Autor procedury: Agnieszka Witoszek, Administrator bezpieczeństwa informacji w Beskidzkiej Izbie Lekarskiej

Załącznik do uchwały nr 84/VIII/2018 Okręgowej Rady Lekarskiej Beskidzkiej Izby Lekarskiej z dnia 8 maja 2018 roku w sprawie przyjęcia i zatwierdzenia procedury zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu.

Procedura zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu.

Spis treści

§1 Postanowienia ogólne.

1. Niniejsza procedura ma na celu praktyczne uregulowanie sposobu zgłaszania naruszenia bezpieczeństwa danych osobowych w Beskidzkiej Izbie Lekarskiej organowi nadzorczemu.
2. Dokument wskazuje działania przewidziane do wykonania w przypadku naruszenia bezpieczeństwa danych osobowych w Izbie, określa kiedy konieczne jest dokonanie zgłoszenia, wskazuje podmiot odpowiedzialny za dokonanie zgłoszenia oraz sposób dokumentowania naruszeń.

§2 Podstawa prawna.

Przedmiotowa procedura została opracowana na podstawie art.33 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 rozporządzenia o ochronie danych), zwanym dalej RODO.

§3 Definicje.

1. Administrator danych osobowych (ADO) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, tj. Beskidzka Izba Lekarska, a w jej imieniu zadania w zakresie ochrony danych osobowych wykonuje Prezes Okręgowej Rady Lekarskiej pełniący obowiązki Administratora danych osobowych.
2. Inspektor ochrony danych osobowych (IOD, ang. DPO – Data Protection Officer) – osoba wyznaczona przez Administratora danych osobowych, która w sposób niezależny monitoruje właściwe przetwarzanie danych osobowych i pełni w tym zakresie funkcje doradcze i konsultacyjne dla Administratora danych osobowych.
3. Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować.
4. Przetwarzanie danych osobowych – operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
5. Interesariusz – osoba lub organizacja, która może wpływać na daną organizację (Izbę) lub/i pozostaje pod wpływem jej działalności.
6. Zasada rozliczalności – obowiązek wykazania/udowodnienia przez Administratora danych osobowych przetwarzania danych osobowych zgodnie z prawem oraz z zasadami przetwarzania danych osobowych, przy czym zasady te muszą być realizowane łącznie (m.in. zasada prawidłowości danych, poufności, integralności, dostępności).
7. Podmioty współpracujące z Izbą – osoby zatrudnione w Izbie w oparciu o umowy cywilnoprawne, wykonujące dla Izby usługi na mocy umów oraz inni Interesariusze.
8. Incydent naruszenia bezpieczeństwa danych osobowych i innych informacji – sytuacja naruszenia m.in. poufności, integralności, dostępności danych osobowych i innych informacji przetwarzanych tradycyjnie (w formie papierowej, ustnie) oraz w systemach informatycznych.

§4 Przesłanki zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu. Podmiot odpowiedzialny za dokonanie zgłoszenia.

1. Zgłoszenia należy dokonać zawsze, gdy naruszenie ochrony danych osobowych może powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jednocześnie naruszenie musi zostać umieszczone w rejestrze naruszeń bezpieczeństwa danych osobowych i innych informacji, którego wzór stanowi załącznik nr 1 do niniejszej procedury.
2. Za dokonanie zgłoszenia organowi nadzorczemu odpowiedzialny jest Administrator danych osobowych. ADO może wyznaczyć poprzez pisemnie upoważnienie osobę, która przygotuje treść zgłoszenia i wykona czynności techniczne niezbędne do dokonania zgłoszenia.
3. Administrator danych osobowych może zadecydować o niezgłoszeniu naruszenia ochrony danych osobowych organowi nadzorczemu, jeżeli jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Naruszenie musi być zawsze odnotowane w

rejestrze naruszeń, bez względu na decyzję Administratora danych osobowych co do zgłoszenia naruszenia do organu nadzorczego.

4. Rejestr naruszeń prowadzi Kierownik Biura Izby i umieszcza w nim zarówno incydenty dotyczące Biura Izby, jak i Organów Izby. Pracownicy Izby, podmioty współpracujące z Izbą oraz Organy Izby mają obowiązek pisemnie zgłaszać wszelkie przypadki naruszenia bezpieczeństwa danych osobowych i innych informacji Kierownikowi Biura Izby. Formularz zgłoszenia stanowi Załącznik nr 2 do niniejszej Procedury.
5. O każdym zgłoszonym naruszeniu Kierownik Biura Izby niezwłocznie informuje Inspektora ochrony danych oraz Administratora danych, który podejmuje decyzję o zgłoszeniu incydentu do organu nadzorczego.

§5 Naruszenie praw i wolności. Ryzyko.

