Załącznik nr 1 do uchwały nr 155/VIII/2018 Okręgowej Rady Lekarskiej Beskidzkiej Izby Lekarskiej z dnia 3 lipca 2018 roku w sprawie zmiany uchwały nr 118/VII/2017 Okręgowej Rady Lekarskiej Beskidzkiej Izby Lekarskiej z dnia 24 lutego 2017 roku w sprawie polityki bezpieczeństwa Beskidzkiej Izby Lekarskiej.

POLITYKA BEZPIECZEŃSTWA

Beskidzka Izba Lekarska
ul. Krasińskiego 28
43-300 Bielsko-Biała

Spis treści

§1 Postanowienia ogólne. 3
§2 Definicje i skróty....3
§3 Obszary przetwarzania danych osobowych. 4
§4 Zbiory danych osobowych oraz ich struktura. 5
§5 Rejestr czynności przetwarzania. 5
§6 Środki techniczne i organizacyjne służące ochronie danych osobowych. 6
§7 Nadawanie, zmiana i odbieranie uprawnień do przetwarzania danych osobowych. 7
§8 Zakres zadań IOD. 7
§9 Zakres odpowiedzialności Administratora Systemu Informatycznego. 8
§10 Zakres odpowiedzialności Opiekunów. 10
§12 Zarządzanie ryzykiem w BIL. 11
§13 Ocena skutków dla ochrony danych osobowych. 11
§14 Zasady postępowania w przypadku naruszenia bezpieczeństwa systemu ochrony danych. 11
§15 Kontrole wewnętrzne i audyty bezpieczeństwa. 12
§11 Odpowiedzialność karna. 13
§12 Postanowienia końcowe. 13
SPIS ZAŁĄCZNIKÓW 13
Z-01 Karta obszaru przetwarzania danych osobowych. 13
Z-02 Karta zbioru danych osobowych. 13
Z-03 Zasady ochrony danych osobowych. 13
Z-04 Upoważnienie do przetwarzania danych osobowych. 13
Z-05 Ewidencja osób upoważnionych do przetwarzania danych osobowych. 13
Z-06 Oświadczenie Użytkownika 13
Z-07 Procedura nadawania, zmiany, odebrania uprawnień do przetwarzania danych osobowych 13
Z-08 Instrukcja postępowania w przypadku naruszenia bezpieczeństwa danych osobowych. 13
Z-09 Wzór rejestru czynności przetwarzania. 13
Z-10 Zgłoszenie naruszenia bezpieczeństwa danych osobowych przetwarzanych w formie tradycyjnej i/lub w systemie informatycznym 13
Z-11 Wzór raportu pokontrolnego IOD. 13
KARTA OBSZARU PRZETWARZANIA DANYCH OSOBOWYCH 14
KARTA ZBIORU DANYCH OSOBOWYCH 15
ZASADY OCHRONY DANYCH OSOBOWYCH 16
UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH 21
EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH 22
OŚWIADCZENIE UŻYTKOWNIKA 23

PROCEDURA NADAWANIA, ZMIANY, ODEBRANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH 25

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH .. 26

WZÓR REJESTRU CZYNNOŚCI PRZETWATWARZANIA 29

ZGŁOSZENIE NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH PRZETWARZANYCH W FORMIE TRADYCYJNEJ I/LUB W SYSTEMIE INFORMATYCZNYM 30

WZÓR RAPORTU POKONTROLNEGO IOD. 32

§1 Postanowienia ogólne.

1. Niniejszy dokument określa zakres i sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
2. Polityka ma zastosowanie do zbiorów danych osobowych przetwarzanych w Beskidzkiej Izbie Lekarskiej (dalej zwaną również Izbą lub BIL), w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.
3. Dokument został opracowany na podstawie:
   a. 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),
   b. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000),
   c. Ustawy z dnia 2 grudnia 2009 r. o izbach lekarskich (tj. Dz.U. 2018 poz. 168).
4. Szczegółowe omówienie środków zabezpieczenia technicznego i organizacyjnego systemu informatycznego znajduje się w Instrukcji.
5. Dane osobowe w Beskidzkiej Izbie Lekarskiej są chronione zgodnie z polskim prawem oraz europejskimi standardami wyznaczanymi aktami prawa Wspólnotowego, a administrator danych osobowych deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.

§2 Definicje i skróty.

1. **Polityka** - Polityka Bezpieczeństwa w Beskidzkiej Izbie Lekarskiej.
2. **Izba/BIL** – Beskidzka Izba Lekarska.
3. **Dokument –** Polityka Bezpieczeństwa.
4. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
5. **System informatyczny** - sprzęt i programy komputerowe którego funkcją jest przetwarzanie danych osobowych.
6. **Bezpieczeństwo systemu informatycznego** - wdrożenie przez Administratora lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem Ustawy, nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
7. **Administrator Danych Osobowych (ADO) –** Beskidzka Izba Lekarska reprezentowana przez Prezesa Okręgowej Rady Lekarskiej**,** zwany dalej ADO.
8. **Inspektor ochrony danych (IOD)** - osoba wyznaczona przez Administratora, odpowiedzialna za nadzorowanie bezpieczeństwa danych osobowych w Izbie, zwany dalej IOD.

9. **Administrator Systemów Informatycznych (ASI)** - osoba wyznaczona przez Administratora odpowiedzialna za wdrażanie technicznych zabezpieczeń systemów informatycznych, ich sprawność i konserwację oraz ochronę w przetwarzanych zbiorach danych osobowych, zwany dalej ASI.

10. **Użytkownik** - osoba posiadająca upoważnienie wydane przez Administratora lub wyznaczoną przez niego osobę uprawnioną, dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu.

11. **Przełożony** - osoba pełniąca funkcję kierownika komórki organizacyjnej, będąca przełożonym użytkownika.

12. **Opiekun** - kierownik komórki organizacyjnej lub inna wyznaczona przez ADO osoba odpowiedzialna za dany zasób danych osobowych, zgodnie z zakresem pełnionych obowiązków.

13. **Osoba uprawniona** - osoba posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności.

14. **Ustawa –** Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000).

15. **Rozporządzenie** - 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),

16. **Zasady** - Zasady ochrony danych osobowych – szczegółowe wytyczne w zakresie ochrony danych osobowych stanowiące załącznik do Polityki.

17. **Instrukcja** - Instrukcja zarządzania systemem informatycznym.

18. **Oświadczenie** – Druk Oświadczenie użytkownika, stanowiący załącznik do Polityki.

§3 Obszary przetwarzania danych osobowych.

1. Obszar przetwarzania danych osobowych w Izbie obejmuje budynki, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe, tzn. miejsca w których wykonuje się operacje na danych osobowych, jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji, a także pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych).

2. Obszary przetwarzania danych osobowych określone zostały w wykazie obszarów przetwarzania danych osobowych. Wykaz obszarów składa się z Kart obszaru przetwarzania danych osobowych. Wzór Karty stanowi załącznik nr 1 do Polityki.

3. Wykaz ten może być prowadzony w wersji elektronicznej i musi zawierać następujące informacje:

    a) adres budynku,

    b) zabezpieczenia budynku,

    c) piętro,

d) numer pomieszczenia,

e) rodzaj pomieszczenia,

f) komórka organizacyjna użytkująca pomieszczenie,

g) miejsce i sposób przetwarzania danych osobowych (tradycyjnie, elektronicznie).

§4 Zbiory danych osobowych oraz ich struktura.

1. Wykaz zbiorów danych osobowych stanowią „Karty zbiorów danych osobowych" – wzór karty stanowi załącznik nr 2 do Polityki.
2. Wykaz ten może być prowadzony w wersji elektronicznej i musi zawierać następujące informacje:
   a) nazwę zbioru,
   b) miejsce przechowywania/składowania – nazwa komórki organizacyjnej,
   c) piętro, nr pomieszczenia,
   d) stanowisko osoby odpowiedzialnej za zbiór danych,
   e) zakres gromadzonych danych,
   f) oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 28 Rozporządzenia, i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi.
3. Jeżeli zbiór danych przetwarzany jest w systemie informatycznym musi zawierać, oprócz wymienionych powyżej, również następujące informacje:
   g) nazwę programu przetwarzającego dane,
   h) oznaczenie producenta,
   i) lokalizację bazy danych,
   j) informację o wersji: jednostanowiskowej lub sieciowej,
   k) miejsca eksportowania danych (innych systemów informatycznych),
4. Szczegółowe informacje dotyczące platformy sprzętowej oraz oprogramowania danego systemu informatycznego znajdują się w poszczególnych instrukcjach zarządzania danym systemem.
5. Struktura określonego zbioru danych osobowych opisana jest w Karcie zbioru (Zał. nr 2) wraz z zakresem gromadzonych danych.

