Spis treści

1. PRZEDMIOT / CEL

Celem niniejszego dokumentu jest opisanie sposobu postępowania w przypadku wykrycia incydentu skutkującego naruszeniem bezpieczeństwa danych osobowych.

2. ODPOWIEDZIALNOŚĆ

2.1. Inspektor Ochrony Danych monitoruje realizacje założeń niniejszego dokumentu, by przetwarzanie pozostawało w zgodzie z Rozporządzeniem.

2.2. Obowiązek zgłaszania incydentów skutkujących naruszeniem bezpieczeństwa danych osobowych ciąży na każdym pracowniku i współpracowniku oraz osobie za pomocą której NRA wykonuje swoje obowiązki.

2.3. Dział IT jest odpowiedzialny za podjęcie działań mających na celu wyjaśnienie incydentu, w tym minimalizację wynikających z niego skutków, opisanie incydentu oraz przekazanie stosownych informacji Dyrektorowi Biura Naczelnej Rady Adwokackiej oraz, gdy zachodzi taka potrzeba, IOD.

2.4. Naczelna Rada Adwokacka jest odpowiedzialna za zgłoszenie incydentu do organu nadzorczego i osoby, której dane dotyczą, jeśli zachodzą ku temu przesłanki określone w art. 33 i 34 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) (dalej jako RODO).

2.5. Prezes Naczelnej Rady Adwokackiej przy pomocy Dyrektora Biura Naczelnej Rady Adwokackiej odpowiedzialny jest za podjęcie decyzji o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo.

3. DEFINICJA NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

3.1. Przez naruszenie ochrony danych osobowych należy rozumieć 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.

3.2. Na potrzeby niniejszej procedury wprowadza się następujące pojęcia:

3.2.1. atak - próba zniszczenia, ujawnienia, zmiany, uniemożliwienia dostępu, kradzieży lub uzyskania nieautoryzowanego dostępu albo nieautoryzowanego użycia danych osobowych

3.2.2. zdarzenie związane z bezpieczeństwem danych osobowych - stwierdzone wystąpienie stanu systemu, usługi lub sieci, który wskazuje na możliwe naruszenie procedur bezpieczeństwa NRA lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem danych osobowych

3.3. Za naruszenie bezpieczeństwa danych osobowych uznawany jest każdy stwierdzony fakt (w tym atak skutkujący wystąpieniem zdarzenia) oraz uzasadnione podejrzenie wystąpienia zdarzenia, w szczególności:

3.3.1. nieuprawnione ujawnienie danych osobowych

3.3.2. naruszenie hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać informacje bez wprowadzenia hasła)

3.3.3. częściowy lub całkowity brak informacji, w tym danych osobowych albo dostęp do informacji w zakresie szerszym niż wynikający z przyznanych uprawnień

3.3.4. brak dostępu do właściwej aplikacji lub zmiana zakresu wyznaczonego dostępu do zasobów serwera

3.3.5. wykrycie wirusa komputerowego

3.3.6. zauważenie elektronicznych śladów próby włamania do systemu informatycznego

3.3.7. znaczne spowolnienie działania systemu informatycznego

3.3.8. podejrzenie kradzieży sprzętu komputerowego lub dokumentów zawierających chronione informacje

3.3.9. istotna zmiana położenia sprzętu komputerowego

3.3.10. zauważenie śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf

3.3.11. zabrania informacji chronionych, w tym danych osobowych przez osobę nieuprawnioną

3.3.12. uszkodzenie lub zniszczenie informacji lub jakiegokolwiek elementu systemu informatycznego

3.3.13. działanie wbrew postanowieniom procedur bezpieczeństwa danych osobowych obowiązujących w NRA.

4. TRYB POSTĘPOWANIA

4.1. Każdy pracownik / współpracownik oraz osoba za pomocą której NRA wykonuje swoje obowiązki posiadająca informacje o ataku, zdarzeniu lub innym naruszeniu albo uzasadnione podejrzenie wystąpienia ataku, zdarzenia lub naruszenia bezpieczeństwa danych osobowych, obowiązana jest bezzwłocznie poinformować o danym fakcie Dyrektora Biura Naczelnej Rady Adwokackiej według wzoru stanowiącego Załącznik nr 1 do niniejszej procedury, który następnie informuje Dział IT. Do czasu przybycia na miejsce przedstawiciela Działu IT, podejmuje się tylko takie czynności, które zmierzają do:

4.1.1. zabezpieczenia śladów naruszenia

4.1.2. zapobieżenia dalszym zagrożeniom

4.1.3. powstrzymania skutków naruszenia

4.1.4. ustalenia przyczyny i sprawcy naruszenia

4.1.5. przygotowania opisu incydentu

4.2. Pracownik / współpracownik oraz osoba, za pomocą której NRA wykonuje swoje obowiązki nie opuszcza bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia przedstawiciela Działu IT.

4.3. Dział IT powinien niezwłocznie:

4.3.1. przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia bezpieczeństwa danych osobowych

4.3.2. podjąć działania chroniące system przed ponownym naruszeniem

4.3.3. w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych odnotować fakt wystąpienia incydentu w ewidencji incydentów (Załącznik nr 2 do niniejszej procedury), a następnie niezwłocznie, nie później niż w ciągu 48 godzin od wykrycia zdarzenia, przesłać jego opis do Dyrektora Biura Naczelnej Rady Adwokackiej oraz do IOD.

4.4. Dyrektor Biura Naczelnej Rady Adwokackiej w uzgodnieniu z Działem IT mogą zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.

