**POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH**

**W INDYWIDUALNEJ PRAKTYCE LEKARSKIEJ/PRAKTYCE STOMATOLOGICZNEJ/NZOZ**

***(wpisać właściwą nazwę)***

*(miejscowość, data)*

**§1 Postanowienia ogólne**

1. Polityka Bezpieczeństwa rozumiana jest jako wykaz praw, reguł i wewnętrznych praktyk regulujących sposób zarządzania i ochrony danych osobowych wewnątrz praktyki\* (wpisać właściwą nazwę podmiotu oraz pełny adres) ………………………, zwanej dalej Praktyką/NZOZ/Podmiotem.
2. Dokument obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie, jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

**§2 Podstawa prawna**

1. Polityka Bezpieczeństwa została opracowana na podstawie:
2. 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),
3. Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. t.j. Dz. U. z 2016 r. poz. 1638, 1948, 2260, z 2017 r. poz. 2110, 2217),
4. Ustawa z dnia 06 kwietnia 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2017 r. poz. 1318, 1524),
5. Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach zdrowotnych finansowanych ze świadczeń publicznych (t.j. Dz. U. z 2017 r. poz. 1938, 2110, 2217, 2361, 2434),
6. Ustawa z dnia 21 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. 2017 tj. poz.1845),
7. Pozostałe przepisy regulujące system ochrony danych osobowych, w tym przepisy wydane na podstawie art. 40 RODO.
8. Administratorem danych osobowych jest Praktyka/NZOZ (wpisać pełną nazwę podmiotu).
9. Dane pacjentów Praktyki są chronione zgodnie z polskim prawem oraz procedurami dotyczącymi bezpieczeństwa i poufności przetwarzanych danych.

**§3 Definicje**

1. **Administrator Danych Osobowych (ADO)** – rozumie się przez to …………………….(wpisać pełną nazwę podmiotu).
2. **Inspektor ochrony danych (IOD)** – osoba wyznaczona przez Administratora, odpowiedzialna za nadzorowanie prawidłowego przetwarzania danych osobowych i doradzająca w tym zakresie ADO.
3. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Dane te mogą dotyczyć pracowników podmiotu wykonującego działalność leczniczą, jego pacjentów lub osoby współpracujące z podmiotem.
4. **Przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
5. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.
6. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
7. **Identyfikator użytkownika** (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
8. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
9. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
10. **Integralność danych** – funkcjonalność zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
11. **Poufność danych** – funkcjonalność zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
12. **Rozporządzenie (RODO)** – 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).

**§4 Deklaracja**

1. Administrator danych mając świadomość, iż przetwarza dane wrażliwe pacjentów deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.
2. Administrator deklaruje, że proces przetwarzania danych osobowych uwzględnia zasady, o których mowa w Motywie 39 RODO oraz artykule 5 ust. 1 ppkt a) – e) RODO.
3. Każdy pracownik upoważniony do przetwarzania danych, świadomy odpowiedzialności, zobowiązany jest postępować zgodnie z przyjętymi zasadami i minimalizować zagrożenia wynikające z błędów ludzkich.
4. W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.
5. Dane osobowe w podmiocie przetwarzane są w sposób legalny, na podstawie art. 6 ust. 1 ppkt a) i b) oraz art. 9 ust. 2 ppkt h) RODO w związku z art. 3 ust. 1 i 2 ustawy o działalności leczniczej oraz art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, a także w związku z art. 54 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa lub innych właściwych przepisów z zakresu prawa ubezpieczeń społecznych.
6. W przypadku konieczności pozyskania zgody na przetwarzanie danych osobowych podmiot korzysta z szablonu, którego wzór stanowi Załącznik nr 7. Zgoda na przetwarzanie danych osobowych może zostać pozyskana w inny sposób, ale musi ona spełniać przesłanki, o których mowa w art. 7 ust. 1 RODO.
7. Zakres pozyskiwanych danych wynika z przepisów prawa, o których mowa w §2 niniejszego dokumentu i jest adekwatny do zdefiniowanych celów przetwarzania.
8. Okres czasu, przez jaki dane osobowe są przetwarzane wynika z przepisów prawa, o których mowa w §2 niniejszego dokumentu. Terminy przechowywania dokumentacji medycznej określa art. 29 Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

**§5 Wykaz zbiorów osobowych**

1. Dane osobowe przetwarzane przez ADO są zorganizowane są w zbiory, za pomocą których Administrator może ocenić ryzyko ich przetwarzania oraz ocenić konieczność przeprowadzenia procedury oceny skutków dla systemu ochrony danych, o którym mowa w art. 35 RODO.
2. Zbiory danych osobowych opisane są z uwzględnieniem poniższych informacji:
3. Nazwa zbioru,
4. Rodzaj pomieszczenia, gdzie przetwarzany jest zbiór,
5. Piętro i nr pomieszczenia,
6. Miejsce składowania danych,
7. Opis struktury danych (zbierane dane),
8. Programy, aplikacje służące do przetwarzania danych i sposób przepływu danych między nimi.
9. Szczegółowy opis zbiorów danych osobowych stanowi Załącznik nr 1 do Polityki.