§5 Rejestr czynności przetwarzania.

1. Dla zbiorów, w których przetwarzane są dane, o których mowa w art. 9 ust. 1 RODO prowadzony jest rejestr czynności przetwarzania.
2. Rejestr, o którym mowa w punkcie 1 niniejszego rozdziału może być również prowadzony dla innych zbiorów lub jedna czynność przetwarzania może obejmować kilka zbiorów danych osobowych.

3. Rejestr czynności przetwarzania winien zawierać co najmniej informacje, o których mowa w art. 30 RODO tj.:

    a. Imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,

    b. cele przetwarzania;

    c. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

    d. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

    e. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;

    f. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

    g. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

4. Rejestr czynności przetwarzania jest prowadzony w oparciu o załącznik nr 9 do Polityki.

§6 Środki techniczne i organizacyjne służące ochronie danych osobowych.

1. W Beskidzkiej Izbie Lekarskiej stosuje się następujące środki techniczne i organizacyjne służące ochronie danych osobowych:
    a) Inspektor ochrony danych prowadzi Dokumentację Ochrony Danych Osobowych opisującą sposób przetwarzania danych osobowych w Izbie.
    b) Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie do przetwarzania danych osobowych (załącznik nr 4 do Polityki). Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych (wzór ewidencji stanowi załącznik nr 5 do Polityki).
    c) W celu skutecznej ochrony danych osobowych powołani są Inspektor ochrony danych oraz Administrator Systemu Informatycznego.
    d) Przypisane zostają zakresy odpowiedzialności za sposób przetwarzania danych osobowych zarówno osobom nadzorującym przetwarzanie danych osobowych, jak i użytkownikom.
    e) Każdy pracownik Izby co najmniej raz do roku musi odbyć szkolenie z zakresu ochrony danych osobowych. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.

2. Wprowadza się Zasady Ochrony Danych Osobowych (załącznik nr 3 do Polityki), regulujące:

    a) Udostępnianie danych osobowych,

    b) Powierzanie danych osobowych,

    c) Ochronę pomieszczeń i organizację pracy przy przetwarzaniu danych,

d) Warunki przetwarzanie danych osobowych poza obszarem przetwarzania oraz danych znajdujących się na nośnikach papierowych,

e) Monitorowanie ochrony zasobów danych osobowych,

f) Techniczne oraz organizacyjne środki ochrony obszarów stanowiących szczególne strefy ochrony- archiwum oraz serwerowni.

§7 Nadawanie, zmiana i odbieranie uprawnień do przetwarzania danych osobowych.

1. Uprawnienia do przetwarzania danych osobowych w Beskidzkiej Izbie Lekarskiej nadaje Prezes Okręgowej Rady Lekarskiej, natomiast Kierownik Biura BIL przygotowuje stosowną dokumentację.
2. Zakres upoważnienia wynika z przypisanych danemu pracownikowi obowiązków służbowych.
3. Pracownik, któremu nadano uprawnienia składa pisemne Oświadczenie (załącznik nr 6 do Polityki) w którym potwierdza fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa oraz zobowiązuje się do zachowania poufności.
4. Kierownik Biura BIL odpowiedzialny jest za gromadzenie i przechowywanie wszystkich Wniosków, Oświadczeń oraz Upoważnień wydawanych Użytkownikom.
5. W celu nadania uprawnień do przetwarzania danych osobowych ma zastosowanie Procedura nadania, zmiany, odebrania uprawnień do przetwarzania danych osobowych – załącznik nr 7 do Polityki.
6. Osobą odpowiedzialną za rejestrację osoby upoważnionej do przetwarzania danych osobowych w ewidencji osób upoważnionych jest Kierownik Biura BIL, natomiast za rejestrację uprawnień użytkownika w systemach informatycznych osobą odpowiedzialną jest ASI.
7. Ustanie stosunku pracy jest równoważne z cofnięciem uprawnień do przetwarzania danych osobowych.
8. Użytkownicy dopuszczeni do przetwarzania danych osobowych zobowiązani są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.
9. W celu nadania uprawnień w systemie informatycznym ma zastosowanie Procedura nadawania, zmiany, odebrania uprawnień użytkownikowi do systemu– załącznik nr 1 do Instrukcji.
10. IOD nadzoruje procedury nadawania uprawnień do przetwarzania danych osobowych.

§8 Zakres zadań IOD.

1. Do zadań Inspektora ochrony danych należy nadzorowanie przestrzegania w Izbie przepisów o ochronie danych osobowych, w szczególności przez:

   a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie informacji dla Administratora danych,

b) opracowywanie i aktualizowanie dokumentacji ochrony danych osobowych oraz nadzorowanie przestrzegania określonych w niej zasad,

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

2. IOD prowadzi rejestr zbiorów danych osobowych przetwarzanych przez Administratora oraz Rejestr czynności przetwarzania.

3. IOD wykonując obowiązki wymienione w pkt. 1, identyfikuje i uwzględnia ryzyka występujące w Izbie i podejmuje proporcjonalne do nich działania.

4. Do szczegółowych obowiązków IOD należy:

a) kontrolowania procesów udostępniania danych osobowych,

b) podział obowiązków w zakresie ochrony danych osobowych oraz wydawanie wiążących zaleceń dla kierowników komórek organizacyjnych w zakresie standardów zabezpieczeń danych osobowych,

c) współpraca z ASI w zakresie bezpieczeństwa systemów informatycznych,

d) podejmowania działań zgodnych z obowiązującymi w Izbie procedurami w sytuacji naruszenia ochrony danych osobowych.

5. ADO zapewnia, aby IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych w Izbie.

6. IOD podlega bezpośrednio Prezesowi Okręgowej Rady Lekarskiej i nie otrzymuje instrukcji dotyczących wykonywania zadań w zakresie ochrony danych osobowych.

7. IOD zobowiązany jest do zachowania poufności co do wykonywanych przez siebie zadań.

§9 Zakres odpowiedzialności Administratora Systemu Informatycznego.

1. ASI, w imieniu Administratora danych osobowych wykonuje zadania w zakresie bezpieczeństwa systemu informatycznego.

2. Do obowiązków ASI w zakresie ochrony danych osobowych należy:

a) Zapewnienie możliwie najwyższego poziomu bezawaryjnego funkcjonowania systemu informatycznego.

b) Prowadzenia nadzoru nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe.

c) Prowadzenie w Izbie nadzoru nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych oraz podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych.

d) Powiadamianie IOD o naruszeniu lub podejrzeniu naruszenia zabezpieczeń informatycznych.

e) Prowadzenie nadzoru nad przesyłaniem danych osobowych drogą teletransmisji.

f) Analiza ryzyka w kontekście bezpieczeństwa danych osobowych w systemie informatycznym.

g) Kooperacja z IOD w zakresie czuwania nad treścią Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Izbie.

h) Tworzenie i aktualizacja kart zbiorów danych osobowych dla poszczególnych systemów informatycznych.

i) Nadzór nad procedurami dotyczącymi bezpieczeństwa systemu informatycznego w Izbie.

3. ASI prowadzi rejestru użytkowników systemu informatycznego. Rejestr ten może być prowadzony elektronicznie i musi zawierać co najmniej następujące informacje:

   a) dane Użytkownika (nazwisko i imię, stanowisko, identyfikator, komórkę organizacyjną),

   b) dane nadanych uprawnień (datę nadania, system i uprawnienia, okres obowiązywania),

   c) weryfikację IOD (nazwisko i imię, datę weryfikacji, decyzję zgody lub odmowy oraz uzasadnienie), jeżeli nadawane uprawnienia wykraczają poza przypisane do danego stanowiska służbowego lub pełnionych obowiązków,

   d) dane osoby nadającej uprawnienia (nazwisko i imię, datę realizacji, uwagi do realizacji).

4. ASI przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe poprzez:

   a) podejmowanie odpowiednich działań w przypadku naruszeń w systemie zabezpieczeń,

   b) ustalanie, po konsultacji z IOD, poziomu dostępu do systemów informatycznych przez poszczególnych Użytkowników,

   c) właściwy nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,

   d) podejmowanie działań zgodnie przepisami w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,

   e) nadzór nad wykonywaniem kopii awaryjnych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu,

   f) nadzór na zabezpieczeniem antywirusowym systemu informatycznego opisanym w Procedurze zabezpieczenia antywirusowego systemu informatycznego (dokument stanowiący załącznik do Instrukcji).