4.5. W razie odtwarzania informacji z kopii zapasowych, Dział IT obowiązany jest upewnić się, że odtwarzane informacje zapisane zostały przed wystąpieniem zdarzenia (dotyczy to zwłaszcza przypadków infekcji wirusowej).

4.6. Naczelna Rada Adwokacka, po zapoznaniu się z opisem zdarzenia, podejmuje – po przeprowadzeniu konsultacji z IOD- decyzję o ewentualnym powiadomieniu organu nadzorczego oraz, jeśli to konieczne osoby (osób), której dane dotyczą.

4.6.1. Zawiadomienie organu nadzorczego musi nastąpić bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

4.6.2. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

4.6.3. Zgłoszenie do organu nadzorczego 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 IOD 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 danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków

4.6.4. Jeżeli informacji, o których mowa w podpunkcie c) powyżej nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

4.6.5. Naczelna Rada Adwokacka 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 art. 33 RODO.

4.6.6. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Naczelna Rada Adwokacka, bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie to musi zostać sformułowane jasnym i prostym językiem i opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej:

a) imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji
b) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych
c) 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.

4.6.7. Zawiadomienie, o którym mowa w podpunkcie 4.7.6. powyżej, nie jest wymagane, w następujących przypadkach:

a) 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
b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą
c) wymagałoby ono niewspółmiernie dużego wysiłku. 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.

5. GROMADZENIE MATERIAŁU DOWODOWEGO

5.1. Każdy element materiału dowodowego – dokument papierowy, dokument elektroniczny, kopia zapasowa bazy danych lub plików systemowych i konfiguracyjnych, obraz dysku, dziennik (logów) zdarzeń, dziennik audytu – jest gromadzony i przechowywany w sposób gwarantujący jego poufność, integralność i kompletność.

5.2. Każdy element materiału dowodowego jest utrwalany z zachowaniem integralności całego procesu przetwarzania, od utworzenia do ewentualnego przedstawienia jako dowodu w postępowaniu sądowym:

5.2.1. dla dokumentów papierowych - oryginał jest bezpiecznie przechowywany wraz z informacją o źródle, czasie i okolicznościach utrwalenia dokumentu

5.2.2. dla zapisów utrwalanych na nośnikach komputerowych – sporządzenie kopii zapasowej lub obrazu dysku wraz z udokumentowaniem procesu kopiowania oraz bezpieczne ich przechowanie.

5.3. Wszelkie działania w systemie informatycznym, związane z postępowaniem ze zdarzeniami, mogą być prowadzone wyłącznie z wykorzystaniem kopii zapasowych, obrazów dysków, kopii plików konfiguracyjnych i systemowych, rejestrów systemowych i aplikacji, plików dokumentów, identycznych ze sporządzonymi uprzednio kopiami przechowywanymi jako materiał dowodowy.

ł

6. TABELA ZMIAN

L.p.	Numer wydania dokumentu	Miejsce zmiany (nr punktu)	Opis zmiany	Nowy numer wydania dokumentu	Wprowadzający zmiany	
					Data	Imię i Nazwisko
	2		Zmiana polega na aktualizacji i weryfikacji aktualności tego dokumentu	2	27.01.2025 r.	

Załącznik nr 1

do Procedury zgłaszania naruszeń ochrony danych osobowych

Instrukcja zgłaszania zdarzeń związanych z naruszeniem ochrony danych osobowych

Każdy w przypadku zaistnienia podejrzenia lub stwierdzenia faktu zagrożenia bezpieczeństwa danych osobowych w obszarze infrastruktury teleinformatycznej, ma obowiązek zgłoszenia naruszenia bezpieczeństwa, używając do tego celu dostępnych mu w takim przypadku środków.

Pracownik / współpracownik oraz osoba za pomocą której NRA wykonuje swoje obowiązki zgłasza incydent:

1. Do Dyrektora Biura Naczelnej Rady Adwokackiej:
   a) za pośrednictwem e-mail: dyrektor@nra.pl
2. Do IOD:

a) Telefonicznie: +48 22 308 10 18

b) Za pośrednictwem e-mail: naruszenia@isecure.pl

Niezależnie od stosowanego kanału, w miarę możliwości należy przedstawić możliwie wyczerpujący opis zdarzenia:

1) termin(y) zdarzenia – data i godzina z podaniem dokładnego czasu,
2) jeśli występuje i jest znane - źródło(a) ataku – adres IP/nazwa urządzenia, z którego nastąpiło zagrożenie,
3) jeśli występuje i jest znany - cel(e) ataku – adres IP/nazwa urządzenia docelowego miejsca ataku, rodzaj narażonej usługi, atakowanego systemu itp.,
4) typ zdarzenia (np. spam, złośliwy kod, podszywanie się, wyłudzanie),
5) opis zdarzenia (obserwacje, spostrzeżenia, uwagi) – opis wykrycia oraz przebiegu incydentu, konsekwencje (rozmiar możliwych do oszacowania szkód), zasięg szkodliwych działań (liczba zaatakowanych systemów), inne źródła (urządzenia/sieci), termin rozpoczęcia, zakończenia i czas trwania ataku (np. czy zdarzenie ma dalej miejsce) itp.,
6) dowody zdarzenia (nagłówki pocztowe, kopia ekranu itp.) – jako załącznik.

Załącznik nr 2

do Procedury zgłaszania naruszeń ochrony danych osobowych

Ewidencja zdarzeń związanych z naruszeniem ochrony danych osobowych

Data zdarzenia	**Nazwa zdarzenia**	**Kategoria zdarzenia**	**Rodzaj komponentu, którego dotyczy zdarzenie**	**Nazwa systemu, którego dotyczy zdarzenie**	**Środki zaradcze**