**§6 Wykaz miejsc przetwarzania**

1. Obszarem przetwarzania danych są wszystkie pomieszczenia, korytarze oraz obszar Praktyki.
2. Szczegółowy wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowi załącznik nr 2 do niniejszej dokumentacji. Dla pomieszczeń, w których dane są gromadzone na czas nieobecności w nich osób upoważnionych opisano zastosowane środki ochrony technicznej.

**§7 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.:
4. Imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
5. cele przetwarzania;
6. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
8. 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;
9. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
10. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
11. Rejestr czynności przetwarzania jest prowadzony w oparciu o załącznik nr 8.

**§9 Ewidencja osób upoważnionych do przetwarzania danych osobowych**

1. Wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi załącznik nr 3 do niniejszej dokumentacji.
2. Ewidencja zawiera: imię i nazwisko osoby upoważnionej, stanowisko, datę nadania i ustania uprawnień oraz zakres, a w przypadku, kiedy dane są przetwarzane za pomocą programu komputerowego również identyfikator dostępowy do tego programu.

**§10 Środki organizacyjne ochrony danych osobowych**

1. Przetwarzanie danych osobowych na terenie Praktyki może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień jest ściśle proporcjonalny do tych zadań.
2. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
3. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie wydane przez Administratora danych osobowych. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 4 do niniejszej dokumentacji.
4. Unieważnienie upoważnienia do przetwarzania danych osobowych następuje na piśmie, wg. wzoru stanowiącego załącznik nr 5 do niniejszej dokumentacji.
5. Każdy pracownik Praktyki co najmniej raz na rok musi odbyć szkolenie z zakresu ochrony danych osobowych. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.
6. Każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą dokumentacją i zrozumieniem wszystkich zasad bezpieczeństwa. Wzór potwierdzenia stanowi załącznik nr 6 do niniejszej dokumentacji. Podpisany dokument jest dołączany do akt osobowych pracownika lub stanowi załącznik do zawartej umowy.
7. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.
8. Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz.
9. Po zakończeniu pracy, przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
10. W podmiocie zabronione jest udzielanie wszelkich informacji zawierających dane osobowe osobom, których tożsamości nie można zweryfikować. Weryfikacja tożsamości może odbywać się poprzez żądanie okazania dokumentu tożsamości lub innego dokumentu zawierającego zdjęcie wnioskodawcy lub poprzez wykorzystanie informacji zawartej w dokumentacji medycznej, która jest znana jedynie wnioskodawcy. Do tego celu należy wykorzystać metodę pytań bezpośrednich, w których wnioskodawca udzieli poprawnych informacji w co najmniej dwóch zapytaniach.
11. W Praktyce niedopuszczalne jest przekazywania jakichkolwiek informacji zawierających dane osobowe podmiotom, instytucjom czy też organom, które nie mogą się wykazać prawidłową podstawą prawną dostępu do danych osobowych.
12. W przypadku konieczności wydania dokumentów zawierających dane osobowe (np. wynik badań, recepty itp.) należy każdorazowo weryfikować tożsamość odbierającego za pomocą mechanizmu, o którym mowa w ust.11 niniejszego artykułu, a w przypadku, kiedy odbierającym nie jest adresat dokumentu należy zażądać upoważnienia.
13. Organizacja rejestracji i poczekalni podmiotu umożliwia zachowanie poufności osobom przebywającym bezpośrednio przy rejestracji.
14. Udzielanie świadczeń zdrowotnych w Praktyce odbywa się w miejscach specjalnie do tego wyznaczonych. Zabrania się udzielania informacji dotyczących pacjentów na korytarzach, w poczekalni lub innych nieprzystosowanych do tego miejscach w podmiocie leczniczym.
15. Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, parapetach itp.
16. 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/ danego pacjenta. Stosowana jest zasada tzw. czystego biurka.
17. Nie należy gromadzić w podręcznej dokumentacji danych osobowych. Wszystkie dane niezbędne do prawidłowej pracy powinny znajdować się w zbiorach, zgodnie z załącznikiem nr 1 do dokumentacji.
18. Dokumenty zawierające dane osobowe należy niszczyć w niszczarkach lub w przypadku dużej ilości dokumentów, korzystać w tym celu z usług profesjonalnych podmiotów, zajmujących się utylizacją dokumentacji.
19. Wobec osób, których dane są przetwarzane wykonuje się obowiązek informacyjny, zgodnie z art. 12-14 RODO, a wzór klauzul informacyjnych znajduje się w załączniku nr 7.
20. Obowiązek informacyjny wobec pacjentów może być wykonywany poprzez umieszczenie na tablicy informacyjnej przy okienku rejestracyjnym i w poczekalni stosownych tablic. W przypadku posiadania strony internetowej podmiot leczniczy zamieszcza również klauzule informacyjne na stronie internetowej.
21. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
22. Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza obszary przetwarzania lub przesyłane pocztą elektroniczną, należy zabezpieczyć poprzez nadanie im haseł odczytu.
23. Zbiory osobowe przetwarzane elektronicznie należy zabezpieczać poprzez wykonywanie kopii bezpieczeństwa, zapisywanych na zewnętrznych nośnikach i przechowywanych pod zamknięciem.
24. Komputery, które przetwarzają zbiory osobowe wyszczególnione w załączniku nr 1 do dokumentacji, za wyjątkiem komputerów służących jedynie do edycji tekstu, należy wyposażyć w urządzenia podtrzymujące napięcie na wypadek braku zasilania.
25. Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczać stosując wytyczne zawarte w Instrukcji zarządzania systemem informatycznym.
26. W celu zapewnienia danych przetwarzanych elektronicznie należy zapewnić logowanie do systemu operacyjnego (np. WINDOWS) oraz bezpośrednio do programów przetwarzających dane.
27. Z wszystkimi współpracującymi podmiotami gospodarczymi podpisano, na mocy art. 28 RODO, umowy powierzenia przetwarzania danych osobowych lub w umowach podstawowych wprowadzono uregulowania odnoszące się do obowiązków zapewnienia przestrzegania przepisów RODO przez te podmioty. W podmiocie leczniczym prowadzona jest ewidencja podmiotów, z którymi podpisano umowy powierzenia, której wzór stanowi załącznik nr 11.
28. Szczegółowe zasady postępowania ze zbiorami przetwarzanymi elektronicznie określa Instrukcja zarządzania systemem informatycznym.