§10 Zakres odpowiedzialności Opiekunów.

1. Administrator danych osobowych lub IOD na podstawie specjalnego upoważnienia wydanego przez ADO, wyznacza Opiekunów poszczególnych zasobów danych osobowych.

2. Rolę Opiekunów zasobów danych osobowych pełnią kierownicy komórek organizacyjnych odpowiedzialni za dany zasób danych osobowych wynikający z zakresu pełnionych obowiązków lub inne osoby wskazane przez ADO lub ABI.

3. Zakres odpowiedzialności Opiekuna powinien zostać ujęty w zakresie obowiązków służbowych lub stosownej umowie cywilnoprawnej. Zakres obowiązków (w umowie o pracę lub umowie cywilnoprawnej) przygotowuje pracownik odpowiedzialny za kwestie kadrowe i przedstawia IOD do konsultacji.

4. Do obowiązków Opiekunów zasobów danych osobowych należy:

    a) zarządzanie zasobem danych osobowych w ramach zadań realizowanych przez te komórki organizacyjne,

    b) występowanie z wnioskiem (stanowiącym załącznik do Instrukcji) do ASI o nadanie, zmianę, odebranie uprawnień do systemów informatycznych podległym pracownikom,

    c) zgłaszanie do IOD zamiaru utworzenia zbioru danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania zbiorów danych,

    d) prowadzenie w podległej komórce organizacyjnej nadzoru nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe, w tym generowanych przez system informatyczny,

    e) przestrzeganie postanowień Zasad ochrony danych osobowych,

    f) zapoznawanie pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych,

    g) dokonywanie na polecenie IOD analizy ryzyka dotyczącego bezpieczeństwa danych osobowych w podległej komórce organizacyjnej.

5. Opiekun realizuje proces udostępniania danych osobowych innemu podmiotowi lub osobie, której dane dotyczą oraz prowadzi z tego tytułu odpowiednią ewidencję zawierającą co najmniej:

a) datę udostępnienia,

b) zakresu udostępnianych danych osobowych,

c) cel udostępnienia,

d) komu dane udostępniono,

e) dane osoby udostępniającej.

6. Ewidencję o której mowa w pkt. 5, Opiekun udostępnia IOD w określonej przez niego formie.

§12 Zarządzanie ryzykiem w BIL.

1. W Izbie przeprowadzana jest analiza ryzyka. Analiza ryzyka odbywa się dla wszystkich wyodrębnionych czynności przetwarzania.
2. Analiza ryzyka przeprowadzana jest w celu określenia, oceny i minimalizacji zagrożeń, których efektem ma być wdrożenie optymalnych i adekwatnych zabezpieczeń.
3. Analiza ryzyka przeprowadzona jest corocznie dla wszystkich czynności przetwarzania lub w przypadku wprowadzenia nowych procedur lub rozwiązań organizacyjnych w podmiocie leczniczym, zgodnie z odrębną procedurą przyjętą przez Izbę.

§13 Ocena skutków dla ochrony danych osobowych.

1. Dla danych osobowych, których nieuprawnione ujawnienie wiąże się z wysokim ryzykiem uszczerbku dla osób, których dane dotyczą przeprowadzana jest ocena skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO.
2. Ocena skutków dla ochrony danych osobowych polega na:
    a. opisie planowanych operacji i celów przetwarzania,
    b. opisie i ocenie przez administratora czy planowane operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów,
    c. ocenie ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
    d. opisie środków planowanych w celu zaradzenia ryzykiem, w tym określeniu mechanizmów, zabezpieczeń i środków technicznych, mających zapewnić bezpieczeństwo procesu,
3. Ocena skutków dla ochrony danych odbywa się odrębną procedurą przyjętą przez BIL.
4. Za zarządzanie ryzykiem oraz ocenę skutków dla ochrony danych osobowych odpowiada Administrator danych osobowych.
5. Analiza ryzyka i ocena skutków dla systemu ochrony danych może odbywać się przy udziale Inspektora Ochrony Danych Osobowych.
6. Wyznaczony pracownik ma obowiązek sporządzenia corocznego raportu związanego z ryzykiem w Izbie.

§14 Zasady postępowania w przypadku naruszenia bezpieczeństwa systemu ochrony danych.

1. Każda osoba, której Administrator wydał upoważnienie do przetwarzania danych osobowych, ma obowiązek natychmiastowego powiadamiania o występującym zagrożeniu lub wystąpieniu incydentu związanego z systemem ochrony danych osobowych w Izbie.
2. Szczegółowy sposób postępowania w przypadku naruszenia bezpieczeństwa systemu ochrony danych określa załącznik nr 8 do Polityki.
3. Powiadomienie ma charakter pisemny. Wzór zgłoszenia stanowi załącznik nr 10 do Polityki.
4. Adresatem takiego powiadomienia jest Inspektor Ochrony Danych Osobowych, a w przypadku, gdy incydent dotyczy systemu informatycznego także ASI.
5. Po otrzymaniu takiego powiadomienia Inspektor Ochrony Danych Osobowych podejmuje niezwłocznie czynności w celu ustalenia stanu faktycznego.

6. W przypadku uzasadnionego podejrzenia wystąpienia incydentu lub naruszenia systemu ochrony danych osobowych podejmuje działania mające zapobiec dalszym skutkom oraz powiadamia Administratora.

7. Po dokonaniu czynności zabezpieczających, Inspektor Ochrony Danych Osobowych, ma za zadanie przeprowadzić postępowanie wyjaśniające, które:

    a. ustali ostateczny zakres, przyczyny wystąpienia oraz skutki, zarówno dla Izby, jak i osób, których dane dotyczyły,

    b. podejmuje niezbędne czynności mające na celu przywrócenie prawidłowości działania systemu ochrony danych osobowych w BIL,

    c. opracowuje działania naprawcze i zapobiegawcze, których zadaniem jest wyeliminowanie niepożądanych zdarzeń w przyszłości,

    d. wskazuje osoby odpowiedzialne za wystąpienie sytuacji.

8. Powyższe czynności są dokumentowane przez Inspektora Ochrony Danych Osobowych za pomocą formularza, którego wzór stanowi załącznik nr 11 do Polityki.

9. Rejestr formularzy, o których mowa w punkcie 7 niniejszego rozdziału prowadzi Administrator.

10. Inspektor Ochrony Danych Osobowych, na ile jest to możliwe, ma obowiązek przedstawienia raportu Administratorowi w czasie umożliwiającym Administratorowi powiadomienie o incydencie lub naruszeniu systemu ochrony danych osobowych organu nadzorczego nie później niż na 72 godziny od czasu jego wykrycia, zgodnie z odrębną procedurą obowiązującą w Izbie.

§15 Kontrole wewnętrzne i audyty bezpieczeństwa.

1. Kontrolą przetwarzania danych osobowych zajmuje się Inspektor Ochrony Danych Osobowych.
2. Kontrole przeprowadzane są regularnie, co najmniej raz do roku, a w przypadku wystąpienia incydentu w podmiocie, kompleksową kontrolę obejmującą wszystkie aspekty działalności rozpoczyna się nie później niż 7 dni po zakończeniu działań związanych z incydentem, który wystąpił.
3. Kontrola przeprowadzana jest przy uwzględnieniu minimalnych wytycznych jakimi są: badanie pod względem zgodności z prawem, branżowymi standardami postepowania, normami i przepisami wewnętrznymi.
4. Inspektor Ochrony Danych Osobowych może wykonywać kontrole osobiście, może, przy pisemnej zgodzie Administratora wyznaczyć do tego inną osobę lub podmiot.
5. Kontrole przeprowadzane są na podstawie programów kontroli, w których opisywany jest ich zakres, termin, cele oraz metody ich przeprowadzania oraz doraźnie.
6. Proces kontroli musi być dokumentowany i uzupełniony pozyskaniem obiektywnych dowodów na prawidłowość procesu kontrolnego.
7. Jeśli podczas kontroli stwierdzone zostają nieprawidłowości zagrażające systemowi ochrony danych osobowych w podmiocie, kontroler musi niezwłocznie powiadomić o tym fakcie administratora.
8. Wynik kontroli musi być udokumentowany i przekazany administratorowi w ciągu 21 dni od jej zakończenia.
9. Wzór raportu pokontrolnego określa załącznik nr 11 do Polityki.

