UCHWAŁA ZARZĄDU REVIT SP. Z O.O. Z SIEDZIBĄ W BIAŁYMSTOKU NR 2/08/2025
z dnia [18.08.2025r.]

w sprawie wprowadzenia Polityki bezpieczeństwa

Na podstawie art. 24 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) oraz w związku z koniecznością zapewnienia zgodności przetwarzania danych osobowych w REVIT sp. z o.o. z siedzibą w Białymstoku z przepisami o ochronie danych osobowych, zarządzam, co następuje:

§ 1

Zarząd przyjmuje i wprowadza do stosowania Politykę Bezpieczeństwa w brzmieniu stanowiącym załącznik do niniejszej uchwały, z dniem 1 września 2025r. Polityka Bezpieczeństwa stanowi aktualizację oraz formalizację dotychczas obowiązujących zasad bezpieczeństwa, w tym ochrony danych osobowych w REVIT sp. z o.o., ul. Swobodna 38, 15-756 Białystok.

§ 2

Polityka Bezpieczeństwa stanowi wewnętrzny dokument określający:

1. zasady przetwarzania danych osobowych w placówce,
2. obowiązki pracowników i osób współpracujących w zakresie ochrony danych,
3. środki organizacyjne i techniczne mające na celu zabezpieczenie danych osobowych,
4. zakres odpowiedzialności osób przetwarzających dane osobowe.

§ 3

Wszyscy pracownicy oraz współpracownicy zobowiązani są do:

1. zapoznania się z treścią Polityki Bezpieczeństwa,
2. przestrzegania jej postanowień,
3. potwierdzenia zapoznania się z dokumentem poprzez podpisanie stosownego oświadczenia.

§ 4

Nadzór nad przestrzeganiem Polityki Bezpieczeństwa sprawuje Członek Zarządu Damian Raczkowski /osoba wyznaczona przez Zarząd.

§ 5

Wykonanie uchwały powierza się zarządowi.

§ 6

Uchwała wchodzi w życie z dniem podpisania.

załącznik do uchwały zarządu Revit sp. z o.o. z siedzibą w Białymstoku nr 2/08/2025 z dnia 18.08.2025r.
w sprawie wprowadzenia Polityki bezpieczeństwa

POLITYKA BEZPIECZEŃSTWA

Oznaczenie administratora danych i adres jego siedziby

Administrator:	REVIT sp. z o.o. z siedzibą w Białymstoku
siedziba:	Swobodna 38/8, 15-756 Białystok

zgodnie z:

Art 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679z 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)

Administrator Ochrony Danych, reprezentowany przez:

[Damian Raczkowski]

wprowadza dokument o nazwie: Polityka Bezpieczeństwa.

Niniejsza Polityka Bezpieczeństwa, zwana dalej także Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w organizacji, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).

SPIS TREŚCI

I. Podstawa prawna Polityki

Niniejsza Polityka została opracowana w szczególności w oparciu o przepisy:

- 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)
- ustawy o ochronie danych osobowych 24 maja z 2018 r. (Dz.U. 2018 poz. 1000 z późn. zm.)
- ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2024 r. poz. 581);
- ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (t.j. Dz. U. z 2025 r. poz. 450 z późn. zm.);
- ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz. U. z 2025 r. poz. 302 z późn. zm.);
- ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t.j. Dz. U. z 2024 r. poz. 146 z późn. zm.).
- Kodeksu postępowania dla sektora ochrony zdrowia wydany zgodnie z art. 40 RODO dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających;

II. Cele Polityki

Celem Polityki jest uaktualnienie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w jednostce, a w szczególności:

1) zapewnienie spełnienia wymagań prawnych;
2) zapewnienie poufności, integralności oraz rozliczalności danych osobowych przetwarzanych w jednostce;
3) podnoszenie świadomości osób przetwarzających dane osobowe;
4) zaangażowanie osób przetwarzających dane osobowe firmy w ich ochronę.

III. Wykaz podstawowych skrótów

Skrót	Opis
RODO	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)
ADO lub Administrator	Administrator Danych Osobowych
IOD	Inspektor Ochrony Danych Osobowych

IV. Definicje podstawowych pojęć

Ilekroć w niniejszej Polityce Ochrony Danych mowa o:

- Administratorze Danych Osobowych – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych – REVIT sp. z o.o. z siedzibą w Białymstoku;
- pracowniku – osobach zatrudnionych przez Administratora na podstawie umowie o pracę lub umowie cywilno-prawnej, nie prowadzących działalności gospodarczej, także osoba odbywająca wolontariat, praktykę lub staż;
- współpracowniku – osobach zatrudnionych przez Administratora na podstawie umów cywilno-prawnych, prowadzących działalność gospodarczą;
- osobie upoważnionej – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Osobą upoważnioną może być pracownik, współpracownik lub inna osoba wykonująca prace na podstawie umowy zlecenia lub innej umowy cywilno-prawnej (w tym B2B);
- danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);