**§11 Udostępnianie danych**

1. Podmiot udostępnia dane osobowe jedynie na podstawie obowiązujących przepisów prawa i w granicach prawa.
2. 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.
3. Ewidencja udostępnionej dokumentacji medycznej prowadzona jest na podstawie art. 27 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta i zawiera, co najmniej: imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna, sposób udostępnienia dokumentacji medycznej;, zakres udostępnionej dokumentacji medycznej, imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna, a w przypadkach, o których mowa wart. 26 *udostępnianie dokumentacji medycznej* ust. 3 i 4, także nazwę uprawnionego organu lub podmiotu, imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną, datę udostępnienia dokumentacji medycznej, podpis przyjmującego dokumentację medyczną.
4. Wzór ewidencji, o której mowa w ustępie 3 niniejszego paragrafu stanowi załącznik nr 10.
5. Praktyka udostępnia również dane, na podstawie innych przepisów prawa niż te, o których mowa w ustępie 2 niniejszego paragrafu jedynie na pisemny wniosek i za potwierdzeniem.
6. Podmiot przekazując dane drogą pocztową przekazuje je listem poleconym za potwierdzeniem odbioru.
7. W przypadku udostępniania dokumentów za pomocą korespondencji mailowej podmiot ma obowiązek szyfrować przekazywane pliku.

**§12 Administrator systemu informatycznego**

1. Dla celów obsługi i zabezpieczenia systemu informatycznego Administrator danych może powołać Administratora systemu informatycznego i wyznaczyć mu mi.in. następujący zakres zadań:
2. prowadzenie monitoringu przetwarzania danych,
3. administrowanie systemem informatycznym,
4. nadawanie uprawnień użytkownikom do systemu informatycznego,
5. stosowanie środków ochrony w ramach oprogramowania użytkowego, systemów operacyjnych, urządzeń teletransmisyjnych, programów antywirusowych oraz ochrony sprzętowej,
6. kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych,
7. kontrola systemu antywirusowego,
8. kontrola awaryjnego zasilania komputerów,
9. kontrola i wykonywanie kopii awaryjnych,
10. konserwacja oraz uaktualnienia systemów informatycznych,
11. informowanie na bieżąco ADO o przypadkach awarii programowych wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem, nie przestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystywania sprzętu komputerowego,
12. przedstawianie Administratorowi danych, nie rzadziej niż raz na rok, kompleksowej analizy przetwarzania danych osobowych w systemem informatycznym oraz ewentualne potrzeby w zakresie zabezpieczeń.
13. W przypadku, kiedy ADO nie powołuje ASI wszystkie zapisy w dokumentacji, które odwołują się do ASI są rozumiane jako zapisy dot. ADO.

