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

Załącznik do uchwały nr 85/VIII/2018 Okręgowej Rady Lekarskiej Beskidzkiej Izby Lekarskiej z dnia 8 maja 2018 roku w sprawie przyjęcia i zatwierdzenia procedury oceny skutków dla ochrony danych osobowych (DPIA) dla Beskidzkiej Izby Lekarskiej w Bielsku-Białej.

# Procedura oceny skutków dla ochrony danych osobowych (DPIA)

# dla Beskidzkiej Izby Lekarskiej w Bielsku-Białej.

## Spis treści

## §1 Postanowienia ogólne.

Przedmiotowa procedura obejmuje całokształt zagadnień związanych z przeprowadzaniem oceny skutków dla ochrony danych osobowych. Wskazuje działania przewidziane do wykonania, osoby odpowiedzialne za dokonanie oceny oraz sposób jej prowadzenia, dokumentowania, a także zasady publikacji.

## §2 Podstawa prawna.

Procedura oceny skutków dla ochrony danych osobowych została opracowana na podstawie 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. Ocena skutków dla ochrony danych - (DPIA – Data Protection Impact Assesment) – nałożony przez RODO obowiązek analizy w jaki sposób operacja przetwarzania danych osobowych (planowana a także już prowadzona) wpływa lub będzie wpływać na prawa i wolności osób, których dane są przetwarzane w ramach danej operacji przetwarzania.
2. 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.
3. 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.
4. 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.
5. 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.
6. Interesariusz – osoba lub organizacja, która może wpływać na daną organizację (Izbę) lub/i pozostaje pod wpływem jej działalności.
7. Branżowy kodeks postępowania zatwierdzony przez organ nadzorczy – listy dobrych praktyk /referencji/zaleceń/praktycznych rozwiązań organizacyjnych opisujących jak w najlepszy sposób w danym sektorze/branży/środowisku biznesowo – organizacyjnym (np. w sektorze medycznym) wykonywać zadania związane z ochroną danych osobowych.

## §4 Przesłanki stosowania DPIA.

1. DPIA stosowana jest dla operacji przetwarzania danych osobowych, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.
2. Ocena skutków dla ochrony danych w praktyce przeprowadzana będzie dla wszelkich przedsięwzięć (np. projektów, zakupów urządzeń i nowych technologii) i procesów, podczas których przetwarzane są lub będą dane osobowe i z tym przetwarzaniem wiąże się ryzyko (obecnie lub w przyszłości) naruszenia praw i wolności osób fizycznych.
3. Operacje przetwarzania danych osobowych w Izbie mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, ponieważ:
   a) Przetwarzane są dane osobowe wrażliwe oraz o charakterze wysoce osobistym,
   b) Dane osobowe przetwarzane są na dużą skalę,
   c) Izba objęta jest systematycznym monitoringiem wizyjnym,
   d) Przetwarzane są dane o stanie zdrowia/dane osób wymagających szczególnej opieki – w przypadku przetwarzania dokumentacji medycznej na skutek śmierci lekarza/lekarza dentysty prowadzącego indywidualną praktykę lekarską/stomatologiczną lub przez Okręgowy Sąd Lekarski albo Okręgowego Rzecznika Odpowiedzialności Zawodowej.
4. Konieczność przeprowadzenia DPIA będzie rozpatrywana indywidualnie dla każdej operacji, a decyzja o braku konieczności przeprowadzenia oceny musi zostać uzasadniona pisemnie przez administratora danych osobowych.

## §5 Naruszenie praw i wolności.

1. Odniesienie do praw i wolności należy rozumieć możliwie szeroko. Dotyczy przede wszystkim prawa do prywatności a także między innymi:
   a) Wolności słowa,
   b) Wolności myśli,
   c) Swobodę przemieszczania się,
   d) Zakaz dyskryminacji,
   e) Prawo do wolności sumienia i religii
   f) Szeroko pojętych praw pacjenta – w przypadku przetwarzania dokumentacji medycznej.
2. Powyższy katalog ma charakter otwarty. Każda ocena wpływu na ochronę danych osobowych musi uwzględniać prawa i wolności odpowiednio do rozpatrywanej operacji przetwarzania danych osobowych i musi uwzględniać wszelkie negatywne skutki, które mogą prowadzić do szkód fizycznych, materialnych i niematerialnych.