- możliwej do zidentyfikowania osobie fizycznej - rozumie się przez to osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- przetwarzaniu danych osobowych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- zbiorze danych osobowych – rozumie się przez to uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- podmiocie przetwarzającym – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych;
- odbiorcy danych - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
- systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
- bezpieczeństwie danych osobowych – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania danych osobowych, by w każdych okolicznościach dostęp do nich był zgodny z założeniami i zapewniał ich poufność, integralność oraz dostępność;
- poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;
- integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- dostępności danych – rozumie się przez to właściwość zapewniającą, że dane są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez uprawnioną osobę lub podmiot;
- państwie trzecim – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
- incydencie – rozumie się przez to zdarzenie zagrażające bezpieczeństwu danych osobowych;
- zagrożeniu - rozumie się przez to potencjalną możliwość wystąpienia incydentu;
- naruszeniu ochrony danych osobowych - rozumie się przez to naruszenie bezpieczeństwa danych osobowych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

V. Postanowienia ogólne

1. Polityka określa reguły przetwarzania danych osobowych oraz sposobów ich zabezpieczenia, jako zestaw praw, zasad i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w jednostce.
2. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.
3. Niniejszy dokument jest zgodny z obowiązującymi przepisami prawa, a w szczególności z Rozporządzeniem 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.
4. Polityka dotyczy wszystkich danych osobowych przetwarzanych w jednostce, niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
5. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
6. Polityka jest udostępniana do wglądu pracownikom i współpracownikom, w szczególności osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
7. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
    - odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
    - kontrolę i nadzór nad przetwarzaniem danych osobowych,
    - monitorowanie zastosowanych środków ochrony.
8. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
9. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.
10. Administrator wdraża środki ochrony danych już na etapie projektowania (privacy by design) oraz zapewnia, by domyślnie przetwarzano tylko te dane, które są niezbędne do realizacji celu (privacy by default), zgodnie z art. 25 RODO.

VI. Zakres rozpowszechniania Polityki

Procedury i zasady określone w niniejszym dokumencie powinny być znane i są stosowane przez wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych i tradycyjnych jednostki, bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy – w tym pracowników i współpracowników.

VII. Dane osobowe przetwarzane przez Administratora Ochrony Danych

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych oraz są ujęte w Rejestrze Czynności Przetwarzania (RCP), który zawiera mapowanie czynności przetwarzania oraz odpowiadające im kategorie zakresów danych.
2. Administrator danych nie podejmuje czynności przetwarzania, które, jak wynika z analizy ryzyka, mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony

danych w fazie ich projektowania (privacy by design/default); odpowiednie informacje o nowych czynnościach i ich podstawach są ujmowane w RCP.

4. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru stanowi załącznik nr 1 do niniejszej Polityki, a RCP określony jest w odrębnym dokumencie wewnętrznym i prowadzony w formie elektronicznej.

VIII. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszyscy pracownicy i współpracownicy zobowiązani są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Osobowych Polityką, a także innymi dokumentami wewnętrznymi i procedurami związanymi z przetwarzaniem danych osobowych w jednostce.
2. Każdy pracownik i współpracownik mający wpływ na nowe czynności przetwarzania wdraża je biorąc pod uwagę ochronę danych osobowych i zapewnia, by domyślnie przetwarzano tylko te dane, które są niezbędne do realizacji celu.
3. Wszystkie dane osobowe w jednostce są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
    a. w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych.
    b. dane są przetwarzane rzetelnie i w sposób przejrzysty.
    c. dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarzane dalej w sposób niezgodny z tymi celami.
    d. dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych.
    e. dane osobowe są prawidłowe i w razie potrzeby uaktualniane.
    f. czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane.
    g. wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.
    h. dane są zabezpieczone przed naruszeniami zasad ich ochrony.
4. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników należy dopilnowanie, by:
    a. pracownicy i współpracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,
    b. pracownicy i współpracownicy przetwarzający dane osobowe byli upoważnieni do przetwarzania danych osobowych, przy czym:
        i. osoby wykonujące zawód medyczny – z mocy prawa upoważnione są do przetwarzania danych osobowych co do czynności mieszczących się w ramach wykonywania zawodu medycznego, na podstawie przepisów prawa; Administrator może dodatkowo nadać im upoważnienie jako środek organizacyjny;
        ii. osoby wykonujące czynności pomocnicze oraz osoby utrzymujące systemy teleinformatyczne – na podstawie imiennego upoważnienia Administratora. zgodnie z „Upoważnieniem do przetwarzania danych osobowych” – wzór Upoważnienia stanowi Załącznik nr 2 do niniejszej Polityki,
    c. pracownicy i współpracownicy przetwarzający dane osobowe zobowiązali się do zachowania w tajemnicy danych osobowych oraz informacji, do których uzyskała dostęp w związku z wykonywaniem obowiązków. Wzór „Oświadczenia i zobowiązania osoby przetwarzającej dane osobowe do zachowania tajemnicy” stanowi załącznik nr 3 do Polityki;

