PROCEDURA ZGŁASZANIA NARUSZEŃ

Spis treści

PROCEDURA POSTĘPOWANIA W SYTUACJI NOSZĄCEJ ZNAMIONA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

I. ISTOTA NARUSZENIA DANYCH OSOBOWYCH

§ 1

Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawniania danych osobowych, udostępniania lub umożliwiania dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1. nieautoryzowany dostęp do danych;
2. spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub kopiowanie danych osobowych;
3. nieautoryzowane modyfikacje lub zniszczenie danych;
4. udostępnienie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
5. nielegalne ujawnianie danych;
6. pozyskiwanie danych z nielegalnych źródeł;
7. przetwarzanie danych bez upoważnienia lub niezgodnie z zakresem określonym w nadanym upoważnieniu;
8. niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
9. naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe;
10. zaniechanie, choćby nieumyślne dopełnienie obowiązku zapewnienia danym ochrony;
11. niewłaściwe zaadresowanie wiadomości e-mail (z ujawnieniem wszystkich adresatów) np. wysłanie wezwania do zapłaty do wielu klientów, potwierdzenie usunięcia konta;
12. spowodowanie incydentu naruszającego prawa osób, których dane są przetwarzane.

II. PRZYKŁADY SYTUACJI NIOSĄCYCH ZA SOBĄ RYZYKO NARUSZENIA

§ 1

Przykładami sytuacji, niosących za sobą ryzyko naruszenia są:

1. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
2. dokumentacja niszczona bez użycia niszczarki;
3. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
4. stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji m.in.:
   - otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe pod nieobecność w pomieszczeniu pracowników;
   - nieodpowiednie zabezpieczenie dokumentacji archiwalnej;
   - przechowywanie danych osobowych w formie tradycyjnej (papierowej) oraz na nośnikach przenośnych (m.in. pendrive) w miejscach ogólnodostępnych i niezabezpieczonych;
   - pozostawienie wydruków z danymi osobowymi na drukarce lub kserokopiarce;
5. niewylogowanie się przed opuszczeniem stanowiska pracy, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych;
6. ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe;
7. wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz podmiotu bez upoważnienia;
8. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
9. próba modyfikacji danych bez odpowiedniego upoważnienia (autoryzacji);
10. telefoniczne próby wyłudzenia danych osobowych;
11. kradzież komputerów lub twardych dysków z danymi osobowymi;
12. utrata kontroli nad kopią danych osobowych;

13. wiadomości e-mail zachęcające do ujawnienia identyfikatora i/lub hasła;
14. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
15. istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki";
16. hasła i loginy do systemów przechowywane w pobliżu komputera.

III. POSTĘPOWANIE W PRZYPADKU NARUSZENIA DANYCH OSOBOWYCH

§ 1

W przypadku stwierdzenia naruszenia bezpieczeństwa danych, należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz (w sytuacjach na to pozwalających) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych (IOD) lub innej osoby upoważnionej przez Administratora danych.

§ 2

O naruszeniu należy niezwłocznie, nie później niż w terminie 24 godzin od powzięcia informacji, iż do takiego naruszenia doszło powiadomić IOD za pośrednictwem adresu e-mail: iod@ahe.lodz.pl oraz w razie potrzeby powołanego Administratora Systemu Informatycznego (ASI), zanim fakt zostanie zgłoszony do organu nadzorczego, a także w przypadku żądania wyjaśnień przez organy prowadzące postępowania przygotowawcze, organy nadzorcze lub w przypadku sporów związanych z przetwarzaniem danych osobowych. Powiadomienia należy zgłosić w formie pisemnej wiadomości, zawierającej ogólny opis zdarzenia.

§ 3

W celu realizacji procedury postępowania w przypadku naruszenia bezpieczeństwa danych osobowych IOD, ASI lub inna upoważniona przez Administratora danych osoba ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

1. żądania wyjaśnień od pracowników/współpracowników Administratora danych;
2. korzystania z pomocy konsultantów (w tym zewnętrznych podmiotów);
3. nakazanie przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§ 4

IOD dokonuje oceny skali incydentu, biorąc pod uwagę wszelkie możliwe szkody i krzywdy, które mogą z niego wynikać dla osób fizycznych. Po ocenie skali, podjęta zostaje decyzja o zakwalifikowaniu incydentu jako naruszenia, które wymaga zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych.