## §6 Odpowiedzialność za DPIA.

1. Za przeprowadzanie oceny skutków dla ochrony danych i inicjatywę w tym zakresie odpowiedzialność ponosi Administrator danych osobowych. Może on skorzystać z pomocy Administratora bezpieczeństwa informacji oraz innych wyznaczonych osób, jednak odpowiedzialność za brak lub niewłaściwe przeprowadzenie DPIA ponosi ADO.
2. Administrator danych przeprowadzając DPIA ma obowiązek konsultowania się z IOD.
3. Z zaleceniem przeprowadzenia DPIA do ADO może wystąpić Inspektor ochrony danych. Ostateczna decyzja co do konieczności przeprowadzenia DPIA spoczywa na ADO.
4. ADO może również zasięgnąć opinii w kwestii oceny skutków dla ochrony danych wśród osób, których dane osobowe są przetwarzane (np. poprzez badanie ankietowe).
5. ADO może czerpać wiedzę dotyczącą operacji przetwarzania danych osobowych, dla których zalecane jest przeprowadzenie DPIA z branżowych kodeksów postępowania zatwierdzonych przez organ nadzorczy.

## §7 Przeprowadzanie DPIA.

1. Ocenę skutków dla ochrony danych przeprowadza się zanim rozpoczęte zostanie przetwarzanie danych osobowych w ramach analizowanej operacji przetwarzania. Ocenę można też przeprowadzić dla operacji już trwających, rozpoczętych przed 25 maja 2018.
2. DPIA nie jest jednorazowym przedsięwzięciem, ale procesem. Ze względu na zmianę jakichkolwiek okoliczności przetwarzania danych może się okazać konieczne powtórzenie DPIA. Ocenę należy również przeprowadzać cyklicznie jako formę monitoringu nad prawidłowym przetwarzaniem danych osobowych.
3. DPIA może być powtarzane na każdym etapie operacji przetwarzania danych – na każdym etapie projektu, procesu, usługi itp.

## §8 Konsultacje i dokumentowanie DPIA.

1. Przeprowadzenie oceny wpływu na ochronę danych osobowych musi być dokumentowane przez Administratora danych osobowych na każdym etapie jej prowadzenia i obejmuje m.in. następujące informacje:
   a) Określenie kto wystąpił z inicjatywą przeprowadzenia DPO,
   b) Terminy DPIA – planowaną datę rozpoczęcia, zakończenia i terminy prowadzenia konsultacji,
   c) Elementy DPIA wymienione w §9,
   d) Podpisane przez autorów i przekazane ADO wszelkie konsultacje, opinie i oceny, które zostały pozyskane podczas prowadzenia DPIA,
   e) Jeżeli nie zasięgnięto opinii u osób, których dane dotyczą – uzasadnienie braku konsultacji.
   f) Datę faktycznego zakończenia DPIA oraz podpis Administratora danych osobowych,
2. Interesariusze, konsultanci oraz osoby, których dane dotyczą powinni otrzymać odpowiednią ilość czasu, aby zapoznać się z rodzajem planowanej operacji przetwarzania danych, jednak ADO czuwa nad tym, aby postępowanie nie było przewlekające się w czasie.
3. Termin przebiegu konsultacji i czasu na przekazanie opinii powinien być nie krótszy niż 14 dni liczonych od dnia przekazania przez ADO opisu operacji przetwarzania danych osobowych. Odbiór powinien zostać potwierdzony pisemnie.

## §9 Elementy DPIA.

1. Ocena wpływu na ochronę danych osobowych zawiera co najmniej następujące elementy:
   a) Systematyczny opis planowanej operacji przetwarzania danych osobowych
   b) Ocenę niezbędności i proporcjonalności przetwarzania danych w stosunku do celów przetwarzania,
   c) Analizę i ocenę ryzyka w odniesieniu do potencjalnego naruszenia praw i wolności osób fizycznych wraz ze środkami minimalizującymi to ryzyko oraz uzasadnieniem dokonanego wyboru środków,
   d) Określenie interesariuszy zaangażowanych w DPIA,
   e) Wyniki konsultacji z Inspektorem ochrony danych,
   f) Opinie osób, których dane dotyczą lub ich przedstawicieli, gdy ich zasięgnięto,
   g) Informacje o uwzględnieniu przestrzegania zatwierdzonych kodeksów postępowania.
2. Szczegółowy opis części elementów DPIA znajduje się w załączniku numer 1 do niniejszej procedury.
3. Jeżeli przeprowadzona w ramach DPIA analiza ryzyka wskazuje na wysokie ryzyko szczątkowe, Administrator danych ma obowiązek zwrócić się pisemnie o uprzednie konsultacje w celu przetwarzania do organu nadzorczego.