    d. pracownicy i współpracownicy odbywali regularne szkolenia z zakresu zasad bezpieczeństwa, w tym ochrony danych osobowych.
5. Pracownicy i współpracownicy zobowiązani są do:
    a. ścisłego przestrzegania zakresu nadanego upoważnienia;
    b. przetwarzania i ochrony danych osobowych zgodnie z przepisami;
    c. zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    d. zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.
    e. korzystania wyłącznie z dostępów wynikających z nadanej roli oraz niepodejmowania czynności wykraczających poza zakres umowny/organizacyjny;
6. Zakres upoważnienia do przetwarzania danych może wynikać z postanowień umowy łączącej z Administratorem lub z przypisanej roli w systemie informatycznym; w każdym przypadku musi on być ograniczony do niezbędnego minimum i zgodny z zasadą minimalizacji.
7. Za organizację szkoleń z zasad bezpieczeństwa, w tym ochrony danych osobowych odpowiada Administrator Danych, który wyznacza koordynatora ds. ochrony danych. Do zadań koordynatora merytorycznego szkoleń należy przygotowanie programu, materiałów i harmonogramu szkoleń, konsultowanie treści z osobą odpowiedzialną za systemy informatyczne i IOD oraz weryfikacja realizacji obowiązków szkoleniowych.
8. Kierownicy komórek organizacyjnych odpowiadają za zapewnienie udziału podległych pracowników i współpracowników w szkoleniach w terminach wyznaczonych przez Administratora oraz za egzekwowanie stosowania zdobytej wiedzy w praktyce oraz współpracują przy identyfikacji potrzeb szkoleniowych właściwych dla danej komórki (np. rejestracja, dokumentacja medyczna, udostępnianie).
9. Osoba odpowiedzialna za systemy informatyczne (Administrator systemów/IT) realizuje i dokumentuje szkolenia techniczne z bezpieczeństwa (m.in. zarządzanie hasłami, phishing, szyfrowanie, praca zdalna, kopie zapasowe) oraz zapewnia, aby program szkoleń był spójny z aktualnymi zabezpieczeniami i regulacjami wewnętrznymi.
10. Szkolenia są obowiązkowe:
    a. przy zatrudnieniu lub nawiązaniu współpracy (szkolenie wstępne przed nadaniem uprawnień dostępowych),
    b. okresowo, nie rzadziej niż raz na 24 miesiące, oraz po istotnych zmianach przepisów, systemów lub po naruszeniu bezpieczeństwa.
11. Nadanie uprawnień do systemów informatycznych oraz dopuszczenie do przetwarzania danych jest możliwe wyłącznie po odbyciu szkolenia wstępnego i złożeniu oświadczeń, o których mowa w pkt 5 lit.c).
12. Administrator gromadzi upoważnienia do przetwarzania, oświadczenia i zobowiązania osoby przetwarzającej dane osobowe do zachowania tajemnicy w aktach osobowych lub odrębnej ewidencji.
13. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania w odniesieniu do personelu pomocniczego/IT oraz osób wykonujących zawód medyczny, gdy nadano im upoważnienia fakultatywne. Wzór ewidencji stanowi Załącznik nr 4 do niniejszej Polityki.
14. Upoważnienia do przetwarzania danych osobowych oraz odpowiadające im dostępy i role w systemach informatycznych podlegają okresowemu przeglądowi pod kątem adekwatności i aktualności. Przegląd przeprowadza się nie rzadziej niż raz na 12 miesięcy oraz każdorazowo po istotnych zmianach organizacyjnych (np. zmiana struktury działów), personalnych (np. zatrudnienie/rozstanie, zmiana stanowiska) lub po stwierdzonym istotnym incydencie bezpieczeństwa. Za przeprowadzenie przeglądu odpowiada osoba odpowiedzialna za systemy informatyczne

(Administrator systemów/IT), działająca we współpracy z Inspektorem Ochrony Danych.