1. Odniesienie do praw i wolności należy rozumieć możliwie szeroko. Dotyczy przede wszystkim prawa do prywatności a także między innymi:
   a) Wolności słowa,
   b) Prawo do dobrego imienia,
   c) Wolności myśli,
   d) Swobodę przemieszczania się,
   e) Zakaz dyskryminacji,
   f) Prawo do wolności sumienia i religii
   g) Szeroko pojętych praw pacjenta.
2. Katalog wymieniony w punkcie 1 ma charakter otwarty. Oceniając naruszenie należy uwzględniać wszelkie negatywne skutki, które mogą prowadzić do szkód fizycznych, materialnych i niematerialnych.
3. Każdy przypadek naruszenia ochrony danych osobowych musi uwzględniać prawa i wolności odpowiednio do rozpatrywanej sytuacji i towarzyszących jej okoliczności oraz osób zaangażowanych w sprawę.
4. Każdy przypadek naruszenia wymaga dokonania analizy ryzyka i określenia możliwie największej liczby skutków naruszenia i ich wpływu na prawa i wolności osoby fizycznej. Wyniki analizy ryzyka powinny zostać przekazane IOD i umieszczone w rejestrze naruszeń.
5. Administrator danych osobowych wyznacza przynajmniej 2 osoby, które z jego udziałem mają dokonać analizy ryzyka.
6. Metodologia analizy ryzyka może być dowolna, jednakże możliwie najlepsza dla danego przypadku naruszenia i zgodna z międzynarodowymi normami i standardami w zakresie analizy ryzyka oraz Procedurą zarządzania ryzykiem w Beskidzkiej Izbie Lekarskiej.

§6 Tryb zgłoszenia naruszenia organowi nadzorczemu.

1. Administrator danych osobowych dokonuje zgłoszenia naruszenia organowi nadzorczemu bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia przez Administratora danych osobowych. Jeżeli zgłoszenie przekazane zostaje po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Treść zgłoszenia reguluje art. 33 ust.3 i 4 Ogólnego Rozporządzenie o Ochronie Danych Osobowych. Poszczególne elementy zgłoszenia mogą być przekazywane przez ADO stopniowo, stosownie do posiadanej najlepszej wiedzy.
3. Zgłoszenie może być przekazane organowi nadzorczemu poprzez list pocztowy priorytetowy polecony, za pośrednictwem kuriera lub zabezpieczoną wiadomością e-mail albo inny sposób wskazany przez organ nadzorczy.

4. W przypadkach określonych w art. 34 ust.1 Ogólnego Rozporządzenie o Ochronie Danych Osobowych Administrator danych osobowych zawiadamia osoby, których dane dotyczą, o naruszeniu ochrony danych osobowych, chyba, że ADO może być zwolniony z tego obowiązku na podstawie art.34 ust.3.
5. Administrator danych osobowych, na podstawie zasady rozliczalności musi być w stanie wykazać organowi nadzorczemu przesłanki zwalniające go z obowiązku zawiadomienia osoby, której dane dotyczą.
6. Jeżeli ADO zawiadamia osobę fizyczną o naruszeniu, musi to uczynić w przejrzystej, zrozumiałej formie oraz opisać zalecenia dla danej osoby fizycznej, które pomogą zminimalizować potencjalne negatywne skutki naruszenia. W zawiadomieniu zawsze podaje się danej osobie dane kontaktowe Inspektora ochrony danych osobowych oraz dane Administratora danych osobowych i osoby faktycznie reprezentującej ADO.
7. Jeżeli naruszenie danych osobowych dotyczy danych osobowych powierzonych do przetwarzania przez inny podmiot, ADO niezwłocznie zawiadamia ten podmiot.

§7 Postanowienia końcowe.

Procedura wchodzi w życie od dnia 25 maja 2018 r.

Autor procedury: Agnieszka Witoszek, Administrator bezpieczeństwa informacji w Beskidzkiej Izbie Lekarskiej

Załącznik nr 1. Wzór Rejestru naruszeń bezpieczeństwa danych osobowych i innych informacji.

Osoba zgłaszająca naruszenie	Data, godzina i miejsce naruszenia	Opis okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze	Wyniki przeprowadzonej analizy ryzyka zdarzenia/wagi skutków	Zgłoszenie organowi nadzorczemu TAK/NIE

Załącznik nr 2. Formularz zgłoszenia naruszenia bezpieczeństwa danych osobowych i innych informacji.

Formularz zgłoszenia naruszenia bezpieczeństwa danych osobowych i innych informacji w Beskidzkiej Izbie Lekarskiej przetwarzanych tradycyjnie i w systemie informatycznym.

I. DANE ZGŁASZAJĄCEGO

Nazwisko i imię:

……

Stanowisko / funkcja

……

Komórka organizacyjna/Organ Izby

……

Podpis ……

II. DANE INCYDENTU

Data i czas incydentu

……

Opis incydentu

……

……

……

……

Autor procedury: Agnieszka Witoszek, Administrator bezpieczeństwa informacji w Beskidzkiej Izbie Lekarskiej

Podjęte przeciwdziałania

……

……

……

……

III. DANE LOAKLIZACJI

Budynek, kondygnacja, pomieszczenie

……

Nr DIN stacji roboczej

……

SEKRETARZ
OKRĘGOWEJ RADY LEKARSKIEJ

MACIEJ SKWARNA

PREZES
OKRĘGOWEJ RADY LEKARSKIEJ

KLAUDIUSZ KOMOR