4. Administrator danych zwraca się do organu nadzorczego niezwłocznie, jednak nie później niż 14 dni od zakończenia oceny skutków operacji dla ochrony danych osobowych. ADO dostarcza organowi nadzorczemu dokumentację DPIA.

## §10 Publikacja DPIA.

1. Wyniki DPIA powinny zostać opublikowane na stronie internetowej Izby, jeżeli operacja przetwarzania ma duży wpływ na liczną grupę społeczeństwa (np. pracowników, lekarzy, których dane są przetwarzane lub pacjentów, których dokumentacja przetwarzana jest na terenie Izby).
2. DPIA może być publikowane w części lub zawierać tylko część oceny z jej zasadniczą treścią albo publikowane jest podsumowanie z najważniejszymi ustaleniami DPIA.
3. Publikacji w ramach DPIA nie podlegają informacje dotyczące zagrożeń dla bezpieczeństwa Administratora danych, stosowane środki zabezpieczeń, tajemnice przedsiębiorstwa lub inne informacje poufne przetwarzane w Beskidzkiej Izbie Lekarskiej.

## §11 Postanowienia końcowe.

Procedura wchodzi w życie od dnia 25 maja 2018 r.

Załącznik nr 1 do Procedury oceny skutków dla ochrony danych.

1. Systematyczny opis operacji przetwarzania zawiera co najmniej:
   a) Określenie charakteru, zakresu, kontekstu i celu (celów) przetwarzania;
   b) Opis kategorii osób, których dane będą przetwarzane, określenie kategorii danych osobowych, informacje o odbiorcach danych i okresie przechowywania danych osobowych;
   c) przedstawienie funkcjonalnego opisu operacji przetwarzania – z uwzględnieniem obiegu, przepływu danych osobowych, cyklu życia danych oraz kwestii powierzenia danych osobowych;
   d) zidentyfikowanie zasobów, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań).

2. Ocena niezbędności oraz proporcjonalności w stosunku do celów przetwarzania wskazuje środki, których podjęcie jest planowane w celu zapewnienia przestrzegania RODO i zawiera co najmniej:

a) opis środków przyczyniających się do proporcjonalności i niezbędności przetwarzania, ze szczególnym uwzględnieniem wykazania przez Administratora danych osobowych następujących kwestii:

   - konkretne, wyraźne i prawnie uzasadnione cele;

   - zgodność przetwarzania z prawem;

   - dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

   - ograniczony czas przechowywania;

b) wykazanie przez ADO środków przyczyniających się do zachowania praw osób, których dane dotyczą:

   - poinformowanie osoby, której dane dotyczą;

   - prawo dostępu i prawo do przenoszenia danych;

   - prawo do sprostowania i do usunięcia danych;

   - prawo do sprzeciwu i prawo do ograniczenia przetwarzania;

   - relacje z podmiotem przetwarzającym;

   - zabezpieczenia przy międzynarodowym przekazywaniu danych.

3. Analiza i ocena ryzyka w odniesieniu do potencjalnego naruszenia praw i wolności osób fizycznych wraz ze środkami minimalizującymi to ryzyko oraz uzasadnieniem dokonanego wyboru środków, ze szczególnym uwzględnieniem:

a) źródła, charakteru, specyfiki i wagi każdego rodzaju ryzyka (np. bezprawnego dostępu, niepożądanej zmiany i zniknięcia danych), ze szczególnym uwzględnieniem punktu widzenia osób, których dane dotyczą;

b) identyfikacji możliwych skutków dla praw i wolności osób, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych;
c) identyfikacji zagrożeń, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych;
d) oszacowano prawdopodobieństwo i wagę ryzyka;
e) określenia środków, których podjęcie jest planowane w celu zaradzenia ryzyku wraz z uzasadnieniem wyboru tych środków;
f) metody analizy ryzyka za pomocą macierzy oraz innych metod odpowiednich dla danej oceny (np. według Normy ISO 31000 i 31010 lub standardu FERMA).