IX. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.
3. Pracownicy i współpracownicy zobowiązani są do przestrzegania i stosowania wprowadzonych środków ochrony.
4. Środki ochrony stosowane przez administratora obejmują:
   a. w zakresie środków organizacyjnych:
      — ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej,
      — stosowanie tzw. polityki czystego biurka:
      i. obowiązkowego przechowywanie dokumentów w pomieszczeniach i szafach zamykanych na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych;
      ii. zamykania pomieszczeń tworzących obszar przetwarzania danych osobowych na czas nieobecności pracowników lub współpracowników, w sposób uniemożliwiający dostęp do nich osób trzecich,
      iii. wykorzystanie zamykanych szafek do zabezpieczenia dokumentów,
      iv. wykorzystania niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe,
      — stosowanie tzw. polityki czystego ekranu:
      i. indywidualne identyfikatory użytkowników oraz wymóg uwierzytelnienia przed dostępem do systemów, z zakazem współdzielenia kont i ponownym nieprzydzielaniem zwolnionych identyfikatorów innym osobom;
      ii. stosowania haseł do systemów z danymi,
      iii. blokowania ekranów po odejściu od stanowiska
      iv. niezwłocznego odbierania wydruków z drukarki;
   b. w zakresie środków technicznych:
      i. każdy komputer, na którym przetwarzane są dane osobowe posiada własne zasilanie bateryjne, zabezpieczające przed skokami napięcia i zanikiem zasilania;
      ii. stosowanie ochrony sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem,
      iii. system informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
      iv. wykonywanie kopii awaryjnych danych,
      v. wydzielenie sieci WIFI;
   c. w zakresie zarządzania dostępem i rozliczalności
      i. nadawanie i odbieranie uprawnień do systemów na podstawie wniosków i ról, zgodnie z zasadą niezbędnego dostępu; prowadzenie rejestru uprawnień oraz historii zmian; zakaz współdzielenia kont i ponownego przydzielania identyfikatorów po ustaniu uprawnień.

ii. stosowanie polityki haseł określającej długość, złożoność i rotację haseł oraz, gdzie adekwatne do ryzyka, uwierzytelniania wieloskładnikowego; obowiązkowe blokowanie ekranu po bezczynności.
iii. rejestrowanie zdarzeń w systemach (logi: identyfikator, czas, typ operacji, źródło) z ochroną integralności dzienników oraz okresowymi przeglądami w ramach audytów bezpieczeństwa.

d. w zakresie bezpieczeństwa sieci i stacji roboczych
   i. segmentacja sieci (oddzielne VLAN/SSID dla gości, personelu i systemów medycznych), filtrowanie ruchu i kontrola dostępu administracyjnego do infrastruktury; aktualizacje zabezpieczeń wdrażane niezwłocznie po publikacji.
   ii. ochrona przed złośliwym oprogramowaniem: centralnie zarządzane rozwiązania anty-malware/EDR, aktualizacje sygnatur i plan skanowań, blokada uruchamiania nieautoryzowanych aplikacji na stacjach roboczych.

e. w zakresie szyfrowania i transmisji
   i. wymóg stosowania szyfrowania danych w transmisji (np. TLS) oraz szyfrowania kopii zapasowych i nośników przenośnych, z uregulowanym cyklem życia i przechowywaniem kluczy.
   ii. przekazywanie dokumentacji elektronicznie wyłącznie bezpiecznymi kanałami; w razie stosowania haseł – przekazanie hasła odrębnym kanałem.

f. w zakresie kopii zapasowych i odtwarzania
   i. wykonywanie i testowanie kopii zapasowych w cyklach adekwatnych do ryzyka, przechowywanie poza środowiskiem produkcyjnym i w kontrolowanych lokalizacjach; okresowe testy odtworzeniowe.
   ii. plan zapewnienia ciągłości działania i odtwarzania po incydencie, w tym utrzymanie długoterminowej dostępności dokumentacji elektronicznej (migracje formatów/nośników).

g. w zakresie nośników i utylizacji - bezpieczne usuwanie danych przed przekazaniem/naprawą/likwidacją, a gdy to niemożliwe – fizyczne zniszczenie nośnika; niszczenie wydruków zgodnie z procedurą.

h. w zakresie rozwoju aplikacji i zmian - rozdzielenie środowisk (dev/test/prod), formalne zarządzanie zmianą, testy bezpieczeństwa adekwatne do ryzyka przed wdrożeniem; wymagania bezpieczeństwa w umowach z wytwórcami i integratorami.

i. w zakresie relacji z dostawcami i powierzeń - umowy z dostawcami i podmiotami przetwarzającymi określają środki techniczno-organizacyjne, podprzetwarzanie, obowiązki poufności, prawo do audytu i reagowania na incydenty; okresowa weryfikacja zgodności.

j. w zakresie szkoleń i świadomości - szkolenia wstępne i cykliczne dla personelu (dostęp, czyste biurko/ekran, phishing, nośniki, incydenty), z dokumentowaniem udziału i weryfikacją wiedzy; komunikaty przypominające dobre praktyki.

k. w zakresie postępowania z incydentami - procedura wykrywania, klasyfikacji, eskalacji i raportowania naruszeń, w tym notyfikacji do organu i osób, analizy przyczyn źródłowych oraz działań naprawczych i zapobiegawczych; prowadzenie rejestru naruszeń.

