Załącznik nr 1 do zarządzenia nr 26/2018
Dyrektora Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji
im. prof. dr hab. Eleonory Reicher
z dnia 7 listopada 2018 r.

ZATWIERDZIŁ:
Dyrektor Narodowego Instytutu Geriatrii,
Reumatologii i Rehabilitacji im. prof. dr hab. med. Eleonory Reicher
Dr n. med. Marek Tombarkiewicz

# POLITYKA
# OCHRONY DANYCH OSOBOWYCH

# w

# Narodowym Instytucie Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher

DOKUMENT DO UŻYTKU WEWNĘTRZNEGO

Warszawa, listopad 2018 r.

# I. Spis treści

## II. Definicje

| Pojęcie | Znaczenie |
|---|---|
| **adekwatność lub minimalizacja danych** | zasada dotycząca przetwarzania danych osobowych polegająca na tym, że administrator danych powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne do realizacji celu dla którego dane są zbierane; |
| **administrator** | osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W niniejszej dokumentacji ochrony danych osobowych przez administratora danych rozumie się Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher; |
| **analiza ryzyka** | proces identyfikacji ryzyka, określania jego wartości i identyfikowanie niezbędnych zabezpieczeń; |
| **anonimizacja** | przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów lub działań; |
| **audyt zgodności** | czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami RODO oraz innymi przepisami o ochronie danych osobowych, a także czynności mające na celu monitorowanie przestrzegania polityki ochrony danych osobowych; |
| **dane biometryczne** | dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne; |
| **dane dotyczące zdrowia** | dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia; |
| **dane genetyczne** | dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej; |
| **dane osobowe** | informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, 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; |
| **docelowy poziom ryzyka** | docelowy poziom pojedynczego ryzyka, jaki administrator zamierza osiągnąć w odniesieniu do konkretnego ryzyka; |
| **dostępność** | właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu; |
| **działania zaradcze** | środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środki w celu |

| | |
|---|---|
| | zminimalizowania ewentualnych negatywnych skutków naruszenia; |
| **hasło** | ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym; |
| **identyfikator** | ciąg znaków literowych, cyfrowych lub innych znaków identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym; |
| **incydent** | naruszenie bezpieczeństwa 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; |
| **Instytut** | Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa; |
| **integralność** | zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób; |
| **Inspektor** | osoba pełniąca funkcję inspektora ochrony danych w rozumieniu art. 37 RODO |
| **istotność ryzyka** | iloczyn prawdopodobieństwa i wpływu ryzyka określający potencjalny skumulowany poziom wpływu ryzyka na osiąganie przez administratora zamierzonych celów; |
| **legalność** | zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane zgodnie z prawem, po spełnieniu przynajmniej jednego z warunków określonych w art. 6 ust. 1 lub art. 9 ust. 2 RODO; |
| **mapa ryzyka** | graficzne zestawienie ryzyka z punktu widzenia ich istotności, lub innych kryteriów; |
| **ocena ryzyka** | proces porównywania ryzyka z założonymi kryteriami ryzyka w celu wyznaczenia wagi ryzyka; |
| **odbiorca** | osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Przy czym odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państw członkowskiego; |
| **ograniczenie celu** | zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; |
| **okresowość** | zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane przez okres nie dłuższy, niż jest to niezbędne do celów, dla realizacji których dane są przetwarzane; |
| **organ nadzorczy** | niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych w Unii Europejskiej, zgodnie z art. 51 RODO; |
| **osoba upoważniona** | osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę; |
| **podmiot przetwarzający** | osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarzana dane osobowe w imieniu administratora; |
| **Polityka** | niniejszy dokument, tj. Polityka ochrony danych osobowych; |
| **poufność** | właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym |

| | |
|---|---|
| | podmiotom; |
| **pracownik lub współpracownik** | osoba zatrudniona przez Instytut na podstawie umowy o pracę oraz osoba świadcząca na rzecz Instytutu usługi na podstawie umów cywilnoprawnych, a także praktykanci, wolontariusze, stażyści i studenci; |
| **prawdopodobieństwo** | oczekiwana częstość materializacji danego ryzyka; |
| **przetwarzanie** | operacja 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; |
| **pseudonimizacja** | przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; |
| **raport zgodności** | dokument opracowywany przez Inspektora Ochrony Danych po dokonaniu audytu zgodności zawierający opis niezgodności przetwarzania danych osobowych z przepisami RODO, innymi przepisami o ochronie danych osobowych oraz Polityką, a także zawierający ogólną ocenę poziomu ochrony danych osobowych; |
| **rejestr czynności przetwarzania danych osobowych** | dokument, o którym mowa w art. 30 ust. 1 RODO, prowadzony w formie pisemnej przez administratora, udostępniany organowi nadzorczemu na jego żądanie; |
| **rejestr wszystkich kategorii czynności przetwarzania** | dokument, o którym mowa w art. 30 ust. 2 RODO, prowadzony w formie pisemnej przez podmiot przetwarzając, udostępniany organowi nadzorczemu na jego żądanie; |
| **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); |
| **rola** | grupa uprawnień przypisanych do stanowiska pracy: np. administracja, lekarz, pielęgniarka, ratownik medyczny, rehabilitant, technik obrazowy, rozliczenia, kadry, płace, księgowość. |
| **rozliczalność przetwarzania** | właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi; |
| **ryzyko** | kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji. Ryzyko związane z bezpieczeństwem danych osobowych to prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów; |
| **rzetelność** | zasada dotycząca przetwarzania danych osobowych zapewniająca merytoryczną poprawność danych osobowych poprzez ich zgodność ze stanem faktycznym, kompletność i aktualność; |
| **skutek** | efekt materializacji ryzyka; |

| | |
|---|---|
| **strona trzecia lub osoba trzecia** | osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe; |
| **system informatyczny** | zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych; |
| **szacowanie ryzyka** | całościowy proces analizy i oceny ryzyka; |
| **właściciel ryzyka** | osoba, która ze względu na zajmowane stanowisko i przydział odpowiedzialności zarządza głównymi czynnikami ryzyka, przypisanego do niej. Właścicielami ryzyka mogą być dyrektorzy, kierownicy, samodzielne stanowiska lub pełnomocnicy odpowiadający za zarządzane przez nich procesy przetwarzania danych osobowych; |
| **wpływ** | potencjalne skutki materializacji ryzyka; |
| **upoważnienie** | oświadczenie nadane przez administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę; |
| **uwierzytelnianie** | działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby upoważnionej; |
| **zabezpieczenie** | środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną; |
| **zagrożenie** | niepożądane zdarzenie, które powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie danych osobowych na utratę, ujawnienie, zniszczenie lub zmianę; |
| **zarządzanie ryzykiem** | skoordynowane działania w celu identyfikacji, minimalizacji lub eliminacji prawdopodobieństwa oraz skutków realizacji zagrożeń; |
| **zbiór danych** | uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie. |

# III. Wstęp

Tworzy się niniejszą Politykę ochrony danych osobowych celem realizacji obowiązków wynikających z powszechnie obowiązującego prawa, w szczególności 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 lub RODO) oraz ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO. Aby móc to wykazać administrator wdraża niniejszą Politykę.

Aby przetwarzanie odbywało się w sposób zapewniający należytą ochronę danych osobowych będących w zasobach administratora, przetwarzanie obywa się z zachowaniem następujących zasad:

- zgodności z prawem;
- rzetelności, przejrzystości i ograniczoności celu;
- adekwatności, prawidłowości i okresowości przetwarzanych danych;
- poufności, integralności i rozliczalności danych.