**§12 Inspektor Ochrony Danych Osobowych**

1. Z uwagi na fakt, że głównym obszarem działalności podmiotu leczniczego jest przetwarzanie danych, o których mowa w art. 9 ust. 1 w podmiocie wyznaczony zostanie Inspektor Ochrony Danych Osobowych.
2. Za wyznaczenie Inspektora Ochrony Danych Osobowych w Praktyce odpowiada Administrator danych osobowych.
3. Inspektorem Ochrony Danych Osobowych w podmiocie może być jedynie osoba, która posiada fachową wiedzę na temat prawa i praktyki w ochronie danych osobowych oraz w sektorze ochrony zdrowia.
4. Inspektor Danych Osobowych nie musi być pracownikiem podmiotu leczniczego.
5. Administrator jest zobowiązany do udostępnienia danych kontaktowych Inspektora Danych Osobowych w sposób umożliwiający jego identyfikację i kontakt oraz jest zobowiązany powiadomić o nich organ nadzorczy.
6. Poprzez udostępnienie danych Inspektora Ochrony Danych Osobowych należy rozumieć, co najmniej ich publikację na stronie internetowej administratora oraz w widocznym miejscu, w siedzibie administratora.
7. Administrator ma obowiązek zapewnić Inspektorowi Ochrony Danych możliwość wykonywania jego obowiązków w sposób niezależny i zapewnić mu status, o którym mowa w art. 38 RODO.
8. Zadania Inspektora Ochrony Danych Osobowych:
9. informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i innych przepisów regulujących tą materię,
10. monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów,
11. podejmowanie działań zwiększających świadomość personelu Praktyki, inicjowanie i organizowanie szkoleń personelu uczestniczącego w operacjach przetwarzania,
12. przeprowadzanie wewnętrznych audytów,
13. udzielanie na żądanie administratora zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z rozdziałem II niniejszego dokumentu,
14. współpraca z organem nadzorczym,
15. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
16. Inspektor Ochrony Danych Osobowych jest wyznaczony na podstawie stosowanego zarządzenia administratora.
17. Dane kontaktowe Inspektora Ochrony Danych Osobowych są przekazywane organowi nadzorczemu według trybu i za pomocą narzędzi opracowanych i wdrożonych przez organ nadzorczy.

**§13 Zarządzanie ryzykiem w Praktyce/NZOZ**

1. W podmiocie przeprowadzana jest analiza ryzyka. Analiza ryzyka może odbywać się dla wszystkich wyodrębnionych zbiorów danych osobowych lub dla procesów 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, nie później niż do dnia 31 marca dla wszystkich czynności przetwarzania lub w przypadku wprowadzenia nowych procedur lub rozwiązań organizacyjnych w podmiocie leczniczym, zgodnie z odrębną procedurą przyjętą przez Praktykę.

**§13 Ocena skutków dla ochrony danych osobowych**

1. Dla zbiorów danych osobowych, w których znajdują się dane osobowe, 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:
3. opisie planowanych operacji i celów przetwarzania,
4. opisie i ocenie przez administratora czy planowane operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów,
5. ocenie ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
6. opisie środków planowanych w celu zaradzenia ryzykiem, w tym określeniu mechanizmów, zabezpieczeń i środków technicznych, mających zapewnić bezpieczeństwo procesu,
7. Ocena skutków dla ochrony danych odbywa się odrębną procedurą przyjętą przez Praktykę.
8. Za zarządzania ryzykiem oraz ocenę skutków dla ochrony danych osobowych odpowiada Administrator danych osobowych.
9. Analiza ryzyka i ocena skutków dla systemu ochrony danych może odbywać się przy udziale Inspektora Ochrony Danych Osobowych.
10. Wyznaczony pracownik ma obowiązek sporządzenia corocznego raportu związanego z ryzykiem w podmiocie leczniczym nie później niż do 30 kwietnia.

**§14 Zasady postępowania w przypadku naruszenia 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 Praktyce.
2. Powiadomienie to może mieć charakter ustny lub pisemny.
3. Adresatem takiego powiadomienia jest Inspektor Ochrony Danych Osobowych.
4. Po otrzymaniu takiego powiadomienia Inspektor Ochrony Danych Osobowych podejmuje niezwłocznie czynności w celu ustalenia stanu faktycznego.
5. W przypadku uzasadnionego podejrzenia wystąpienia incydentu lub naruszenia systemu ochrony danych osobowych podejmuje działania mające zapobiec dalszym skutkom oraz powiadamia administratora.
6. Po dokonaniu czynności zabezpieczających, Inspektor Ochrony Danych Osobowych, ma za zadanie przeprowadzić postępowanie wyjaśniające, które:
7. ustali ostateczny zakres, przyczyny wystąpienia oraz skutki, zarówno dla Praktyki, jak i osób, których dane dotyczyły,
8. podejmuje niezbędne czynności mające na celu przywrócenie prawidłowości działania systemu ochrony danych osobowych w podmiocie,
9. opracowuje działania naprawcze i zapobiegawcze, których zadaniem jest wyeliminowanie niepożądanych zdarzeń w przyszłości,
10. wskazuje osoby odpowiedzialne za wystąpienie sytuacji.
11. Powyższe czynności są dokumentowane przez Inspektora Ochrony Danych Osobowych za pomocą formularza, którego wzór stanowi załącznik nr 12.
12. Rejestr formularzy, o których mowa w punkcie 7 niniejszego rozdziału prowadzi administrator.
13. 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.