§11 Odpowiedzialność karna.

1. Niewłaściwe przetwarzanie danych osobowych jest zagrożone sankcjami karnymi określonymi w art. 107 i 108 Ustawy.
2. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 1, naruszenie zasad ochrony danych osobowych obowiązujących w Izbie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.
3. Osoby, których dane dotyczą, mogą się ponadto ubiegać o ochronę ich interesów na mocy przepisów Kodeksu Cywilnego.

§12 Postanowienia końcowe.

1. Wdrożenie postanowień Polityki ma na celu wprowadzenie jednolitego systemu zarządzania danymi osobowymi w Izbie.
2. W sprawach nieuregulowanych Polityką znajdują zastosowanie przepisy Rozporządzenia, Ustawy oraz aktów wykonawczych.
3. Wszelkie zmiany w Polityce mogą być wprowadzone tylko na podstawie uchwały Okręgowej Rady Lekarskiej lub działającego z jej upoważnienia Prezydium Okręgowej Rady Lekarskiej.

SPIS ZAŁĄCZNIKÓW

Z-01 Karta obszaru przetwarzania danych osobowych.

Z-02 Karta zbioru danych osobowych.

Z-03 Zasady ochrony danych osobowych.

Z-04 Upoważnienie do przetwarzania danych osobowych.

Z-05 Ewidencja osób upoważnionych do przetwarzania danych osobowych.

Z-06 Oświadczenie Użytkownika.

Z-07 Procedura nadawania, zmiany, odebrania uprawnień do przetwarzania danych osobowych.

Z-08 Instrukcja postępowania w przypadku naruszenia bezpieczeństwa danych osobowych.

Z-09 Wzór rejestru czynności przetwarzania.

Z-10 Zgłoszenie naruszenia bezpieczeństwa danych osobowych przetwarzanych w formie tradycyjnej i/lub w systemie informatycznym.

Z-11 Wzór raportu pokontrolnego IOD.

KARTA OBSZARU PRZETWARZANIA DANYCH OSOBOWYCH	**Z-01**

Budynek /nazwa, adres/	

I. ZABEZPIECZENIA BUDYNKU

II. PROCEDURA AWARYJNEGO DOSTĘPU

III. WYKAZ POMIESZCZEŃ

Piętro	**Nr pom.**	**Rodzaj pomieszczenia**	**Komórka organizacyjna**	**Miejsce składowania danych i sposób przetwarzania**

KARTA ZBIORU DANYCH OSOBOWYCH	Z-02

OPIS ZBIORU	
Nazwa zbioru	
Piętro	
Nr pomieszczenia	
Miejsce przechowywania/ składowania danych	
Komórka organizacyjna	
Osoba odpowiedzialna	
Zakres zbieranych dane	
Informacja o powierzeniu danych	
INFORMACJE O WERSJI ELEKTRONICZNEJ	
Nazwa programu/zbioru	
Producent	
Lokalizacja bazy danych	
Miejsca eksportu danych	
Zakres danych	
Wersja (jednostanowiskowa/ sieciowa)	

ZASADY OCHRONY DANYCH OSOBOWYCH	**Z-03**

SPIS TREŚCI

I. DEFINICJE
II. UDOSTĘPNIANIE DANYCH OSOBOWYCH
III. POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH
IV. OCHRONA POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE
V. PRZETWARZANIE DANYCH OSOBOWYCH POZA OBSZAREM PRZETWARZANIA
VI. PRZETWARZANIE DANYCH OSOBOWYCH ZNAJDUJĄCYCH SIĘ NA NOŚNIKACH PAPIEROWYCH
VII. MONITOROWANIE OCHRONY ZASOBÓW DANYCH OSOBOWYCH
VIII. ZABEZPIECZENIE ARCHIWUM
IX. ZABEZPIECZENIE SERWEROWNI

I. DEFINICJE

Izba– Beskidzka Izba Lekarska.
Administrator Danych Osobowych (ADO) – Beskidzka Izba Lekarska reprezentowana przez Prezesa Okręgowej Rady Lekarskiej, zwany dalej ADO.
Inspektor ochrony danych (IOD) - osoba wyznaczona przez Administratora, odpowiedzialna za nadzorowanie bezpieczeństwa danych osobowych w Izbie, zwany dalej IOD.
Administrator Systemów Informatycznych (ASI) - osoba wyznaczona przez Administratora odpowiedzialna za wdrażanie technicznych zabezpieczeń systemów informatycznych, ich sprawność i konserwację oraz ochronę w przetwarzanych zbiorach danych osobowych, zwany dalej ASI.
System informatyczny – sprzęt i programy komputerowe którego funkcją jest przetwarzanie danych osobowych.
Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
Serwerownia – pomieszczenie, w którym zlokalizowane są serwery służące do przetwarzania danych osobowych w Izbie.
Zasady – Zasady ochrony danych osobowych.
Polityka – Polityka Bezpieczeństwa.
Ustawa – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz.1000).
Rozporządzenie – – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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).
Bezpieczeństwo systemu informatycznego – wdrożenie przez Administratora lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
Użytkownik - osoba posiadająca upoważnienie wydane przez Administratora, ABI lub ASI dopuszczona do przetwarzania danych osobowych w Systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu.
Przełożony - osoba pełniąca funkcję kierownika komórki organizacyjnej będąca przełożonym użytkownika.
Opiekun - kierownik komórki organizacyjnej lub inna wyznaczona osoba odpowiedzialna za zbiór danych osobowych.
Osoba uprawniona – osoba posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności.

II.UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Dane osobowe mogą być udostępniane w następujących przypadkach:
   a) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych zgodnie z przepisami prawa,
   b) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych,
   c) wniosku osoby, której dane dotyczą.
2. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
3. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na nie następuje w terminie 30 dni od daty jego otrzymania.
4. Wniosek o udostępnienie przekazywany jest do Opiekuna zbioru, który podejmuje decyzję o udostępnieniu. W przypadku, gdy Opiekun ma uwagi do wniosku i przesyła go wraz z opisem uwag do decyzji IOD.

5. IOD wydaje decyzję o udostępnieniu lub braku udostępnienia i przekazuje ją Opiekunowi zbioru danych osobowych.
6. Opiekun zbioru danych osobowych jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.
7. Odpowiedź na wniosek o udostępnienie danych osobowych jest akceptowana i parafowana przez Opiekuna zbioru danych osobowych.
8. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru w następujący sposób:
   a) listem poleconym za potwierdzeniem odbioru,
   b) osobiście,
   c) poprzez teletransmisję danych, zgodnie z procedurami ochrony danych podczas transmisji – określonymi w instrukcji zarządzania danym systemem teleinformatycznym służącym do przetwarzania danych osobowych,
   d) inny, określony konkretnym wymogiem prawnym lub umową.
9. ASI nadzoruje przestrzeganie zasad bezpieczeństwa w przypadku udostępniania danych osobowych drogą teletransmisji danych.
10. Dane osobowe pacjentów, które znajdują się w dokumentacji medycznej są udostępniane na zasadach, w trybie i na sposób określony w przepisach art. 26 i 27 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta i w odrębnej procedurze obowiązującej w Izbie.

III.POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Powierzenie przetwarzania danych osobowych może odbywać się jedynie na podstawie umowy lub innego instrumentu prawnego, zgodnie z zasadami określonymi w art. 28 Rozporządzenia.
2. Decyzje powierzenia przetwarzania danych osobowych podejmuje Administrator danych osobowych, który informuje o tym opiekuna zbioru.
3. Opiekun zbioru danych, który z upoważnienia ADO koordynuje proces powierzenia danych osobowych, informuje IOD o zamiarze powierzenia danych osobowych do przetwarzania.
4. Opiekun zbioru danych przygotowuje projekt umowy powierzenia przetwarzania danych osobowych innemu podmiotowi, a następnie przedkłada go do weryfikacji IOD.
5. W projekcie umowy należy wyspecyfikować zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz inne wymagania Rozporządzenia dotyczące ochrony danych.
6. Każda osoba delegowana do wykonywania zadań na rzecz Izby, związanych z powierzeniem przetwarzania danych osobowych musi podpisać „Oświadczenie użytkownika" stanowiące załącznik do Polityki.
7. Projekt umowy parafują:
   a) IOD,
   b) Opiekun,
   c) ASI – jeżeli zlecenie czynności dotyczyć będzie przetwarzania danych w Systemie informatycznym,
   d) Radca Prawny.
8. Zaparafowany projekt umowy jest przedkładany przez Opiekuna zbioru danych do akceptacji i podpisu ADO.
9. W Izbie prowadzona jest ewidencja podmiotów, z którymi podpisano umowy powierzenia przetwarzania. Ewidencja ta zawiera, co najmniej: nazwę, adres siedziby i dane kontaktowe podmiotu, datę podpisania umowy, przedmiot umowy, informacja o rodzajach zbiorów, które obejmuje umowa przetwarzania.