Polityka ochrony danych osobowych jest aktualizowana w przypadku zmiany przepisów prawa w zakresie ochrony danych osobowych lub w związku ze zmianą stanu faktycznego, które wpływają na treść dokumentu.

Zakres podmiotowy stosowania niniejszej Polityki obejmuje wszystkich pracowników lub współpracowników mających dostęp do danych osobowych.

Żadna procedura ani regulacja wewnętrzna obowiązująca u administratora nie może naruszać zasad określonych w niniejszej Polityce.

Administrator, zgodnie z treścią art. 37 ust. 1 lit. b) RODO, wyznaczył Inspektora Ochrony Danych, który wykonując zadania zgodnie z art. 39 RODO, podlega bezpośrednio Dyrektorowi Instytutu.

Dane osobowe chronione niniejszą Polityką przetwarzane są w siedzibie administratora danych mieszczącej się w Warszawie, adres: Spartańska 1, 02-637 Warszawa oraz w siedzibach podmiotów przetwarzających dane osobowe wskazanych w wykazie podmiotów przetwarzających dane osobowe w imieniu administratora, prowadzonym zgodnie ze wzorem stanowiącym załącznik nr 12 do niniejszej Polityki.

## IV. Określenie obowiązków

**Administrator** jest zobowiązany do:

- zapewnienia niezbędnych środków do stworzenia i funkcjonowania systemu ochrony danych osobowych;
- wdrożenia niezbędnych środków organizacyjnych i technicznych zapewniających rozliczalność, integralność oraz poufność przetwarzanych danych osobowych;
- zapewnienia, by systemy informatyczne wykorzystywane do przetwarzania danych spełniały odpowiednie środki techniczne zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których dane są przetwarzane;
- wdrożenia odpowiednich środków organizacyjnych, zapewniających stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych;
- zapewnienia, aby osoby dopuszczone do przetwarzania danych osobowych przestrzegały przepisy o ochronie danych osobowych;
- zapewnienia, by dostęp do danych osobowych udzielany był wyłącznie osobom upoważnionym do ich przetwarzania;
- podejmowania odpowiednich środków, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 RODO w sprawie przetwarzania;
- zapewniania, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
- zapewniania, by Inspektor Ochrony Danych nie otrzymywał instrukcji dotyczących wykonywania przez niego zadań;
- zatwierdzania Polityki ochrony danych osobowych oraz dokumentów opracowanych na jej podstawie.

**Inspektor Ochrony Danych** jest zobowiązany do:

- informowania administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisach o ochronie danych osobowych i doradzania im w tym zakresie;
- monitorowania przestrzegania RODO, innych przepisów o ochronie danych osobowych oraz Polityki administratora poprzez wykonywanie audytów zgodności;
- opracowywania, po każdorazowym przeprowadzeniu audytu zgodności, raportu dla administratora;
- nadzorowania wdrażania zabezpieczeń będących wynikiem audytu zgodności oraz analizy ryzyka;
- podejmowania działań zwiększających świadomość z zakresu ochrony danych osobowych, w tym informowanie o zagrożeniach związanych z dostępem do danych osobowych;
- szkolenia personelu uczestniczącego w operacjach przetwarzania;
- udzielania na żądanie, zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
- współpracy z organem nadzorczym;
- pełnienia roli 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;
- pełnienie roli punktu kontaktowego dla osób, których dane dotyczą;
- reagowania na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych, analizowanie ich przyczyn oraz kierowanie wniosków dotyczących usprawnienia ochrony danych osobowych i ukarania winnych naruszeń;
- aktualizacji Polityki ochrony danych osobowych;
- prowadzenia wykazu podmiotów przetwarzających dane;
- prowadzenia rejestru czynności przetwarzania danych osobowych;
- prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu podmiotu powierzającego;
- przygotowania i bieżącej aktualizacji treści informacji podawanych w przypadku zbierania danych od osoby, której dane dotyczą;
- przygotowania i bieżącej aktualizacji treści informacji podawanych w przypadku zbierania danych od osobowych w sposób inny niż od osoby, której dane dotyczą.