X. Postępowanie w przypadku naruszenia przetwarzania danych osobowych

1. Niniejsza procedura określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku gdy stwierdzono naruszenie ochrony danych osobowych.
2. W przypadku stwierdzenia naruszenia ochrony danych osobowych, osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym

administratora danych osobowych lub Inspektora Ochrony Danych jednym z kanałów:

a) osobiście;
b) telefonicznie pod nr [503165944]
c) e-mailem na iod@psychiatria.bialystok.pl

3. W przypadku zdarzeń krytycznych (masowe ujawnienie danych zdrowotnych, ransomware, utrata backupu) zgłoszenia kieruje się niezwłocznie telefonicznie na numer [503165944], a poza godzinami pracy – na **iod@psychiatria.bialystok.pl** z oznaczeniem 'PILNE – NARUSZENIE'.
4. Administrator danych osobowych, we współpracy z Inspektorem Ochrony Danych i osobą odpowiedzialną za systemy informatyczne po otrzymaniu powiadomienia:
   - podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu,
   - zabezpiecza, utrwala wszelkie informacje i dokumenty, które mogą stanowić pomoc przy ustaleniu przyczyn naruszenia,
   - ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu lub dokumentacji,
   - dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
   - sporządza szczegółowy raport zawierający:
     a) datę i godzinę zdarzenia,
     b) wskazanie osoby powiadamiającej o zaistniałym zdarzeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
     c) informacje na temat lokalizacji zdarzenia (nr pokoju, nazwa pomieszczenia określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.),
     d) rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące,
     e) opis podjętych przez siebie działań, mających na celu zaradzenie naruszeniu bezpieczeństwa ochrony danych,
     f) wstępną ocenę przyczyn wystąpienia naruszenia,
     g) opis środków zaradczych (co administrator danych osobowych zamierza zrobić, aby przeciwdziałać wystąpieniu takiego zdarzenia w przyszłości, np. przeszkolenie pracownika, zabezpieczenie pomieszczenia).
5. W przypadku incydentów dotyczących dokumentacji medycznej (EDM lub papierowej), systemów medycznych błędnych udostępnień dokumentacji pacjentom/osobom upoważnionym lub wysyłek na niewłaściwy adres, stosuje się niniejszą procedurę ze szczególnym priorytetem czasowym
6. Wzór raportu z naruszenia przetwarzania danych osobowych stanowi Załącznik nr 5 do niniejszej Polityki.
7. Administrator danych osobowych podejmuje niezbędne działania w celu zapobieżenia naruszeniom zabezpieczeń systemu w przyszłości. Wnioski z incydentu uwzględnia się w przeglądzie Polityki oraz środków technicznych i organizacyjnych.
8. Administrator danych osobowych po stwierdzeniu, iż naruszenie ochrony danych osobowych spowodowało ryzyko naruszenia praw i wolności osób, których dane podlegały naruszeniu, niezwłocznie informuje o tym fakcie organ nadzorczy, ale nie dłużej niż w ciągu 72 godzin od momentu wykrycia naruszenia. Oceny ryzyka dokonuje Administrator we współpracy z IOD.
9. W przypadku braku możliwości zgłoszenia organowi nadzorczemu naruszenia, o którym mowa w ustępie poprzedzającym, w ciągu 72 godzin od momentu jego wykrycia, administrator do zgłoszenia dołącza wyjaśnienie przyczyn opóźnienia.
10. Zgłoszenie naruszenia do organu nadzorczego, musi co najmniej:

a. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

15. Administrator danych osobowych po stwierdzeniu, iż naruszenie ochrony danych osobowych spowodowało wysokie ryzyko naruszenia praw i wolności osób, niezwłocznie informuje o tym fakcie osoby których dane podlegały naruszeniu.
16. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych musi minimum:
    a. zawierać imię i nazwisko oraz dane kontaktowe administratora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji (np. inspektora ochrony danych osobowych);
    b. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
    c. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
17. Zawiadomienie organu nadzorczego o naruszeniu odbywa się za pomocą odpowiedniego formularza dostępnego na stronie internetowej Urzędu Ochrony Danych Osobowych (www.uodo.gov.pl). Zgłoszeń dokonuje się przez system UODO zgodnie z aktualnymi wytycznymi.
18. Administrator nie zawiadamia osób, których dane dotyczą o naruszeniu ochrony danych osobowych, jeżeli:
    a. administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
    b. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
    c. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób

    Decyzję o skorzystaniu z wyjątku podejmuje Administrator po konsultacji z IOD, dokumentując uzasadnienie w raporcie incydentu.
19. Każde naruszenie wpisywane jest do ewidencji naruszeń ochrony danych osobowych, której wzór stanowi załącznik nr 6 do niniejszej Polityki. Ewidencja może być prowadzona elektronicznie.
20. Po zakończeniu obsługi naruszenia Administrator wraz z IOD dokonują przeglądu adekwatności środków oraz, w razie potrzeby, aktualizują Politykę.
21. W celu realizacji praw podmiotu danych, realizuje się procedurę stanowiącą załącznik nr 7 do niniejszej Polityki.

XI. Powierzenie przetwarzania danych osobowych

1. Administrator może korzystać z usług podmiotów zewnętrznych, zwłaszcza jeżeli współpraca ma na celu poprawę bezpieczeństwa danych osobowych lub zapewnia większą efektywność działań Administratora.
2. Rozróżnia się powierzenie przetwarzania danych (podmiot przetwarzający w rozumieniu art. 28 RODO) oraz udostępnienie danych innemu administratorowi (np. innym podmiotom leczniczym, laboratoriom, NFZ, organom publicznym), przy czym w tym drugim przypadku podstawę i zakres udostępnienia określają przepisy właściwe dla dokumentacji medycznej i świadczeń zdrowotnych.
3. Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia ogólnego o ochronie danych i chroniło prawa osób, których dane dotyczą. Obejmuje to w szczególności odpowiednią wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych.
4. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie pisemnej umowy wiążącej podmiot przetwarzający i administratora, określającej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
5. Umowa ta może być zawarta także jako część umowy pierwotnej.
6. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
7. Administrator może zezwolić podmiotowi przetwarzającemu podpowierzenie przetwarzania danych osobowych innemu podmiotowi, w sytuacji gdy jest to zasadne i konieczne.

XII. Przekazywanie danych osobowych do państw trzecich

1. Administrator Danych Osobowych może przekazywać dane osobowe poza Europejski Obszar Gospodarczy wyłącznie zgodnie z rozdziałem V RODO, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony (art. 45) albo odpowiednich zabezpieczeń (art. 46), takich jak standardowe klauzule umowne.
2. Wyjątki określone w art. 49 RODO (np. wyraźna zgoda, konieczność wykonania umowy na żądanie osoby) stosuje się incydentalnie, po spełnieniu warunków i należytym poinformowaniu o ryzykach.
3. Przykładowe kategorie transferów operacyjnych
    a. Usługi infrastrukturalne: hosting strony WWW, hosting poczty elektronicznej, chmura obliczeniowa, narzędzia wsparcia IT, jeżeli wiążą się z dostępem spoza EOG.
    b. Komunikacja i marketing: platformy i wtyczki serwisów WWW, analityka, piksele, media społecznościowe, o ile powodują przekazanie danych do państw trzecich.
    c. Dostawcy i podwykonawcy (podmioty przetwarzające i dalsi podprzetwarzający), gdy świadczą usługi z lokalizacji w państwach trzecich albo umożliwiają z nich dostęp.
4. Przed transferem Administrator identyfikuje podstawę prawną (art. 45 lub 46), dokonuje oceny prawa i praktyki państwa trzeciego oraz ustala środki uzupełniające, w tym szyfrowanie, pseudonimizację, kontrolę dostępu i minimalizację zakresu.

5. Z dostawcami zawierane są umowy zapewniające wymagany poziom ochrony (w tym standardowe klauzule umowne), a ich dalsze powierzenia są weryfikowane i ograniczane odpowiednimi postanowieniami.
6. Gdy stosowany jest wyjątek z art. 49, Administrator dokumentuje podstawę, okoliczności incydentalności i przekazuje osobie jasne informacje o ryzykach.
7. Informacje o kategoriach odbiorców, potencjalnych państwach trzecich, podstawach przekazania i stosowanych zabezpieczeniach są ujawniane w klauzulach informacyjnych odpowiednich kategorii osób i aktualizowane w razie zmian.
8. Administrator ogranicza przekazy do przypadków niezbędnych dla realizacji celów, preferując przetwarzanie w EOG lub w jurysdykcjach objętych decyzją Komisji Europejskiej.