IV.OCHRONA POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

1. Administrator lub wyznaczona przez niego Osoba uprawniona wspólnie z Opiekunami odpowiadają za należyte zabezpieczenie fizyczne zasobów danych osobowych w podległych komórkach.
2. IOD przeprowadza bezpośrednią kontrolę stanu zabezpieczeń fizycznych zbiorów danych osobowych oraz zgłasza do Administratora swoje uwagi lub rekomenduje zlecenie kontroli specjalistycznej firmie.
3. Obszarem, w którym przetwarzane są dane osobowe są budynki należące do Izby wymienione w „Rejestrze obszarów przetwarzania danych osobowych"
4. IOD jest odpowiedzialny za prowadzenie aktualnego wykazu pomieszczeń, w których przetwarzane są dane osobowe.
5. Przebywanie wewnątrz pomieszczeń, o których mowa w pkt 3, osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Opiekuna zbioru danych osobowych.
6. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania zasad dotyczących wprowadzania osób trzecich do obszaru, o którym mowa w pkt 3. Ruch osób z zewnątrz w wymienionym obszarze powinien odbywać się pod kontrolą osób upoważnionych.
7. Administrator zezwala na przebywanie w pomieszczeniach (o których mowa w pkt 3.) osobom sprzątającym te pomieszczenia, bez konieczności obecności osoby dopuszczonej do przetwarzania danych. Osoby te podpisują „Oświadczenie o zachowaniu poufności".
8. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób dopuszczonych do danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

9. Pomieszczenia w których przetwarzane są dane wrażliwe oraz pomieszczenia serwerowni i archiwów powinny podlegać specjalnej ochronie o których mowa w rozdziale VII, VIII i IX niniejszych Zasad.
10. Opiekun zbioru danych osobowych zabezpiecza zgodnie z wytycznymi pkt 7,8,9 obszar przetwarzania danych.
11. Budynki i pomieszczenia Izby posiadają zabezpieczenia które opisane są w „Kartach obszarów przetwarzania danych osobowych" – stanowiących załącznik do Polityki.

V.PRZETWARZANIE DANYCH OSOBOWYCH POZA OBSZAREM PRZETWARZANIA

W sytuacji przetwarzania danych osobowych na komputerach przenośnych lub dokumentach papierowych poza obszarem wymienionym w rozdziale IV pkt 3, należy bezwzględnie chronić te dane przed dostępem do nich osób nieupoważnionych, np. poprzez szyfrowanie dysków, zabezpieczanie plików hasłem.

VI.PRZETWARZANIE DANYCH OSOBOWYCH ZNAJDUJĄCYCH SIĘ NA NOŚNIKACH PAPIEROWYCH

1. Dane osobowe zawarte w dokumentacji papierowej przetwarzane są przez Osoby uprawnione zgodnie z zasadami Polityki.
2. Rejestracje, obieg i udostępnianie dokumentów papierowych Izby zawierających dane osobowe reguluje Instrukcja Kancelaryjna.
3. Archiwizowanie papierowych zbiorów danych osobowych odbywa się w oparciu o obowiązujące przepisy prawa.
4. Kopie papierowe z danymi osobowymi muszą być oznaczone i przechowywane w zamykanych na klucz szafach.
5. Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, parapetach itp.
6. Wydruki i inne dokumenty zawierające dane osobowe są przechowywane w pomieszczeniach do tego wyznaczonych. Na stanowiskach pracy mogą być dostępne jedynie dokumenty dotyczące danej sprawy. Stosowana jest zasada tzw. czystego biurka.
7. Zawsze należy sprawdzać czy w urządzeniu kopiującymi/drukującym nie pozostawiono dokumentacji.
8. Po zakończeniu pracy wszelka dokumentacja zawierająca dane osobowe jest przechowywana w szafach zamykanych na klucz lub w pomieszczeniach o ograniczonym dostępie osób postronnych, do których dostęp jest utrudniony poprzez zastosowanie zabezpieczeń fizycznych takich jak: zamki w drzwiach, kraty w oknach, systemy kontroli dostępu itp.
9. Wszelkie dokumenty zawierające dane osobowe niszczone są z użyciem niszczarek o właściwych parametrach cięcia, zgodnie z przyjętymi normami międzynarodowymi.

VII.MONITOROWANIE OCHRONY ZASOBÓW DANYCH OSOBOWYCH

1. Opiekunowie zbiorów danych osobowych przekazują IOD:
   a) informację na temat stwierdzenie próby lub faktu naruszenia przepisów dotyczących ochrony danych lub bezpieczeństwa Systemu informatycznego, w którym przetwarzane są dane osobowe,
   b) zmiany na temat zabezpieczeń i ochrony danych osobowych przetwarzanych w Izbie,
   c) zmiany pomieszczeń, w których przetwarzany jest poszczególny zasób danych osobowych w podległej komórce organizacyjnej
2. IOD jest na bieżąco informowany o:
   a) zatrudnieniu nowego pracownika
   b) ustaniu zatrudnienia w Izbie określonej osoby, celem kontroli aktywności jego kont w systemie informatycznym,
   c) wykazu osób którzy będą świadczyli usługi w ramach podpisanych umów cywilnoprawnych jak również późniejszych zmian w tym wykazie,
   d) przeniesieniu pracownika do innej komórki organizacyjnej Izby, celem kontroli jego praw do dostępu do danych osobowych.
3. ASI przekazuje IOD:
   a) wykaz systemów teleinformatycznych – aplikacji, w których przetwarzane są dane osobowe z informacją o programach zastosowanych do przetwarzania tych danych, wraz z wprowadzonymi na bieżąco zmianami,
   b) wykaz opisu struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, wraz z wprowadzonymi na bieżąco zmianami,
   c) wykazu opisu sposobu przepływu danych pomiędzy poszczególnymi systemami,
   d) wnioski o nadanie uprawnień do przetwarzania danych w systemie informatycznym do zakresu których ASI ma wątpliwości.
4. IOD ustala szczegółowe zakresy potrzebnych informacji oraz formę i tryb ich przekazywania.
5. Każda zmiana informacji w zakresie ujętym w pkt 1-2 wymaga bieżącej aktualizacji wykazów prowadzonych przez IOD.

VIII.ZABEZPIECZENIE ARCHIWUM

1. Archiwum posiada:
   a) pomieszczenia suche, widne, całkowicie zabezpieczone przed czynnikami szkodliwymi wpływającymi na przechowywaną dokumentację jak i na stan zdrowia pracownika prowadzącego archiwum,
   b) okno z roletą antywłamaniową,
   c) drzwi masywne wyposażone w dwa mocne zamki,
   d) instalację elektryczną której przewody są odpowiednio zabezpieczone,

e) żarówki zamontowane w kloszach,
f) odpowiednią ilość sprzętu przeciwpożarowego,
g) centralne ogrzewanie,
h) podłogi z gładką fakturą,
a) regały metalowe zamykane na klucz dostosowane do przechowywania zasobów archiwalnych,
b) zabezpieczenie systemem alarmowym odnotowującym datę i godzinę jego aktywacji i deaktywacji.