**§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 13.
10. Administrator może zlecić badanie audytowe niezależnemu podmiotowi, po poinformowaniu o tym fakcie Inspektora Ochrony Danych Osobowych.

**§16 Środki techniczne ochrony danych osobowych**

*Z poniżej wymienionych środków wybrać właściwe, wpisać poniżej i usunąć z treści dokumentu:*

***Ogólna ochrona budynku*** *– alarm antywłamaniowy, monitoring wizyjny, całodobowy dozór służb ochrony, gaśnice lub systemy ppoż.*

***Zabezpieczenia okien*** *– pomieszczenia zlokalizowane na parterze lub wyższych kondygnacjach można dodatkowo zabezpieczyć poprzez montaż krat, rolet lub szyb antywłamaniowych, zwłaszcza, jeśli istnieje do nich dostęp przez tarasy, dachy niższych budynków, drabiny ppoż. itp.*

***Zabezpieczenie drzwi*** *– w zależności od kategorii danych i zagrożeń można stosować drzwi tradycyjne zamykane na klucz lub przeciwpożarowe, zaś w miejscach szczególnie narażonych na zagrożenia (drzwi wejściowe, sekretariaty, księgowość, archiwa, itp.) należy stosować drzwi antywłamaniowe.*

***Zabezpieczenia zbiorów tradycyjnych (papierowych)*** *– w zależności od kategorii danych i zagrożeń do przechowywania danych można stosować szafy tradycyjne zamykane na klucz, szafy metalowe lub sejfy (dla danych szczególnie ważnych). Dane przeznaczone do zniszczenia należy niszczyć w specjalistycznych niszczarkach.*

***Zabezpieczenia zbiorów elektronicznych*** *– dane elektroniczne należy zabezpieczyć poprzez wyposażenie komputerów w zasilacze awaryjne podtrzymujące napięcie na wypadek braku zasilania oraz w systemy antywirusowe. Kopie danych należy gromadzić w szafach metalowych lub sejfach ognioodpornych.*

1. Praktyka posiada następujący ogólny system zabezpieczeń:
2. *Np. alarm antywłamaniowy itd.*
3. .........................
4. ………………….
5. W tabeli załącznika nr 2 opisano dla każdego pomieszczenia indywidualnie, stosowane środki bezpieczeństwa.
6. Każdy komputer przetwarzający dane osobowe zabezpieczono w zasilacz awaryjny podtrzymujący napięcie na wypadek braku zasilania oraz w system antywirusowy. Szczegółowe środki ochrony technicznej komputerów z podziałem na miejsca przetwarzania zamieszczono w załączniku nr 2 do niniejszej dokumentacji.
7. Dodatkowe, środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określono w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

## Załącznik nr 1. Wykaz zbiorów danych osobowych przetwarzanych w …………

## Załącznik nr 2. Wykaz miejsc przetwarzania zbiorów danych osobowych w …………….

## Załącznik nr 3. Ewidencja osób upoważnionych do przetwarzania danych osobowych w …………..

## Załącznik nr 4. Wzór upoważnienia do przetwarzania danych osobowych.

## Załącznik nr 5. Wzór unieważnienia upoważnienia do przetwarzania danych osobowych.

## Załącznik nr 6. Wzór potwierdzenia znajomości zasad bezpieczeństwa.

## Załącznik nr 7 Wzór realizacji obowiązku informacyjnego.

## Załącznik nr 8. Wzór zgody.

## Załącznik nr 9. Wzór rejestru czynności przetwarzania.

## Załącznik nr 10. Wzór ewidencji udostępnianej dokumentacji medycznej.

## Załącznik nr 11. Wzór ewidencji podmiotów, którym powierzono przetwarzanie danych osobowych.

## Załącznik nr 12. Wzór raportu z incydentów.

## Załącznik nr 13. Wzór raportu pokontrolnego.

**Załącznik nr 1. Wykaz zbiorów danych osobowych.**

**WYKAZ ZBIORÓW DANYCH OSOBOWYCH**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **LP.** | **NAZWA ZBIORU** | **RODZAJ POMIESZCZENIA** | **PIĘTRO** | **NR POMIESZCZENIA** | **MIEJSCE SKŁADOWANIA DANYCH** | **OPIS STRUKTURY DANYCH (zbierane dane)** | **SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI** |
|  |  |  |  |  |  |  | *(jeżeli dane przetwarzane są w systemach komputerowych, inaczej nie dotyczy)* |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Załącznik nr 2. Wykaz miejsc przetwarzania zbiorów danych osobowych.**

