczyny opóźnienia. Możliwa jest również sytuacja, gdy Administrator przekaże do organu nadzorczego niepełne zgłoszenie, a następnie będzie je sukcesywnie uzupełniał.

Art. 34 RODO nakłada, w niektórych przypadkach, na Administratora obowiązek zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych. Taki obowiązek powstaje, jeżeli naruszenie ochrony danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Artykuł 23 ust. 1 RODO przewiduje możliwość wyłączenia w przepisach szczególnych obowiązku informowania osób o naruszeniu ochrony danych. Administrator powinien zatem sprawdzić, czy nie jest wyłączony z takiego obowiązku na mocy obowiązujących go ustaw szczegółowych.

Zawiadomienie osób, których dane dotyczą o naruszeniu ochrony danych nie jest również wymagane, gdy:

- Administrator wdrożył odpowiednie techniczne o organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności szyfrowanie, które uniemożliwia odczyt danych przez osoby nieuprawnione,
- Administrator, po stwierdzeniu naruszenia, zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osoby, której dane dotyczą,
- powiadomienie wszystkich osób wymagałoby niewspółmiernego wysiłku – wtedy należy wydać publiczny komunikat o zdarzeniu.

Zawiadomienie osoby, której dane dotyczą o naruszeniu powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej następujące informacje:

- imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opis możliwych konsekwencji naruszenia ochrony danych osobowych,
- opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownym przypadku środków służących zminimalizowaniu ewentualnych negatywnych skutków naruszenia.