XIII. Podstawy prawne przetwarzania danych osobowych

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2. Dopuszcza się następujące przesłanki przetwarzania danych szczególnej kategorii:

a. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;

b. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

c. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

d. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych

członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

e. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

i. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

j. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

XIV. Spełnianie obowiązku informacyjnego wobec podmiotów danych

1. Informowanie osób, których dane dotyczą o przetwarzaniu ich danych osobowych, stanowi jeden z podstawowych obowiązków administratora danych i odbywa się zgodnie z art. 13–14 RODO, w sposób przejrzysty, zrozumiały i łatwo dostępny, z wykorzystaniem podejścia warstwowego.
2. Obowiązek informacyjny aktualizuje się w trzech sytuacjach:
    a. przy zbieraniu danych, od osoby, której dane dotyczą;
    b. przy zbieraniu danych w sposób inny niż od osoby, której dane dotyczą;
    c. przez cały okres przetwarzania danych osobowych (w związku z prawem dostępu przysługującym osobie, której dane dotyczą).
3. Przekazanie podmiotowi danych informacji o przetwarzaniu jego danych osobowych, powinno nastąpić w momencie gromadzenia tych danych.
4. W przypadku zbieraniu danych w sposób inny niż od osoby, której dane dotyczą, informacje o przetwarzaniu danych osobowych, administrator danych podaje podmiotowi danych:
    a. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
    b. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub

c. jeżeli planuje ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

5. Obowiązek informacyjny realizowany jest warstwowo:
   a. Warstwa 1 (skrót): zawiera kluczowe informacje – tożsamość administratora, kontakt do IOD, cele i podstawy przetwarzania w ujęciu grup, kategorie odbiorców, zwięzłe wskazanie praw oraz odnośnik (URL/QR) do warstwy pełnej - prezentowana bezpośrednio w miejscu pozyskiwania danych;
   b. Warstwa 2 (pełna): zawiera wszystkie informacje wymagane przez art. 13/14 RODO, w tym okresy przechowywania, źródło danych (dla art. 14), ewentualne przekazania poza EOG i zabezpieczenia, informacje o zautomatyzowanym podejmowaniu decyzji/profilowaniu - dostępna na stronie WWW oraz w dokumentach źródłowych.
6. Za realizację obowiązku informacyjnego, o którym mowa w ustępach poprzedzających, odpowiedzialny jest:
   a. wobec pracowników i kandydatów – Dział Kadr/HR (przekazanie klauzul przy zatrudnieniu i w rekrutacji, aktualność treści w teczkach kadrowych i ogłoszeniach, publikacja/aktualizacja na WWW w części „Praca”);
   b. wobec kontrahentów – Dział Zakupów/Umów (dołączanie klauzul do umów/zamówień i komunikacji B2B, linkowanie w korespondencji oraz formularzach B2B, publikacja/aktualizacja na WWW w sekcji dla dostawców);
   c. wobec pacjentów – kierownicy jednostek medycznych odpowiadają za ekspozycję Warstwy 1 i dostępność Warstwy 2;
7. Wzór klauzuli informacyjnej stanowi załącznik nr 8 do Polityki.

XV. Analiza konieczności powołania Inspektora Ochrony Danych Osobowych i jego obowiązki

1. Ogólne rozporządzenie o ochronie danych w art. 37 ust. 1 przewiduje obowiązek wyznaczenia inspektora dla administratorów i podmiotów przetwarzających wówczas, gdy:
   a. przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
   b. główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę.
   c. główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10.
2. Jednostka wyznacza Inspektora Ochrony Danych.
3. IOD wykonuje zadania w sposób niezależny, nie otrzymuje instrukcji dotyczących wykonywania swoich obowiązków, podlega bezpośrednio Zarządowi i nie pełni funkcji powodujących konflikt interesów.
4. Punkt kontaktowy do IOD: iod@psychiatria.bialystok.pl, tel. 503165944. Dane kontaktowe IOD są podawane w klauzulach informacyjnych oraz udostępniane publicznie na stronie internetowej podmiotu.
5. IOD realizuje zadania określone w art. 39 RODO, w szczególności: informuje i doradza w zakresie przepisów o ochronie danych i polityk wewnętrznych, monitoruje ich przestrzeganie (w tym szkolenia i audyty), współpracuje z organem nadzorczym oraz pełni funkcję punktu kontaktowego.
6. IOD jest włączany we wszystkie sprawy dotyczące ochrony danych, w tym w przegląd i aktualizację Polityki oraz w konsultacje nowych lub istotnie zmienianych projektów, systemów i umów, które mogą wpływać na przetwarzanie danych (privacy by design/default).
7. IOD uczestniczy w ocenie naruszeń ochrony danych, rekomenduje środki zaradcze, wspiera kwalifikację ryzyka oraz przygotowanie zgłoszeń do organu nadzorczego i zawiadomień osób.