|  |
| --- |
| **WYKAZ MIEJSC PRZETWARZANIA ZBIORÓW DANYCH OSOBOWYCH** |
| Budynek |  |
|  |
| 1. **ZABEZPIECZENIA BUDYNKU**
 |
|  |
| 1. **PROCEDURA AWARYJNEGO DOSTĘPU**
 |
|  |
| 1. **WYKAZ POMIESZCZEŃ**
 |
| **Piętro** | **Nr pom** | **Rodzaj pomieszczenia** | **Zastosowane w pomieszczeniu środki bezpieczeństwa** | **Miejsce składowania danych**  |
| **1** | **2** | **3** | **4** | **5** |
|  |  | *Np. gabinet lekarski, pracownia diagnostyczna, recepcja, pokój zabiegowy* | *Np. System: alarmowy, przeciwpożarowy, rolety antywłamaniowe, drzwi kodowane, antywłamaniowe, zamykane na klucz* | *Np. szafa zamykana na klucz, szuflada, komputer, laptop, urządzenia medyczne (np. usg).* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Załącznik nr 3. Ewidencja osób upoważnionych do przetwarzania danych osobowych.**

|  |
| --- |
| **EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH** |
| **LP.** | **NAZWISKO I IMIĘ** | **STANOWISKO** | **ZBIORY DANYCH, DO KTÓRYCH UŻYTKOWNIK MA DOSTĘP** | **DATA NADANIA UPOWAŻNIENIA** | **DATA USTANIA UPOWAŻNIENIA** | **LOGIN** |
| I | II | III | IV | V | VI | VII |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Załącznik nr 4. Wzór upoważnienia do przetwarzania danych osobowych.**

……………..……………………., dn. …………………………….

…………………………………………….

 (sygnatura)

**UPOWAŻNIENIE**

W związku z art. 29 rozporządzenia z dnia 27 kwietnia 2016 r. w sprawie ochrony danych osobowych upoważniam Panią/Pana:

…………………………………………………..

(imię i nazwisko)

……………………………………………………

(nr PESEL)

do przetwarzania, w ramach wykonywanych obowiązków służbowych, następujących zbiorów danych osobowych:

|  |  |
| --- | --- |
| **Nr zbiorów z ewidencji zbiorów** | **Nazwa programu / identyfikator** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Upoważnienie obowiązuje od……………………………do…………………………………………..

…………………………………..…………………………………………………..

(data i podpis Administratora danych osobowych)

## Załącznik nr 5. Wzór unieważnienia upoważnienia do przetwarzania danych osobowych.

……………..……………………., dn. …………………………….

…………………………………………….

 (sygnatura)

**UNIEWAŻNIENIE**

W związku z art. 29 rozporządzenia z dnia 27 kwietnia 2016 r. w sprawie ochrony danych osobowych unieważniam upoważnienie

z dnia …………………………………….….., o sygnaturze ……………………………………….,

dla Pani/Pana:

…………………………………………………..

(imię i nazwisko)

…………………………………………………

(nr PESEL)

…………………………………..…………………………………………………..

 ( data i podpis Administratora danych)

## Załącznik nr 6. Wzór potwierdzenia znajomości zasad bezpieczeństwa.

……………………., dn. …………………………….

…………………………………………….

(imię i nazwisko pracownika)

**OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI**

1. Oświadczam, że zapoznano mnie z przepisami w zakresie ochrony danych osobowych, wynikających z Rozporządzania 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) oraz innymi aktami prawnymi i branżowymi regulującymi zasady postępowania w tym zakresie oraz wszystkimi dokumentami wewnętrznymi organizującymi proces zarządzania danymi osobowymi w ……………………....
2. Zobowiązuję się do:
3. stosowania określonych przez ADO zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne w stosunku do celu przetwarzanie danych,
4. przetwarzania powierzonych mi danych jedynie w zakresie udzielonego upoważnienia,
5. należytego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nie upoważnionym,
6. zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony osób, których dane dotyczą,
7. Zgłaszania wszelkich incydentów, zagrożeń, potencjalnych naruszeń systemu ochrony danych osobowych w podmiocie leczniczym,
8. zachowania w tajemnicy danych oraz ich sposobu zabezpieczeń, nawet po ustaniu stosunku pracy.
9. W zakresie systemu informatycznego zobowiązuję się:
10. nie ujawniać danych zawartych w eksploatowanych systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
11. nie ujawniać szczegółów technologicznych w używanych systemach oraz oprogramowaniu,
12. nie udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
13. nie kopiować lub nie przetwarzać danych w sposób inny niż dopuszczony obowiązującą Polityką Bezpieczeństwa.