2. W archiwum nie wolno:
   a) palić papierosów,
   b) używać grzejników elektrycznych,
   c) przechowywać żadnych innych przedmiotów poza przedmiotami stanowiącymi jego wyposażenie.
3. Za całokształt pracy archiwum zakładowego odpowiedzialny jest Prezes ORL BIL.
4. Pracownik prowadzący archiwum zakładowe winien być przeszkolony w zakresie czynności archiwalnych, fakt ten powinien być odpowiednio udokumentowany.
5. Do podstawowych obowiązków pracownika archiwum zakładowego należy:
   a) współpraca z komórkami organizacyjnymi w zakresie opieki nad dokumentacją i odpowiedniego jej przygotowania do przekazania archiwum,
   b) przyjmowanie w stanie uporządkowanym materiałów archiwalnych i dokumentacji niearchiwalnej z poszczególnych komórek organizacyjnych,
   c) przechowywanie i zabezpieczenie przejętej dokumentacji oraz prowadzenie pełnej ewidencji,
   d) udostępnianie akt osobom upoważnionym,
   e) inicjowanie komisyjnego brakowania dokumentacji niearchiwalnej i przekazywanie jej do zniszczenia odpowiednim firmom.
   f) znajomość struktury organizacyjnej Izby oraz instrukcji kancelaryjnej, Ustawy o narodowym zasobie archiwalnym i archiwach / DZ.U. Nr 38 poz. 173 z 1983r. z późniejszymi zmianami/, Rozporządzenia Ministra Kultury z dnia 16.09.2002r. ws. postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych oraz instrukcji dot. prowadzenia archiwum.
6. Prawo wstępu do archiwum zakładowego mają:
   a) pracownik archiwum,
   b) upoważnieni pracownicy,
   c) przełożeni pracownika archiwum,
   d) pracownicy obsługi technicznej Izby w obecności pracownika zakładu lub jego przełożonego,
   e) osoby z zewnątrz wyłącznie w obecności archiwisty,
   f) upoważnione organy kontroli wewnętrznej i zewnętrznej za okazaniem stosownego upoważnienia,
   g) przedstawiciel archiwum państwowego.
7. Każdorazowe wejście i wyjście z archiwum przez osoby, o których mowa w pkt. 6c, 6d, 6e i 6f, odnotowywane jest w rejestrze wejść i wyjść.
8. Po zakończeniu pracy, pomieszczenie archiwum jest zamykane, plombowane i zabezpieczane alarmem.
9. Rejestr wejść i wyjść musi być przechowywany pod właściwym zabezpieczeniem.
10. Klucze do archiwum i kod dostępu do alarmu przechowuje się pod właściwym zabezpieczeniem.
11. Klucze do archiwum może pobrać tylko pracownik archiwum lub jego przełożeni.
12. Rejestr kluczy powinien zawierać następujące informacje
    a) Datę i czas
    b) Numer klucza
    c) Nazwisko i imię osoby pobierającej

IX.ZABEZPIECZENIE SERWEROWNI

1. Pomieszczenie jest wyposażone w:
   a) drzwi antywłamaniowe
   b) system alarmowy (czujnik otwarcia drzwi, czujnik ruchu) potrafiący odnotować w pamięci datę i godzinę jego aktywacji i deaktywacji.
   c) system przeciwpożarowy
   d) systemem wentylacji bytowej
   e) systemem wentylacji wywietrzania
   f) koryta siatkowe do prowadzenia kabli
   g) zasilanie awaryjne z urządzeń podtrzymujących napięcie
   h) sejf na nośniki z danymi osobowymi
2. W pomieszczenie serwerowni nie wolno:
   a) palić papierosów,
   b) używać grzejników do ogrzewania pomieszczenia,
   c) przechowywać żadnych innych przedmiotów poza przedmiotami stanowiącymi jego wyposażenie.
3. Nadanie uprawnień do zarządzania infrastrukturą znajdującą się w serwerowni, następuje na pisemny wniosek IOD, po zatwierdzeniu przez Administratora.
4. Prawo wstępu do serwerowni mają:
   a) upoważnieni pracownicy

b) przełożeni upoważnionych pracowników
c) pracownicy obsługi technicznej Izby w obecności pracownika zakładu lub jego przełożonego,
d) osoby z zewnątrz wyłącznie w obecności upoważnionego pracownika
e) upoważnione organy kontroli wewnętrznej i zewnętrznej za okazaniem stosownego upoważnienia.

5. Każdorazowe wejście i wyjście z serwerowni przez osoby, o których mowa w pkt. 4c, 4d, i 4e, odnotowywane jest w rejestrze wejść i wyjść.
6. Po zakończeniu pracy, pomieszczenie serwerowni jest zamykane i zabezpieczane alarmem.
7. Klucze do serwerowni i kod dostępu do alarmu przechowuje się w pomieszczeniach zabezpieczonych przed dostępem osób nieupoważnionych w szafkach na klucze zabezpieczone zamkiem.
8. Rejestr wejść i wyjść musi być przechowywany pod właściwym zabezpieczeniem.
9. Klucze do serwerowni i kod dostępu do alarmu przechowuje się pod właściwym zabezpieczeniem.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH	**Z-04**

Nazwisko i imię		
Sygnatura upoważnienia		

DEFINICJE

Izba – Beskidzka Izba Lekarska,
Administrator – Beskidzka Izba Lekarska reprezentowana przez Prezesa Okręgowej Rady Lekarskiej,
Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie,
Osoba uprawniona – osoba posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności,
Użytkownik - osoba wykonująca zadania i obowiązki wynikające z umowy o pracę, umów cywilnoprawnych, umowy praktyki na rzecz Izby,
Rozporządzenie - Rozporządzenie 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),

DANE UŻYTKOWNIKA

Identyfikator użytkownika	
PESEL	
Stanowisko / pełnione obowiązki*	
Komórka organizacyjna	

UPOWAŻNIENIE ADMINISTRATORA

Na podstawie art. 29 i 32 ust. 4 Rozporządzenia upoważniam wyżej wymienionego Użytkownika do Przetwarzania danych osobowych i wydaję polecenie przetwarzania danych osobowych w następujących zbiorach:

Dokumentacja papierowa (podać nazwy zbiorów z rejestru)	**Systemy informatyczne (podać nazwy zbiorów i login)**

W zakresie: (właściwe wstawić do tabeli powyżej w odniesieniu do zbiorów):
kopiowanie (K) drukowanie (DK) przeglądanie (P), wprowadzanie (W), modyfikacja (M), usuwanie (U), archiwizowanie (A), przekazywanie na zewnątrz (PZ), niezbędne do realizacji zadań stanowiska pracy (I)

Upoważnienie jest ważne**
- ☐ na czas obowiązywania podpisanej przez Użytkownika umowy z Izbą,
- ☐ ważne do dnia ……
- ☐ przez okres wykonywania zadania …….

Upoważnienie niniejsze nie upoważnia do udzielania dalszych upoważnień i może być w każdym czasie zmienione lub odwołane.
Wcześniej wydane upoważnienie nr …….. z dnia …… zostaje odwołane.***

Data	**…….** **Podpis *ADO***

POTWIERDZENIE ODBIORU PRZEZ UŻYTKOWNIKA

Data ……	**…….** **Podpis *Użytkownika***

** niewłaściwe skreślić, ** właściwe zaznaczyć, *** należy uzupełnić w przypadku zmiany zakresu upoważnienia*

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH					**Z-05**
Sygnatura upoważnienia	**Imię i nazwisko osoby upoważnionej**	**Data nadania uprawnień**	**Data odebrania uprawnień**	**Zakres uprawnień**	**Identyfikator w systemie informatycznym**

OŚWIADCZENIE UŻYTKOWNIKA	**Z-06**

Nazwisko i imię	

DEFINICJE

Izba– Beskidzka Izba Lekarska
Administrator – Prezes Okręgowej Rady Lekarskie
IOD - osoba wyznaczona przez Administratora, pełniąca obowiązki Inspektora Ochrony Danych, odpowiedzialna za nadzorowanie bezpieczeństwa danych osobowych w Izbie.
Użytkownik - osoba wykonująca zadania i obowiązki wynikające z umowy o pracę, umów cywilnoprawnych, umowy praktyki na rzecz Izby.
Przełożony - osoba pełniąca funkcję kierownika komórki organizacyjnej lub koordynatora będąca przełożonym Użytkownika.
Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
System informatyczny – sprzęt i programy komputerowe którego funkcją jest Przetwarzanie danych osobowych.
Polityka – Polityka Bezpieczeństwa
Zasady – Zasady ochrony danych osobowych.
Instrukcja – Instrukcja zarządzania systemami informatycznymi.
Procedury – Regulaminy, instrukcje i procedury obowiązujące w Izbie.
Ustawa – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz.1000).
Rozporządzenie – Rozporządzenie 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).