**Komórka właściwa ds. IT** jest zobowiązana do:

- nadzorowania stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych przetwarzanych w systemie informatycznym;
- bieżącego utrzymania systemów informatycznych służących do przetwarzania danych osobowych i ich funkcjonowania, zapewniającego ich poufność, integralność i dostępność, m.in. poprzez właściwą aktualizację tych systemów;
- zarządzania systemem komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji w sposób zapewniający bezpieczeństwo wymiany danych;
- nadzorowania funkcjonowania mechanizmów uwierzytelniania użytkowników w systemie informatycznym oraz kontroli dostępu do danych osobowych;
- wykonywania kopii bezpieczeństwa elektronicznych zbiorów danych osobowych;
- okresowego sprawdzania kopii bezpieczeństwa pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
- prowadzenia depozytu kopii bezpieczeństwa i logów danych;
- przydzielania użytkownikom indywidualnych identyfikatorów i haseł do systemu informatycznego oraz dokonywania ewentualnych modyfikacji uprawnień, a także usuwania kont użytkowników;
- okresowego zmieniania haseł dostępu użytkowników do systemu informatycznego w przypadkach, gdy system informatyczny nie wymusza okresowej zmiany haseł użytkowników;
- prowadzenia bieżącej ewidencji wszystkich użytkowników systemów informatycznych służących do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik nr 8 do niniejszej Polityki ;
- osobistego wykonywania lub sprawowania nadzoru na wykonaniem napraw, konserwacji oraz likwidacji urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe;
- uczestniczenia w procesie zakupów aplikacji oraz oprogramowania zatwierdzonego do włączenia do sytemu informatycznego służącego do przetwarzania danych osobowych;
- zapewnienia legalności oprogramowania wykorzystywanego w systemie informatycznym służącym do przetwarzania danych osobowych oraz zarządza licencjami do odpowiednich elementów systemu informatycznego;
- zapewnienia właściwej konfiguracji systemów zarządzania hasłami;
- inwentaryzacji sprzętu komputerowego oraz systemów informatycznych;
- bieżącej inwentaryzacji przepływów danych osobowych pomiędzy systemami służącymi do przetwarzania danych osobowych;
- prowadzenie, przy współpracy z Inspektorem, postępowania wyjaśniającego w sytuacji wystąpienia naruszenia ochrony danych osobowych.

**Osoba upoważniona** jest zobowiązana do:

- przestrzegania przyjętych u administratora zasad ochrony danych osobowych ze szczególnym uwzględnieniem zasady bezpieczeństwa;
- informowania bezpośredniego przełożonego lub komórkę właściwą ds. IT o incydentach godzących w bezpieczeństwo danych osobowych;
- dochowywania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane są przetwarzane;
- zachowania w poufności przetwarzanych danych osobowych oraz sposobów ich zabezpieczania;
- usuwania danych osobowych, które administrator pozyskuje lub są na rzecz administratora przekazywane, zawsze wtedy, gdy administrator nie posiada interesu prawnego i faktycznego w przetwarzaniu (w tym archiwizacji) tych danych. W razie wątpliwości, co do obowiązku usunięcia danych osobowych osoba upoważniona powinna zwrócić się o opinię do Inspektora;
- uporządkowania swojego stanowiska pracy, wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych, w szczególności: zabezpieczenia komputerów i wszelkich nośników danych, wyłączenia wszystkich urządzeń elektrycznych (niewymagających stałego zasilania), zamknięcia okien i drzwi oraz zdania kluczy po zakończeniu pracy.

# V. Odpowiedzialność

**Administrator** za naruszenie ochrony danych osobowych może ponieść odpowiedzialność cywilną zgodnie z art. 82 RODO lub odpowiedzialność administracyjną na podstawie wskazanej w art. 83 lub 84 RODO.

Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony może ponieść odpowiedzialność karną przewidzianą w art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

**Podmiot przetwarzający** za naruszenie ochrony danych osobowych może ponieść odpowiedzialność cywilną zgodnie z art. 82 RODO lub odpowiedzialność administracyjną na podstawie wskazanej w art. 83 i 84 RODO.

Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony może ponieść odpowiedzialność karną przewidzianą w art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

**Osoba upoważniona** za naruszenie ochrony danych osobowych może ponieść odpowiednio odpowiedzialność wskazaną w art. 52 lub 108 kodeksu pracy albo odpowiedzialność kontraktową przewidzianą w art. 471 kodeksu cywilnego. Osoba upoważniona może także ponieść odpowiedzialność karną przewidzianą w art. 266 kodeksu karnego.

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku wykrycia incydentu lub uzasadnionego podejrzenia powstania incydentu nie podjęła działania określonego w niniejszej Polityce, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie udokumentowała takiego przypadku, możne zostać wszczęte postępowanie dyscyplinarne.

Kara dyscyplinarna nałożona na osobę uchylającą się od powiadomienia, o którym mowa powyżej, nie wyklucza odpowiedzialności karnej tej osoby oraz możliwości kierowania wobec takiej osoby roszczeń cywilnych przez administratora o zrekompensowanie poniesionych strat.

# VI. Zapewnienie poufności, integralności oraz rozliczalności danych osobowych

Administrator zapewnia poufność, integralność oraz rozliczalność przetwarzanych danych osobowych, poprzez zastosowanie niezbędnych środków organizacyjnych oraz technicznych.

Dobór powyższych środków ma na celu obniżyć poziom ryzyka wystąpienia incydentów, związanych z bezpieczeństwem przetwarzania danych osobowych, do poziomu akceptowalnego przez administratora.

Wprowadzenie omawianych środków, zostało poprzedzone przeprowadzeniem analizy kosztów ich wdrożenia w odniesieniu do stopnia bezpieczeństwa przetwarzania danych osobowych, jaki administrator zamierza osiągnąć po ich wdrożeniu.

**W ramach grupy środków organizacyjnych wprowadza się, w szczególności:**

- monitorowanie przestrzegania niniejszej Polityki przez wyznaczonego Inspektora Ochrony Danych;
- nadzór środowiska informatycznego przez kierownika komórki właściwej ds. IT;
- upoważnienia do przetwarzania danych osobowych, które są wydawane każdemu pracownikowi zgodnie z zakresem obowiązków;
- ewidencję upoważnień do przetwarzania danych osobowych;
- oświadczenia o zachowaniu w poufności danych osobowych i sposobów zabezpieczenia danych, które są zbierane od osób upoważnionych;
- szkolenia dla osób upoważnionych z zasad bezpiecznego przetwarzania danych osobowych;
- umowy powierzenia w rozumieniu art. 28 ust. 3 RODO, zawierane z podmiotami przetwarzającymi dane w imieniu administratora danych;
- ewidencję umów powierzenia;
- rejestr czynności przetwarzania danych osobowych zgodnie z art. 30 RODO;
- zasadę, zgodnie z którą osoby trzecie przebywają w obszarze przetwarzania danych wyłącznie w obecności osoby upoważnionej. Osoby trzecie mogą w wyjątkowych okolicznościach przebywać bez obecności osoby upoważnionej - w obszarze przetwarzania danych - po uprzednim wydaniu na to zgody przez administratora danych.

Ponadto, została określona odpowiedzialność pracownika lub podmiotu przetwarzającego za działania związane z naruszeniem bezpieczeństwa przetwarzania danych osobowych.