IV. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

§ 1

W przypadku naruszenia ochrony danych osobowych, Administrator danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, 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.

§ 2

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu, powinno co najmniej:

1. 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;
2. oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji;
3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

4. opisywać środki zastosowane lub proponowane przez Administratora danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli (w zakresie, w jakim) – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

§ 3

Administrator danych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

V. ZAWIADOMIENIE 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 danych bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu.

Zawiadomienie, o którym mowa powyżej, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w rozdziale IV pkt. 2 powyżej.

Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych nie jest wymagane w następujących przypadkach:

1. Administrator danych 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.
2. Administrator danych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.
3. Wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku, wydany zostaje komunikat publiczny lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane równie w skuteczny sposób.

VI. DOKUMENTOWANIE NARUSZEŃ

§ 1

IOD dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze zgodnie z arkuszem incydentów niniejszej Procedury.

PROCEDURA ZARZĄDZANIA NARUSZENIAMI OCHRONY DANYCH OSOBOWYCH

I. IDENTYFIKACJA ZAGROŻEŃ

§ 1

IOD określa rodzaj danych, wobec których zaszło podejrzenie wystąpienia naruszenia ochrony danych.

§ 2

IOD po zidentyfikowaniu naruszenia ochrony danych, przeprowadza ocenę wagi naruszenia.

Przeprowadzenie oceny wagi naruszenia pozwoli na podjęcie decyzji, zarówno o powiadomieniu organu nadzorczego, jakim jest Prezes Urzędu Ochrony Danych Osobowych o wystąpieniu naruszenia, jak i osób których dane zostały naruszone.

§ 3

IOD określa potencjalne skutki zidentyfikowanego naruszenia, które mogą prowadzić do wystąpienia ograniczenia prawa i wolności osób, których dane dotyczą w związku z wystąpieniem naruszenia.

§ 4

IOD na podstawie zebranych informacji określa przyczyny wystąpienia incydentu, które są częścią składową niezbędną do przeprowadzenia oceny naruszenia.

II. METODYKA OCENY WAGI NARUSZENIA WG ENISA

§ 1

Ocena wagi naruszenia dokonywana jest na podstawie poniższego wzoru:

WN=KPD*PI+ON

gdzie:

WN – Waga Naruszenia – określa stopień potencjalnego wpływu naruszenia na prawa i wolności osób, których dane dotyczą.

KPD – Kontekst Przetwarzania Danych – określa poziom krytyczności zestawu naruszonych danych w konkretnym kontekście przetwarzania.

PI – Prawdopodobieństwo Identyfikacji – określa czynnik korygujący kontekst przetwarzania danych, który obniża możliwość identyfikacji osoby na podstawie naruszonych danych dla osób, które uzyskały do nich dostęp.

ON – Okoliczności Naruszenia – określa czynnik wzmacniający wagę naruszenia, który odnosi się do okoliczności naruszenia.

1. Kontekst przetwarzania danych obliczany jest na podstawie poniższego wzoru:

KPD=A+B

gdzie:

A – określa rodzaj i poziom wrażliwości danych:

- Dane podstawowe = 1
- Dane dotyczące zachowań osoby = 2
- Dane finansowe = 3
- Dane szczególnej kategorii = 4

B – określa kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę:

- Szeroki zakres danych/ wolumen danych (+)
- Charakter danych (+/-)
- Specyfikacja podmiotu danych lub Administratora danych (+/-)
- Możliwe negatywne skutki dla podmiotu danych (+)
- Publiczna dostępność danych przed naruszeniem (-)
- Nieważność danych (-)
- Inne wpływające na wycenę (+/-)

2. Prawdopodobieństwo identyfikacji może przyjąć cztery poziomy identyfikacji osoby, której dotyczyło naruszenie danych, a mianowicie:
   - Znikome = 0,25
   - Ograniczone = 0,5
   - Wysokie = 0,75
   - Maksymalne = 1

3. Okoliczności naruszenia - są to atrybuty bezpieczeństwa, mianowicie: poufność, integralność, dostępność oraz intencjonalne działanie sprawcy, które po zsumowaniu określą wartość czynników, które wypłynęły na okoliczności naruszenia.