8. IOD ma dostęp do informacji niezbędnych do wykonywania zadań oraz do czynności przetwarzania i dokumentacji; Administrator zapewnia IOD zasoby i wsparcie organizacyjne.
9. Administrator zapewnia ciągłość funkcji IOD (zastępstwo/obsada) oraz niezwłocznie aktualizuje publicznie dostępne dane kontaktowe w razie zmiany.

XVI. Analizowanie poziomu ryzyka utraty bezpieczeństwa danych osobowych

1. Administrator stosuje podejście oparte na ryzyku, utrzymując proces identyfikacji, analizy, oceny i traktowania ryzyka prywatności oraz bezpieczeństwa danych, tak aby stopień bezpieczeństwa odpowiadał ryzyku dla praw i wolności osób fizycznych.
2. Administrator i podmioty przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku.
3. Administrator i podmioty przetwarzające uwzględniają ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Administrator stosuje podejście oparte na ryzyku przy doborze środków technicznych i organizacyjnych; w przypadkach uzasadnionych charakterem i skalą przetwarzania dokumentuje przyjęte założenia i wnioski z oceny.
4. Szacując ryzyko, Administrator Danych Osobowych i podmioty przetwarzające uwzględniają w szczególności ryzyko wiążącego się z przetwarzaniem, w szczególności wynikające z:
   a. przypadkowego lub niezgodnego z prawem zniszczenia,
   b. utraty, modyfikacji, nieuprawnionego ujawnienia,
   c. lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
5. Ocena ryzyka w ramach oceny skutków dla ochrony danych jest jednym z przypadków szacowania ryzyka. Przeprowadzenie oceny skutków dla ochrony danych jest wymagane zawsze wtedy, gdy:
   a. poziom ryzyka został określony jako wysoki w wyniku jego szacowania przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania oraz wysokiego prawdopodobieństwa lub
   b. dany rodzaj przetwarzania został wskazany w przepisie prawa (np. art. 35 ust. 3 RODO), lub
   c. dany rodzaj przetwarzania został wskazany w wykazie podanym do publicznej wiadomości przez krajowy organ nadzorczy (zgodnie z art. 35 ust. 4 RODO) .
6. Metodyka oceny ryzyka i ewentualne wzory dokumentów są określone w odrębnym dokumencie wewnętrznym i mogą być dostosowywane do skali i specyfiki działalności placówki medycznej.

XVII. Postanowienia końcowe

1. Polityka podlega przeglądowi co najmniej raz w roku oraz każdorazowo po wystąpieniu istotnego naruszenia ochrony danych osobowych lub po innych istotnych zmianach organizacyjnych, prawnych lub technologicznych wpływających na przetwarzanie danych.
2. Za przygotowanie przeglądu oraz propozycji zmian Polityki odpowiada koordynator ds. ochrony danych, we współpracy z Inspektorem Ochrony Danych.
3. Inspektor Ochrony Danych opiniuje wynik przeglądu, przedstawia rekomendacje działań korygujących oraz może wnioskować o aktualizację Polityki, wnioski i opinie IOD dołącza się do materiałów przeglądowych.
4. Zmiany Polityki wymagają zatwierdzenia przez Zarząd/Administratora Danych i wchodzą w życie z dniem podpisania zarządzenia wprowadzającego.

5. Administrator Danych zapewnia poinformowanie personelu o zmianach Polityki i, w razie potrzeby, organizuje odpowiednie działania szkoleniowe związane z wprowadzonymi zmianami.
6. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy 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).

XVIII. Lista załączników i załączniki

ZAŁĄCZNIK NR 1	wzór rejestru czynności przetwarzania
ZAŁĄCZNIK NR 2	wzór upoważnienia do przetwarzania danych osobowych
ZAŁĄCZNIK NR 3	wzór oświadczenia i zobowiązania osoby przetwarzającej dane osobowe do zachowania tajemnicy
ZAŁĄCZNIK NR 4	wzór ewidencji osób upoważnionych do przetwarzania
ZAŁĄCZNIK NR 5	wzór raportu z naruszenia przetwarzania danych osobowych
ZAŁĄCZNIK NR 6	wzór ewidencji naruszeń ochrony danych osobowych
ZAŁĄCZNIK NR 7	procedura realizacji praw podmiotu
ZAŁĄCZNIK NR 8	wzór klauzuli informacyjnej