DANE UŻYTKOWNIKA

Identyfikator użytkownika*	
PESEL	
Stanowisko / pełnione obowiązki**	
Komórka organizacyjna / nazwa firmy zewnętrznej**	

OŚWIADCZENIE O ZAPOZANIU SIĘ I PRZESTRZEGANIU PRZEPISÓW PRAWA

Oświadczam, że:

1. Zobowiązuję się do zachowania w tajemnicy wszelkich informacji dotyczące przetwarzania oraz sposobów zabezpieczenia danych osobowych, do których mam lub będę miał(a) dostęp w związku z wykonywaniem:***
   - ☐ zadań i obowiązków wynikających z umowy o pracę zarówno w trakcie wykonywania umowy i po jej ustaniu,
   - ☐ zadań wynikających z umowy cywilnoprawnej zarówno w trakcie wykonywania umowy i po jej ustaniu,
   - ☐ zadań wynikających z umowy praktyki zarówno w trakcie wykonywania umowy i po jej ustaniu.
2. Zostałem(am) poinformowany(a) o obowiązujących w Izbie Procedurach, Zasadach i Instrukcjach oraz zobowiązuje się je przestrzegać.
3. Zapoznałem(am) się z zapisami zawartymi w Polityce i przyjmuję je do wiadomości i stosowania.
4. Zostałem(am) poinformowany(a) o obowiązującej Ustawie i Rozporządzeniu oraz o grożącej stosownie do przepisów rozdziału 8 Ustawy o odpowiedzialności karnej,
5. Zobowiązuję się do przestrzegania zapisów określonych w zarządzeniach Administratora.
6. Zobowiązuję się do zachowania tajemnicy służbowej.

OCHRONA DANYCH

1. Będę wykorzystywał swój służbowy adres poczty elektronicznej wyłącznie w celu prowadzenia korespondencji związanej z działalnością Izby.
2. Bez upoważnienia służbowego nie będę wykorzystywał(a) danych osobowych ze zbiorów Izby.
3. Zapewnię ochronę danym osobowym przetwarzanym w Izbie, a w szczególności zabezpieczę je przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem.
4. Nie będę wykorzystywać przetwarzanych danych osobowych w celach osobistych lub wykraczających poza posiadany zakres obowiązków, a także w prywatnych rozmowach na terenie Izby i poza nią. Przyjmuję do wiadomości, że niezastosowanie się do niniejszego postanowienie skutkuje naganą z wpisaniem do akt lub zwolnieniem dyscyplinarnym.
5. Natychmiast zgłoszę Przełożonemu lub IOD stwierdzenie próby lub faktu naruszenia ochrony danych

osobowych przetwarzanych w jakiejkolwiek formie, w tym w systemie informatycznym.
OŚWIADCZENIE O POUFNOŚCI
1. Wszelkie zobowiązania w niniejszym Oświadczeniu obejmują okres w trakcie lub/ i w związku z pracą w Izbie oraz okres po jej zakończeniu. 2. Przyjmuję do wiadomości, że jestem zobowiązany/a do zachowania w poufności tj. nie przekazywania komukolwiek w jakiejkolwiek formie jakiejkolwiek informacji o których powziąłem/am wiedzę w trakcie lub/ i w związku z pracą w Izbie w czasie trwania umowy, na podstawie której wykonywałem/am te prace i po jej rozwiązaniu. 3. Po rozwiązaniu umowy w związku z pracą lub na zlecenie Izby zobowiązuję się do zwrotu Izbie wszelkich dokumentów, w posiadanie których wszedłem w trakcie wykonywania pracy, lub innym materiałów dotyczących Izby, jakie zostały sporządzone, zebrane, opracowane, uzyskane, otrzymane lub w inny sposób utrwalone w jakimkolwiek z okresów, o których mowa w ust.2, włączając w to kopie, odpisy, a także zapisy utrwalone na dowolnych nośnikach zapisu najpóźniej do dnia zaprzestania pracy.

I. POTWIERDZENIE UŻYTKOWNIKA	**Podpis *Użytkownika* stanowiący jednocześnie jego wzór**
…… **Data**	

** wypełnia ABI , ** niewłaściwe skreślić, *** właściwe zaznaczyć*

PROCEDURA NADAWANIA, ZMIANY, ODEBRANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH	**Z-07**

DEFINICJE

Izba– Beskidzka Izba Lekarska
Administrator – Prezes Okręgowej Rady Lekarskie
IOD - osoba wyznaczona przez Administratora, pełniąca obowiązki Inspektora Ochrony Danych, odpowiedzialna za nadzorowanie bezpieczeństwa danych osobowych w Izbie.
Użytkownik - osoba wykonująca zadania i obowiązki wynikające z umowy o pracę, umów cywilnoprawnych, umowy praktyki na rzecz Izby.
Przełożony - osoba pełniąca funkcję kierownika komórki organizacyjnej lub koordynatora będąca przełożonym Użytkownika.
Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
System informatyczny – sprzęt i programy komputerowe którego funkcją jest Przetwarzanie danych osobowych.
Polityka – Polityka Bezpieczeństwa
Zasady – Zasady ochrony danych osobowych.
Instrukcja – Instrukcja zarządzania systemami informatycznymi.
Procedury – Regulaminy, instrukcje i procedury obowiązujące w Izbie.
Ustawa – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz.1000).
Rozporządzenie – Rozporządzenie 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).

1. Administrator Danych Osobowych nadaje, zmienia i odbiera uprawnienia Użytkowników do przetwarzania danych osobowych.
2. Kierownik Biura BIL przygotowuje 2 egzemplarze Oświadczeń i przekazuje je Użytkownikowi do podpisu.
3. Po otrzymaniu podpisanego Oświadczenia Kierownik Biura BIL przygotowuje 2 egzemplarze Upoważnienia:
   - nadaje sygnaturę upoważnienia i wprowadza go do rejestru upoważnień,
   - uzupełnia rozdział „Dane użytkownika”,
   - uzupełnia rozdział „Upoważnienie administratora” określając w porozumieniu z Przełożonym w jakim zakresie jest nadane upoważnienie i na jaki okres,
   - przedstawia ADO upoważnienie do podpisu.
4. Jeżeli wymagana jest zmiana uprawnień Użytkownika lub odebranie uprawnień Kierownik Biura BIL przygotowuje 2 nowe egzemplarze Upoważnienia, które jednocześnie unieważniają poprzednie i przedstawia je ADO do podpisu.
5. Przygotowaną dokumentację (Upoważnienia, Oświadczenia) przedstawia Użytkownikowi do podpisu.
6. Podpisane komplety dokumentów Kierownik Biura BIL:
   a. dołącza do akt osobowych Pracownika lub jako załącznik do umów cywilnoprawnych oraz
   b. dołącza do ewidencji osób upoważnionych.

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH	**Z-08**

SPIS TREŚCI

DEFINICJE
POSTANOWIENIA OGÓLNE
PODEJRZENIE LUB STWIERDZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH
TRYB POSTĘPOWANIA

DEFINICJE

Izba– Beskidzka Izba Lekarska
Administrator – Prezes Okręgowej Rady Lekarskie
IOD - osoba wyznaczona przez Administratora, pełniąca obowiązki Inspektora Ochrony Danych, odpowiedzialna za nadzorowanie bezpieczeństwa danych osobowych w Izbie.
Użytkownik - osoba wykonująca zadania i obowiązki wynikające z umowy o pracę, umów cywilnoprawnych, umowy praktyki na rzecz Izby.
Przełożony - osoba pełniąca funkcję kierownika komórki organizacyjnej lub koordynatora będąca przełożonym Użytkownika.
Przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
System informatyczny – sprzęt i programy komputerowe którego funkcją jest Przetwarzanie danych osobowych.
Polityka – Polityka Bezpieczeństwa
Zasady – Zasady ochrony danych osobowych.
Instrukcja – Instrukcja zarządzania systemami informatycznymi.
Procedury – Regulaminy, instrukcje i procedury obowiązujące w Izbie.
Ustawa – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz.1000).
Rozporządzenie – Rozporządzenie 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).

POSTANOWIENIA OGÓLNE

1. Instrukcja określa tryb postępowania w sytuacji naruszenia ochrony danych osobowych gromadzonych i przetwarzanych zarówno w zbiorach informatycznych, jak i w sposób tradycyjny (w formie papierowej, ustnej). Instrukcję stosuje się także w przypadku, gdy stwierdzono naruszenie zabezpieczeń sprzętu informatycznego, sieci komputerowej, systemu alarmowego, systemu zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe.
2. Przez naruszenie bezpieczeństwa danych osobowych rozumie się niezgodne z przepisami obowiązującego prawa przetwarzanie danych osobowych (m.in. zbieranie, utrwalanie, przechowywanie, zabezpieczanie, opracowywanie, zmienianie oraz usuwanie), wynikające zarówno z działań umyślnych jak i niezamierzonych, wywołane działaniem człowieka, błędami urządzeń a także działaniem sił natury.
3. Każdy Pracownik Izby odpowiedzialny jest za zgodną z prawem ochronę danych osobowych i ich zabezpieczenie.

