

Procedura postępowania w sytuacji naruszenia ochrony danych osobowych

Spis treści

Istota naruszenia danych osobowych	3
Postępowanie w przypadku naruszenia danych osobowych	3
Naruszenie danych osobowych - odpowiedzialność	5
Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu	6
Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych	7
Postanowienia końcowe	7

§ 1

Istota naruszenia danych osobowych

1. Zdarzeniem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
 - a) nieautoryzowany dostęp do danych,
 - b) nieautoryzowane modyfikacje lub zniszczenie danych,
 - c) udostępnienie danych nieautoryzowanym podmiotom,
 - d) nielegalne ujawnienie danych,
 - e) pozyskiwanie danych z nielegalnych źródeł.

§ 2

Postępowanie w przypadku naruszenia danych osobowych

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu.
2. Przełożony zgłasza fakt Inspektorowi ochrony danych.
3. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych:
 - a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
 - b) dokumentacja jest niszczona w sposób umożliwiający identyfikację
 - c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
 - d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

- e) nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,
- f) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
- g) wnoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;
- h) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
- i) stwierdzenie próby lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji); j. telefoniczne próby wyłudzenia danych osobowych;
- j) kradzież komputerów lub twardych dysków z danymi osobowymi;
- k) utrata kontroli nad kopią danych osobowych;
- l) maile zachęcające do ujawnienia identyfikatora i/lub hasła;
- m) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
- n) istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki"
- o) hasła do systemów przechowywane są w pobliżu komputera.

§ 3

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .

§ 4

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać

bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora danych.

§ 5

Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora ochrony danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6

Inspektor ochrony danych podejmuje następujące kroki:

- 1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
- 2) odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
- 3) nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7

Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając Protokół naruszenia, który stanowi załącznik do Polityki Bezpieczeństwa Informacji.

§ 8

1. Inspektor ochrony danych zasięga potrzebnych opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych).
2. Uzupełnia również Rejestr zdarzeń, który stanowi załącznik do Polityki Bezpieczeństwa Informacji.

§ 9

Naruszenie danych osobowych - odpowiedzialność

1. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej

osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe.

2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.
3. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§ 10

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorcemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Do zgłoszenia przekazanego organowi nadzorcemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
 - a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
 - b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
 - c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
 - d) opisywać 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.
4. Jeżeli powyższych informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorcemu weryfikowanie przestrzegania niniejszego artykułu.

§ 11

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. 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.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 lit. b), c) i d).
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
 - a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
 - b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
 - c) wymagałoby ono niewspółmiernie dużego wysiłku.
4. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

§ 12

Postanowienia końcowe

1. Pracodawca jest obowiązany zapoznać pracownika z treścią niniejszej Procedury przed dopuszczeniem go do pracy.
2. Procedura zostaje wprowadzona na czas nieokreślony.