ON=NP+NI+ND+IDS

Naruszenie poufności (NP) – dane ujawnione:

- Znane odbiorcom (+0,25)
- Nieznane liczbie odbiorców danych (+0,5)

Naruszenie integralności (NI) – dane zmienione:

- Możliwe jest ich odzyskanie (+0,25)
- Brak jest możliwości ich odzyskania (+0,5)

Naruszenie dostępności (ND) – niedostępność danych

- Czasowa (+0,25)
- Pełna i brak możliwości ich odzyskania przez Administratora danych lub podmiot przetwarzający (+0,5)

Intencjonalne działanie sprawcy (IDS) - (+0,5)

III. OCENA WAGI NARUSZENIA

§ 1

Administrator danych na podstawie przeprowadzonej oceny wagi naruszenia i otrzymanych wyników, podejmuje stosowne działania zgodne z poniższą tabelą nr 1, określającą wagę naruszenia.

Tabela nr 1

Wynik	*Waga naruszenia*	*Opis*	*Działanie*
WN<2	***Niska***	***Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności.***	***Odnotowanie incydentu w rejestrze incydentów.***
2<=WN<3	***Średnia***	***Osoby mogą dotknąć niedogodności, które są możliwe do pokonania.***	***Odnotowanie incydentu w rejestrze incydentów oraz zgłoszenie do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych.***
3<=WN<4	***Wysoka***	***Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami.***	***Odnotowanie incydentu w rejestrze incydentów oraz zgłoszenie do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych.***

4<=WN	*Bardzo wysoka*	*Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje.*	*Odnotowanie incydentu w rejestrze incydentów oraz zgłoszenie do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych oraz powiadomienie osób, których dane zostały naruszone.*

ARKUSZ INCYDENTU

I. Incydent					
	Miejsce i data incydentu				
	Opis incydentu				
	Czy incydent stanowił naruszenie ?	***TAK***	☐	***NIE***	☐
II. Naruszenie					
	Rodzaj naruszenia	***Naruszenie ochrony danych osobowych, które nie podlega zgłoszeniu organowi nadzorczemu*** *(naruszenie ochrony danych osobowych nie spowodowało ryzyka naruszenia praw i wolności osób fizycznych)*			☐
		Naruszenie, o którym trzeba zawiadomić zarówno organ nadzorczy, jak i osobę, której dane dotyczą *(naruszenie ochrony danych osobowych spowodowało wysokie ryzyko naruszenia praw lub wolności osób fizycznych)*			☐
		Naruszenie podlegające zgłoszeniu jedynie organowi nadzorczemu *(jest mało prawdopodobne, aby naruszenie skutkowało wysokim ryzykiem naruszenia praw lub wolności osób fizycznych)*			☐
		Naruszenie podlegające zgłoszeniu jedynie organowi nadzorczemu (*naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, jednakże zawiadomienie osoby, której dane dotyczą, nie jest konieczne ze względu na wypełnienie przesłanek: i. Administrator danych 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; ii. Administrator danych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; iii. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku Administrator danych wydaje publiczny komunikat, lub stosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.*			☐
	Kategoria i przybliżona liczba osób, których dane dotyczą				
	Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie				
	Okoliczności naruszenia ochrony danych osobowych.				
	Skutki naruszenia ochrony danych osobowych				

	Podjęte działania zaradcze	
	Dzień zgłoszenia incydentu naruszenia ochrony danych osobowych organowi nadzorczemu (jeżeli dotyczy)	
	Dzień zawiadomienia osób, których dane dotyczą (jeżeli dotyczy)	

REJESTR INCYDENTÓW

Lp.	*Opis zdarzenia/ incydentu/ słabości*	*Nazwa systemu i/lub usługi*	*Kategoria*	*Wykrycie*			*Podjęcie działań*		*Data zamknięcia incydentu*	*Uwagi*
				Data	*Godz.*	*Czas trwania*	*Data*	*Godz.*		
1.										
2.										
3.										
4.										
5.										