PODEJRZENIE LUB STWIERDZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH. ZAPOBIEGANIE NARUSZENIOM.

1. Na fakt naruszenia zabezpieczeń systemu informatycznego mogą wskazywać:
   a) stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem, naruszenie lub uszkodzenie obudowy stacji roboczej),
   b) wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach oraz wirusach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach),
   c) różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych),
   d) zmiany w jakości komunikacji w sieci telekomunikacyjnej (gwałtowne opóźnienia lub przyśpieszenia wykonywanych czynności),
   e) inne sytuacje nadzwyczajne, np. nieprawidłowości w działaniu sprzętu komputerowego po otwarciu podejrzanej wiadomości e-mail.
2. Na fakt naruszenia bezpieczeństwa danych osobowych przetwarzanych w formie tradycyjnej może wskazywać:
   a) uszkodzenia lub nieprawidłowe działanie zabezpieczeń pomieszczenia, np. plomb, zamków (np. wyłamanie, naruszenie), kluczy elektronicznych, systemów alarmowych, przeciwpożarowych itp.,
   b) nieprawidłowe przechowywanie, udostępnienie, przekazanie danych osobowych, w tym omawianie kwestii osobistych dotyczących pacjenta/pracownika w rozmowie prywatnej lub wykraczającej poza

zakres obowiązków,
c) przebywanie osób nieupoważnionych w miejscach, gdzie przetwarza się dane osobowe,
d) niezgodne z procedurami niszczenie danych osobowych, w tym wyrzucanie ich do koszy na śmieci,
e) dostęp do danych wykraczający lub niezgodny z zakresem obowiązków służbowych.

3. Aby odpowiednio wcześnie wykryć przypadki naruszenia zabezpieczenia danych osobowych przetwarzanych:
   a) w systemie informatycznym i zapobiec ich negatywnym skutkom - należy okresowo przeglądać uprawnienia użytkowników. Za nadzór nad uprawnieniami użytkowników w systemie informatycznym odpowiedzialny jest IOD, który zgłasza ADO wszelkie nieprawidłowości w tym zakresie;
   b) w formie tradycyjnej (dokumentacja papierowa) – należy okresowo przeglądać zakresy obowiązków Użytkowników w celu sprawdzenia czy określony zakres obowiązków jest zgodny z zajmowanym stanowiskiem. Nadzór w tej materii pełni IOD, który zgłasza ADO wszelkie nieprawidłowości w tym zakresie.
4. IOD ma prawo wnioskować do Przełożonego o wyjaśnienie posiadania przez Użytkownika nadmiernych uprawnień do przetwarzania danych osobowych, nieadekwatnych do realizowanych zadań, zarówno w systemie informatycznym oraz/lub do danych przetwarzanych w postaci zbiorów papierowych (dokumenty). W przypadku braku satysfakcjonującej odpowiedzi IOD ma prawo obniżyć uprawnienia do bezpiecznego poziomu.
5. W uzasadnionych przypadkach możliwe jest odebranie uprawnień Użytkownikowi zanim nastąpi wypowiedzenie umowy o pracę lub wypowiedzenie współpracy. Środki takie są stosowane w sytuacjach:
   a) kiedy istnieje uzasadnione ryzyko, że Użytkownik może podjąć działania mogące spowodować zniszczenie albo skompromitowanie dostępnych mu informacji,
   b) uszkodzenie administrowanych przez niego zasobów informatycznych,
   c) użytkownik posiada nadmierne uprawnienia, nieadekwatne do realizowanych zadań.

TRYB POSTĘPOWANIA

1. Użytkownik, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie informatycznym lub w formie tradycyjnej zobowiązany jest do niezwłocznego poinformowania o tym Opiekuna bazy danych osobowych.
2. Opiekun zbioru danych osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:
   - zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
   - powiadomienia o zaistniałym fakcie IOD (a jeśli naruszenie dotyczy bazy danych przetwarzanej w systemie informatycznym, również ASI) za pomocą formularza Z-10, stanowiącego załącznik do Polityki Bezpieczeństwa.
   - jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
   - przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.
   - podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.
     a) zabezpieczenia urządzeń, które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
     b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,
     c) zmianę hasła na konto administratora i użytkownika, poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu,
     d) zabezpieczenia miejsca zdarzenia i ograniczenie do niego dostępu.
3. ASI zobowiązany jest do:
   - szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
   - przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.
4. Po przywróceniu normalnego stanu zbioru danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości, tj:

   - Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
   - Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać

zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
- Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z Kodeksu Pracy.
- Przegląd zabezpieczeń danych osobowych, których bezpieczeństwo zostało naruszone, wykonanie analizy ryzyka.
- Podjąć inne działania, jeżeli wymagają tego przepisy prawa (np. zgłosić incydent do organu ochrony danych osobowych).

5. Opiekun zbioru danych osobowych, w której nastąpiło naruszenie ochrony danych osobowych, przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 14 dni od daty jego zaistnienia przekazuje IOD.
6. IOD przeprowadza analizę raportów pochodzących od Opiekunów zbiorów danych osobowych i na ich podstawie sporządza raport na temat sposobu zabezpieczenia naruszonego zbioru danych osobowych, w związku z jego naruszeniem oraz sposobu wyeliminowania podobnych zdarzeń w przyszłości.

Załącznik Z-09

WZÓR REJESTRU CZYNNOŚCI PRZETWATWARZANIA

1. Nazwa czynności przetwarzania	
2. Jednostka organizacyjna	
3. Cel przetwarzania	
4. Kategorie osób	
5. Kategorie danych osobowych	
6. Podstawa prawna przetwarzania	
7. Źródło danych	
8. Planowany termin usunięcia kategorii danych (jeśli to możliwe)	
9. Nazwa współadministratora i dane kontaktowe (jeśli dotyczy)	
10. Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy)	
11. Kategorie odbiorców (innych niż podmiot przetwarzający)	
12. Nazwa systemu lub oprogramowania	
13. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe)	
14. Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu) **- jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń**	

ZGŁOSZENIE NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH PRZETWARZANYCH W FORMIE TRADYCYJNEJ I/LUB W SYSTEMIE INFORMATYCZNYM	**Z-10**
I. DANE ZGŁASZAJĄCEGO	
Nazwisko i imię	
Stanowisko / funkcja	
Komórka organizacyjna	
Podpis	
II. DANE INCYDENTU	
Data i czas incydentu	
Określenie, czy incydent dotyczy przetwarzania danych osobowych /informacji w systemie informatycznym czy w formie tradycyjnej (lub obydwu form przetwarzania)	
Opis incydentu, w tym określenie ilości danych, których bezpieczeństwo zostało naruszone (jeśli to możliwe)	
Określenie Podmiotów danych osobowych oraz kategorii danych osobowych, których bezpieczeństwo zostało naruszone/mogło zostać naruszone lub określenie	

innych kategorii informacji	
Podjęte przeciwdziałania – jeśli podjęto	
III. DANE LOKA**LIZACJI** STACJI ROBOCZEJ	
Budynek, kondygnacja, pomieszczenie	
Nr DIN stacji roboczej	

Definicje:

1. **Podmiot danych osobowych -** osoby/grupy osób, których dane osobowe przetwarzane są w Izbie, np. lekarze, pracownicy, Kontrahenci.
2. **Kategorie danych osobowych –** rodzaje przetwarzanych danych osobowych, np. imię i nazwisko, adres, PESEL, dane o stanie zdrowia, dane genetyczne, dane biometryczne.

Załącznik Z-11

WZÓR RAPORTU POKONTROLNEGO IOD.

Data przeprowadzenia kontroli	
Rodzaj kontroli – planowa/ doraźna/ w wyniku incydentu	
Opis kontrolowanego obszaru ochrony danych osobowych	
Wykaz zbiorów, które podlegały kontroli	
Wykaz podjętych czynności kontrolnych	
Wykaz załączników dokumentujących przebieg kontroli	
Zakres kontroli	
Wnioski pokontrolne	
Rekomendowane działania	
Osoba/ podmiot kontrolujący	
Data sporządzenia raportu	

Lista załączników:

……..

……

(podpis i pieczęć kontrolującego)

SEKRETARZ
OKRĘGOWEJ RADY LEKARSKIEJ

MACIEJ SKWARNA

WICEPREZES
OKRĘGOWEJ RADY LEKARSKIEJ

RADOSŁAW PIWOWARCZYK