Instrukcja nr 1 do Polityki
bezpieczeństwa danych w
systemach informacyjnych.

Instrukcja
postępowania w sytuacji naruszenia ochrony danych w tym danych osobowych.

§ 1

Niniejsza instrukcja przeznaczona jest dla osób przetwarzających dane w tym dane osobowe zwykłe i dane szczególnej kategorii w Instytucie Matki i Dziecka i określa tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

§ 2

1. Za naruszenie ochrony danych osobowych (incydent) uważa się 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, a w szczególności:
   a. nieuprawniony dostęp lub próbę dostępu do systemu informatycznego lub pomieszczeń, w których następuje proces przetwarzania danych osobowych (widoczne uszkodzenia bądź naruszenia zabezpieczeń),
   b. naruszenie lub próbę naruszenia integralności zbioru danych i/lub systemu informatycznego, w którym przetwarzane są dane osobowe,
   c. nieautoryzowane zniszczenie lub próbę zniszczenia danych zgromadzonych w formie papierowej i/lub w systemie informatycznym,
   d. zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany,
   e. nieuprawniony dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem),
   f. inny stan systemu informatycznego lub pomieszczeń, w których następuje proces przetwarzania danych osobowych niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy,
   g. podejrzenie wycieku danych osobowych,
   h. zagubienie lub nieautoryzowane usunięcie danych osobowych,
   i. podejrzenie, że do systemów informatycznych lub pomieszczeń, gdzie są przetwarzane dane osobowe miały dostęp osoby nieuprawnione.
2. Naruszenia mogą dotyczyć zarówno danych osobowych przetwarzanych w formie elektronicznej, jak i papierowej.

§ 3

1. W przypadku zaistnienia zdarzeń (incydentu) zagrażających bezpieczeństwu danych osobowych, a szczególnie naruszenia, podejrzenia lub możliwości naruszenia systemu ochrony danych osobowych użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Kierownika użytkownika. W razie nieobecności należy powiadomić osobę zastępującą.
2. Obowiązek określony w § 3 pkt. 1 ciąży również na pozostałych pracownikach Administratora Danych.
3. Kierownik użytkownika, o zaistniałym incydencie niezwłocznie informuje Inspektora Ochrony Danych lub jego Zastępcę, oraz udaje się na miejsce wystąpienia incydentu.
4. Do czasu przybycia Inspektora Ochrony Danych lub jego Zastępcy, zgłaszający wraz z Kierownikiem użytkownika:

a) zabezpiecza dowody naruszenia, urządzeń, na których stwierdzono naruszenia oraz pomieszczeń, w których doszło do naruszenia ochrony danych, a zwłaszcza danych osobowych lub danych medycznych;
b) nie rozpoczyna lub nie kontynuuje pracy, jak również nie podejmuje czynności mogących spowodować zatarcie śladów naruszenia ochrony danych, a zwłaszcza danych osobowych lub danych medycznych;
c) podejmuje inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować dalszą utratą danych, a zwłaszcza danych osobowych lub danych medycznych.

5. Zgłaszający oraz osoby zatrudnione przy przetwarzaniu danych w miejscu wystąpienia incydentu mogą kontynuować prace dopiero po otrzymaniu pozwolenia od osoby wyjaśniającej sprawę, czyli Inspektora Ochrony Danych lub jego Zastępcy.

§ 4

1. W sytuacji, o której mowa w §3 Inspektor Ochrony Danych lub jego Zastępca, przy współpracy z Kierownikiem użytkownika po przybyciu na miejsce zaistnienia incydentu:
   a) ocenia zaistniałą sytuację, biorąc pod uwagę: stan urządzeń, stan zbioru danych, stan pomieszczeń, a następnie identyfikuje negatywne następstwa zaistniałego incydentu;
   b) przeprowadza z pracownikami rozmowę wyjaśniającą zaistniałe naruszenie,
   c) podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia.
2. Następnie sporządza raport z przebiegu zdarzenia, w którym powinny znaleźć się następujące informacje:
   a) miejsce i data sporządzenia raportu, oraz numer ewidencyjny raportu;
   b) data i godzina zgłoszenia incydentu, oraz osoba zgłaszająca;
   c) data i godzina stwierdzenia wystąpienia incydentu przez osobę zgłaszającą;
   d) osoba odpowiedzialna za powstały incydent;
   e) opis incydentu, oraz sytuacji;
   f) podjęte działania i uzasadnienie tych działań.
   g) rekomendacje dotyczące zgłoszenia incydentu do organu nadzorczego oraz poinformowania osoby (osób), której (których) dane dotyczą.
3. Kopia sporządzonego raportu przekazywana jest niezwłocznie Administratorowi Danych, oraz Inspektorowi Ochrony Danych w przypadku, gdy raport został przygotowany przez jego Zastępcę.
4. Administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Treść zgłoszenie reguluje art. 33 RODO.
5. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Treść powiadomienia reguluje art. 34 RODO.

§ 5

1. Inspektor Ochrony Danych lub jego Zastępca podejmuje działania celem likwidacji naruszenia ochrony danych, oraz zapobiega ponownemu ich wystąpieniu. W tym celu:
   a) W miarę posiadanych możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu, określonymi w Polityce Bezpieczeństwa.
   b) Po wyczerpaniu niezbędnych środków doraźnych zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych oraz terminu wznowienia przetwarzania danych.

c) W razie potrzeby nakazuje odpowiednim osobom odtworzenie utraconych danych (np. z kopii bezpieczeństwa, poprzez uzupełnienie brakujących wpisów, poprzez naprawę zbioru danych).
d) W razie potrzeby wnioskuje o wprowadzenie nowych form zabezpieczeń.
e) Informuje Administratora Danych o wykonanych czynnościach.
f) Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy przeprowadzonej przez Dyrekcję Instytutu, Inspektora Ochrony Danych i Zastępcy Inspektora Ochrony Danych.

§ 6

W sprawach nie uregulowanych w instrukcji mają zastosowanie przepisy RODO.

§ 7

1. Administrator prowadzi ewidencję zaistniałych incydentów może być prowadzona w formie tradycyjnej (papierowej) lub w formie elektronicznej.
2. W Ewidencji powinny być zamieszczone wszelkie informacje dotyczące zaistniałego incydentu, a w szczególności:
    a) Numer naruszenia.
    b) Opis naruszenia.
    c) Datę i godzinę zgłoszenia do UODO.
    d) Datę zawiadomienia osoby (osób), której (których) dane dotyczą.
    e) Datę i godzinę stwierdzenia naruszenia.
    f) Datę i godzinę powstania naruszenia (jeśli jest to możliwe).
    g) Kategorię oraz liczbę osób, których naruszenie dotyczy.
    h) Zakres danych, których dotyczy naruszenie.
    i) Opis skutku/konsekwencji naruszenia.
    j) Środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
    k) Prawdopodobieństwo naruszenia praw i wolności osób, których dane dotyczą.
3. W Ewidencji powinno być ujęte każde zdarzenie będące incydentem zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych, danych osobowych i danych medycznych”.