TRYB I ZASADY POSTĘPOWANIA W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH

O naruszeniu ochrony danych osobowych mówimy wtedy, gdy naruszenie bezpieczeństwa prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych, lub w inny sposób przetwarzanych. (art. 4 pkt 12 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1 z dnia 2016.05.04))

Niniejszy załącznik określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku gdy:
1) stwierdzono naruszenie zabezpieczeń mechanicznych pomieszczeń,
2) stwierdzono naruszenie zabezpieczenia danych w systemie informatycznym,
3) sposób działania programu, ujawnione metody pracy, zawartość zbioru danych osobowych, wskazują na naruszenie zabezpieczeń danych,
4) stan urządzenia, jakość komunikacji w sieci teleinformatycznej wskazuje na naruszenie zabezpieczeń systemu informatycznego,
5) stwierdzono niekontrolowane wprowadzenie, usunięcie, modyfikację, edycję, zniekształcenie danych,
6) otrzymano zgłoszenie na okoliczność domniemanego naruszenia bezpieczeństwa,
7) istnieje ryzyko naruszenia praw wolności podmiotu przetwarzanych danych.

I. Tryb i zasady postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych osobowych w systemie tradycyjnym.

1) W przypadku stwierdzenia naruszenia zabezpieczenia dostępu do danych w formie kartotek, zestawień, wykazów (włamania do pomieszczenia) osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym IOD oraz administratora budynku.
2) IOD i administrator budynku po otrzymaniu powiadomienia:
a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia danych osobowych (zamkniecie pomieszczeń, zmiana zamków),
b) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
c) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,
d) po przywróceniu prawidłowego stanu systemu zabezpieczeń przetwarzania tradycyjnego, dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,

e) sporządza szczegółowy raport zawierający w szczególności:
- datę i godzinę otrzymania informacji o naruszeniu (włamaniu do pomieszczenia),
- opis jego przebiegu,
- przyczyny oraz wnioski ze zdarzenia.
3) Raport wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) IOD przekazuje Administratorowi.
4) IOD w porozumieniu z Administratorem podejmuje niezbędne działania w celu zapobieżenia naruszeniom zabezpieczeń danych w systemie w przyszłości.

II. Tryb i zasady postępowania w przypadku naruszenia zabezpieczenia danych osobowych w systemie informatycznym.

PROCEDURA POSTĘPOWANIA PRZY PODEJRZENIU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

O podejrzeniu naruszenia ochrony danych osobowych możemy mówić wtedy, gdy administrator bezpieczeństwa informacji wejdzie w posiadanie informacji o naruszeniu któregoś z zabezpieczeń stałych (czy to poprzez włamanie, próbę włamania, zaniedbanie pracownika, lub drobny incydent) lub o wyraźnym zaniedbaniu (zaniechaniu) któregoś z zabezpieczeń okresowych.

a) należy skontrolować stan zabezpieczeń stałych i okresowych,
b) kompetentny pracownik powinien przejrzeć dane, by określić czy nie zostały zniszczone lub uszkodzone,
c) należy sprawdzić nośniki, wydruki i inne dokumenty papierowe, etc. oraz skontrolować techniczną sprawność sprzętu komputerowego.

PROCEDURA POSTĘPOWANIA PRZY NARUSZENIU OCHRONY DANYCH OSOBOWYCH

O naruszeniu ochrony danych osobowych mówimy wtedy, gdy mamy pewność, że ochrona danych osobowych została naruszona.