Przyjmuję jednocześnie do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami będą traktowane jako ciężkie naruszenie moich obowiązków wobec Praktyki i może rodzić sankcje karne i finansowe, wynikające z przepisów prawa, w tym mogą stanowić podstawę dochodzenia odszkodowań w trybie cywilno-prawnym.

…………………………………………… …………………………………………

 (podpis pracownika) (podpis przełożonego)

## Załącznik nr 7. Wzór klauzuli informacyjnej.

**WZÓR KLAUZULI INFORMACYJNEJ**

***(przy zbieraniu danych od osób, których one dotyczą):***

***………………………… ……………………………***

***(pieczęć nagłówkowa) (data i miejsce)***

Zgodnie z art. 13 ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. o ochronie danych osobowych informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest (Nazwa Administratora) z siedzibą w (Adres Administratora), którego reprezentuje (Imię i nazwisko, funkcja),
2. Inspektorem Danych Osobowych jest ……………………………..(imię i nazwisko) kontakt z Inspektorem Ochrony Danych w (Nazwa Administratora) możliwy jest pod numerem tel. nr. ……………. lub adresem email (adres email),
3. Pani/Pana dane osobowe przetwarzane będą w celu…………………. na podstawie art…………….. ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.,
4. odbiorcami Pana/Pani danych osobowych będą (podać nazwę odbiorców lub kategorię odbiorców),
5. Pana/Pani dane osobowe przechowywane będą w okresie niezbędnym do realizacji celów przetwarzania tj……………………….
6. posiada Pani/ Pan prawo do: żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych – *należy rozstrzygnąć czy nie ma konieczności ograniczeń uprawnień wynikających z innych przepisów prawa*,
7. istnieje możliwość wniesienia skargi do organu nadzorczego na tryb i sposób przetwarzania danych osobowych przez administratora, jeśli uzna Pani/ Pan za uzasadnione, że Pani/ Pana dane osobowe są przetwarzane niezgodnie z Rozporządzeniem o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
8. podanie danych osobowych jest obligatoryjne i wynika z mocy przepisu prawa tj. ustawy o działalności leczniczej i ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, a brak podania danych osobowych będzie skutkował możliwością odstąpienia od udzielenia świadczeń, chyba, że inne przepisy stanowią inaczej,
9. administrator nie będzie przekazywał Pani/ Pana danych osobowych odbiorcom w państwach trzecich oraz organizacjom międzynarodowym – *opcjonalne,*
10. administrator nie podejmuje czynności związanych ze zautomatyzowanym podejmowaniem decyzji wobec danych osobowych, w tym o profilowaniu - *opcjonalne*

***(Dla danych pozyskanych z innych źródeł):***

***…………………………. …………………………***

***(pieczęć nagłówkowa) (data i miejsce)***

Zgodnie z art. 14 ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. o ochronie danych osobowych informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest (Nazwa Administratora) z siedzibą w (Adres Administratora), którego reprezentuje (Imię i nazwisko, funkcja),
2. Inspektorem Danych Osobowych jest ……………………………..(imię i nazwisko) kontakt z Inspektorem Ochrony Danych w (Nazwa Administratora) możliwy jest pod numerem tel. nr. ……………. lub adresem email (adres email),
3. Pani/Pana dane osobowe przetwarzane będą w celu…………………. na podstawie art…………….. ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.,
4. zakres danych, które zostały pozyskane to: …………………………..
5. Pani/ Pana dane pozyskano z ………………………(nazwa źródła),
6. Pana/Pani dane osobowe przechowywane będą w okresie niezbędnym do realizacji celów przetwarzania tj……………………….
7. posiada Pani/ Pan prawo do: żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych – *należy rozstrzygnąć, czy nie ma konieczności ograniczeń uprawnień wynikających z innych przepisów prawa,*
8. istnieje możliwość wniesienia skargi do organu nadzorczego na tryb i sposób przetwarzania danych osobowych przez administratora, jeśli uzna Pani/ Pan za uzasadnione, że Pani/ Pana dane osobowe są przetwarzane niezgodnie z Rozporządzeniem o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
9. odbiorcami Pana/Pani danych osobowych będą (podać nazwę odbiorców lub kategorię odbiorców),
10. administrator nie będzie przekazywał Pani/ Pana danych osobowych odbiorcom w państwach trzecich oraz organizacjom międzynarodowym – *opcjonalne,*
11. administrator nie podejmuje czynności związanych ze zautomatyzowanym podejmowaniem decyzji wobec danych osobowych, w tym o profilowaniu - *opcjonalne*

## Załącznik nr 8. Wzór zgody na przetwarzanie danych osobowych.

………………………………………………………..