**W ramach grupy środków technicznych, wprowadza się w szczególności:**

- zabezpieczenia techniczne zapewniające poufność przetwarzanych danych osobowych:
  - nadzór Agencji Ochrony – obchód nocny i ochrona bramy wjazdowej;
  - obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych poprzez zastosowanie zamków patentowych lub kart wejściowych;
  - dane osobowe przetrzymywane w formie papierowej są przechowywane w zamykanych szafkach, szafach lub szufladach;
  - dostęp do danych w systemie informatycznym jest możliwy wyłącznie po udanym uwierzytelnieniu użytkownika;
  - hasła składają się z 8 znaków (małe, wielkie litery, przynajmniej jedna cyfra lub znak specjalny);
  - hasła są zmieniane nie rzadziej niż co 90 dni;
  - na stacjach roboczych, za pomocą których są przetwarzane dane osobowe, zainstalowano oprogramowanie antywirusowe automatycznie ściągające najnowsze sygnatury wirusów;
  - monitorowanie działania systemu informatycznego;
  - logiczna i fizyczna separacja sieci;
  - logiczny dostęp do danych osobowych z sieci publicznej ograniczony jest poprzez zastosowanie zapory ogniowej (firewall). Chroni ona wszystkie systemy informatyczne przed nieuprawnionym dostępem i atakami z zewnątrz.

- zabezpieczenia techniczne zapewniające integralność przetwarzanych danych osobowych:
  - ochrona przed nieautoryzowanym dostępem;
  - na stacjach roboczych, za pomocą których są przetwarzane dane osobowe, zainstalowano oprogramowanie antywirusowe automatycznie ściągające najnowsze sygnatury wirusów;
  - awaryjne podtrzymywanie zasilania serwerów oraz stacji roboczych za pomocą UPS;
  - właściwe okablowanie sieci;
  - cykliczna weryfikacja integralności baz danych poprzez odtwarzanie danych zawartych na kopiach zapasowych.

- zabezpieczenia techniczne zapewniające rozliczalność przetwarzanych danych osobowych:
  - dostęp do danych w systemie informatycznym możliwy wyłącznie po udanym uwierzytelnieniu użytkownika;
  - awaryjne podtrzymywanie zasilania serwerów oraz stacji roboczych za pomocą UPS;
  - zapis zdarzeń w systemach informatycznych.

**Przetwarzanie danych osobowych poza obszarem przetwarzania dopuszczalne jest wyłącznie po spełnieniu poniższych przesłanek:**

- zachowanie szczególnej ostrożności podczas transportu, przechowywania i użytkowania nośników zawierających dane osobowe;
- stosowanie środków ochrony kryptograficznej wobec przetwarzanych danych;
- zakaz pozostawiania nośników zawierających dane osobowe w miejscach powszechnie dostępnych;
- wykorzystywanie nośników wyłącznie w celach służbowych.

**Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:**

- likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie;
- naprawy – pozbawia się wcześniej zapisu tych danych w sposób umożliwiający ich odzyskanie.

## VII. Zasady szczególne obowiązujące w podmiocie leczniczym

Administrator jest podmiotem wykonującym działalność leczniczą w myśl przepisów ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej. W związku z udzielaniem świadczeń zdrowotnych, podmiot leczniczy ustala następujące zasady:

1. Administrator swoimi działaniami i organizacją podmiotu leczniczego zapewnia, że:
   a) dane osobowe w podmiocie leczniczym przetwarzane są na podstawie art. 6 ust. 1 lit. a) i b) oraz art. 9 ust. 2 lit. 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 zw. z art. 54 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa lub innych właściwych przepisów z zakresu ubezpieczeń społecznych;
   b) zakres pozyskiwanych danych wynika z przepisów prawa, o których mowa w punkcie 1 lit. a) i jest adekwatny do zdefiniowanych celów przetwarzania;
   c) określono konkretny czas przez jaki dane są przetwarzane;
   d) wobec pacjentów wykonano obowiązek informacyjny, zgodnie z art. 12-14 RODO;
   e) obowiązek informacyjny wobec pacjentów może być wykonywany poprzez umieszczenie w dokumentacji medycznej pacjenta, rejestracji, sekretariatach oddziału lub na stronie internetowej.