a) w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym (włamania do systemu) osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o IOD oraz ASI,

b) należy zabezpieczyć dane,

c) jeżeli jest to możliwe, należy przeciwdziałać rozpowszechnianiu zagrożonych danych,

d) jeżeli dane zostały zniszczone (uszkodzone) w stopniu, który kompetentny pracownik uzna za wysoki, należy odtworzyć dane z kopii zapasowych,

e) ASI (LASI) usuwa nieszczelności systemu informatycznego,

f) ASI (LASI) zabezpiecza dane,

g) IOD z ASI ocenia skalę naruszenia bezpieczeństwa danych osobowych,

h) IOD opisuje naruszenie (czas wystąpienia, osoba zgłaszająca, chronologia i opis zdarzenia, możliwe skutki wystąpienia zdarzenia, podjęte działania, uwagi),

i) ASI przywraca system informatyczny do stanu umożliwiającego poprawne i bezpiecznego przetwarzania danych osobowych,

j) IOD ustala osoby odpowiedzialne za naruszenie ochrony danych osobowych,

k) IOD z ASI podejmuje czynności zabezpieczające system informatyczny przed ponownym naruszeniem ochrony danych osobowych,

l) IOD przeciwdziała rozpowszechnianiu zagrożonych danych,

ł) IOD (ADO) zgodnie z art. 33 RODO zgłasza naruszenia ochrony danych osobowych organowi nadzorczemu (UODO),

m) IOD (ADO) zgodnie z art. 34 RODO zawiadamia osobę, której dane dotyczą o naruszeniu ochrony danych osobowych.

PROCEDURA POSTĘPOWANIA PRZY PERMANENTNYM NARUSZANIU OCHRONY DANYCH OSOBOWYCH

O permanentnym naruszaniu ochrony danych osobowych mówimy, gdy pomimo działań IOD i innych podjętych wskutek naruszenia ochrony danych osobowych stan się nie poprawia i następują ponownie przypadki naruszenia tej ochrony

a) należy zawiadomić Administratora o zaistniałym przypadku permanentnego naruszenia ochrony danych osobowych,
b) należy zabezpieczyć kopie archiwalne danych,
c) należy cofnąć uprawnienia wszystkich użytkowników posiadających dostęp do danej bazy danych, jeżeli nawet to nie pomoże, należy zniszczyć bazę danych (pamiętając o zabezpieczeniu kopii archiwalnych).

II. TRYB POSTĘPOWANIA IOD I ASI PO UZYSKANIU INFORMACJI O NARUSZENIU ZABEZPIECZEŃ DANYCH OSOBOWYCH

1) IOD i ASI po otrzymaniu powiadomienia (stosownie do przypuszczalnego rodzaju naruszeń):
a) sprawdza zawartość zbioru danych osobowych,
b) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,
c) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych;
d) sprawdza sposób działania programu (w tym również obecność wirusów komputerowych),
e) sprawdza jakość komunikacji w sieci teleinformatycznej.

2) IOD i ASI w przypadku stwierdzenia naruszenia zabezpieczeń danych :
a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci teleinformatycznej, do programów oraz zbiorów danych itp.),
b) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia (logi systemu oraz logi aplikacji),
c) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,
d) niezwłocznie przywraca prawidłowy stan działania systemu,
e) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek ich naruszenia,
f) sporządza szczegółowy raport zawierający w szczególności:
- datę i godzinę otrzymania informacji o naruszeniu,
- opis jego przebiegu,
- przyczyny oraz wnioski ze zdarzenia.

3) IOD w porozumieniu z Administratorem podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:
a) jeżeli przyczyną zdarzenia były błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, wadliwe metody pracy, przeprowadza dodatkowe szkolenia osób biorących udział przy przetwarzaniu danych,
b) w uzasadnionych przypadkach wnioskuje o wyciągnięcie konsekwencji przewidzianych prawem wobec winnych zaniedbań,
c) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, niezwłocznie poleca administratorowi systemu informatycznego przeprowadzenie, w stosownym zakresie, przeglądu oraz konserwacji urządzeń i programów,
d) w przypadku uaktywnienia się wirusa komputerowego niezwłocznie poleca ASI ustalenie źródła pochodzenia wirusa (o ile jest to możliwe) oraz wdrożenie skuteczniejszych zabezpieczeń antywirusowych,

e) w przypadku złej jakości komunikacji w sieci teleinformatycznej niezwłocznie poleca administratorowi systemu informatycznego wymianę urządzeń powodujących złe funkcjonowanie sieci.

4) Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) IOD przekazuje Administratorowi.