*(miejscowość, data)*

**FORMULARZ ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH**

Ja niżej podpisana/ podpisany oświadczam, że wyrażam zgodę na przetwarzanie moich danych osobowych przez …………… *(wpisać nazwę administratora*) do celów:

1. Marketingowych związanych z udzielaniem świadczeń zdrowotnych przez…………………………\*
2. Udziału w badaniu klinicznym prowadzonym przez …………………………..w zakresie…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………..\*
3. …………………………………………………………………………………………………………………………………\*

\*niepotrzebne skreślić

………………………………………..

 (czytelny podpis)

*Dotyczy dziecka:*

Ja niżej podpisana/ podpisany oświadczam, że jestem rodzicem/ opiekunem prawnym mojego dziecka………………………………………….(*imię i nazwisko dziecka*) ………………………………..(*PESEL dziecka*) i wyrażam zgodę na przetwarzanie danych osobowych mojego dziecka przez ………………………..(*wpisać nazwę administratora*), do celów:

1. Marketingowych związanych z udzielaniem świadczeń zdrowotnych przez…………………………………………….\*
2. Udziału w badaniu klinicznym prowadzonym przez …………………………..w zakresie…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………..\*
3. …………………………………………………………………………………………………………………………………\*

\*niepotrzebne skreślić

………………………………………..

 (czytelny podpis rodzica/ opiekuna prawnego)

## Załącznik nr 9. Wzór rejestru czynności przetwarzania.

**REJESTR CZYNNOŚCI PRZETAWARZANIA**

*Rejestr prowadzony w oparciu o art. 30 ust. 1 przepisów Rozporządzenia PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych*

|  |  |
| --- | --- |
| **Imię i nazwisko/ nazwa oraz dane kontaktowe administratora oraz wszelkich współadministratorów oraz w odpowiednich przypadkach przedstawiciela administratora** |  |
| **Imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych Osobowych** |  |

|  |  |
| --- | --- |
| **Nazwa czynności przetwarzania** |  |
| **Cele przetwarzania** |  |
| **Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych** |  |
| **Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych** |  |
| **Nazwa państwa trzeciego lub organizacji międzynarodowej, którym przekazywane są dane osobowe, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń** |  |
| **planowane terminy usunięcia poszczególnych kategorii danych** |  |
| **ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO** |  |

Rejestr czynności przetwarzania ma formę pisemną, w tym formę elektroniczną.

## Załącznik nr 10. Wzór ewidencji udostępnianej dokumentacji medycznej.

**EWIDENCJA UDOSTĘPNIANEJ DOKUMENTACJI MEDYCZNEJ W TRYBIE ART. 26 I 27 USTAWY O PRAWACH PACJENTA I RZECZNIKU PRAW PACJENTA**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Imię i nazwisko pacjenta, którego dotyczy wniosek** | **Imię i nazwisko osoby/ podmiotu, któremu została udostępniona dokumentacja medyczna** | **Sposób udostępnienia** | **Zakres udostępnienia** | **Data udostępnienia** | **Imię i nazwisko osoby przekazującej dokumentację medyczną** | **Podpis osoby przekazującej dokumentację medyczną** | **Podpis osoby przyjmującej dokumentację medyczną** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

## Załącznik nr 11. Wzór ewidencji podmiotów, którym powierzono przetwarzanie danych osobowych.

**EWIDENCJA PODMIOTÓW, KTÓRYM POWIERZONO PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ ……………………**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **L.p.** | **Nazwa podmiotu, adres, telefon** | **Imię i nazwisko, dane kontaktowe osoby upoważnionej do współpracy w tym zakresie** | **Data podpisania umowy powierzenia** | **Przedmiot umowy** | **Data zakończenia współpracy** | **Przyczyna****zakończenia współpracy** | **Informacja o rodzajach zbiorów, które obejmuje umowa** | **Podpis Inspektora Ochrony Danych** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

## Załącznik nr 12. Wzór raportu z incydentów.

**RAPORT Z INCYDENTÓW/ NARUSZEŃ**

|  |  |
| --- | --- |
| **Data i godzina wystąpienia**  |  |
| **Osoba zgłaszająca** |  |
| **Opis**  |  |
| **Zakres incydentu**  |  |
| **Określenie skutków** |  |
| **Określenie czy prawa i wolności osób fizycznych zostały lub mogą zostać naruszone w wyniku incydentu** |  |
| **Podjęte czynności na rzecz przywrócenia działania systemu ochrony danych osobowych** |  |
| **Wdrożenie działań naprawczych** |  |
| **Wskazanie osób odpowiedzialnych** |  |
| **Konieczność powiadomienia organów** |  |
| **Wykaz załączników do raportu** |  |
| **Data sporządzenia raportu** |  |

 ………………………………………………………….

  *(data i podpis sporządzającego)*

## Załącznik nr 13. Wzór raportu pokontrolnego.

**RAPORT POKONTROLNY**

|  |  |
| --- | --- |
| 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 |  |

Załączniki:

………………………………………………………………………..

 ……………………………………………

 *(podpis i pieczęć kontrolującego)*