2. Dane osobowe w podmiocie leczniczym są pozyskiwane bezpośrednio od pacjentów lub od innych podmiotów uczestniczących w udzielaniu tym pacjentom świadczeń zdrowotnych.

3. W podmiocie leczniczym zabronione jest udzielanie 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 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 odpowiedzi w co najmniej dwóch zapytaniach.

4. W podmiocie leczniczym niedopuszczalne jest przekazywanie informacji zawierających dane osobowe podmiotom, instytucjom czy też organom, które nie mogą się wykazać prawidłową podstawą prawną dostępu do danych osobowych.

5. W przypadku konieczności wydania dokumentów zawierających dane osobowe (np. wyniki badań, recepty itp.) należy każdorazowo weryfikować tożsamość odbierającego za pomocą mechanizmu, o którym mowa w punkcie 3, a w przypadku, kiedy odbierającym nie jest adresat dokumentu żądać upoważnienia.

6. W podmiocie leczniczym zakazuje się wywoływania pacjentów z użyciem ich imion oraz nazwisk i wprowadza się system ich anonimizacji.

7. Organizacja rejestracji i poczekalni podmiotu leczniczego umożliwia zachowanie poufności osobom przebywającym bezpośrednio przy rejestracji.

8. Udzielanie świadczeń zdrowotnych w podmiocie leczniczym 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.

9. Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, parapetach itp.

## VIII. Zapewnienie realizacji praw i wolności osób, których dane dotyczą

Administrator ma świadomość, że zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach.

Administrator zapewniając realizację praw i wolności osób, których dane dotyczą, podjął odpowiednie, środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 RODO w sprawie przetwarzania.

Zapewniając realizację praw i wolności osób, których dane dotyczą administrator ustala następujące zasady:

1. Informacji udziela się na piśmie lub w inny sposób, w tym elektronicznie.
2. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
3. Informacji udziela się bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – osobie, której dane dotyczą, udziela się informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22 RODO.
4. Jeżeli osoba wskazana do udzielenia informacji ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15–21, powinna zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.
5. W przypadku przetwarzania niewymagającego identyfikacji, tam gdzie administrator nie jest w stanie zidentyfikować podmiotu danych, można odmówić podjęcia żądanego działania.
6. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, przedstawia się tej osobie klauzule informacyjne o treści i w miejscach lub dokumentach wskazanych w załączniku nr 2 do niniejszej Polityki.
7. W przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, przedstawia się jej klauzule informacyjne o treści i w miejscach lub dokumentach wskazanych w załączniku nr 3 do niniejszej Polityki.
8. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane zostały pozyskane, przed dalszym przetwarzaniem informuje osobę której dane dotyczą o tym innym celu oraz udziela jej wszelkich innych stosowanych informacji, o których mowa odpowiednio w pkt. 6 lub 7.
9. Administrator, bez zbędnej zwłoki, informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
10. Administrator zapewnia realizację następujących praw i wolności osób, których dane dotyczą:

## Prawo dostępu przysługujące osobie, której dane dotyczą

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz uzyskania informacji, określających:

- cele przetwarzania;
- kategorie odnośnych danych osobowych;
- informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu.

Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.

Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną równocześnie nie wskazując formy ich przekazania, informacji udziela się drogą elektroniczną.

## Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

## Prawo do bycia zapomnianym

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania jej danych osobowych;
- osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega administrator;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Jeżeli administrator upublicznił dane osobowe, a ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

Prawo do usunięcia danych nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że realizacja prawa do bycia zapomnianym uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
- do ustalenia, dochodzenia lub obrony roszczeń.

## Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Jeżeli zgodnie z żądaniem przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia przetwarzania.

## Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy; oraz
b) przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku prawa do bycia zapomnianym. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Administrator odmawia realizacji prawa do przenoszenia danych w sytuacji, gdy realizacja tego prawa może niekorzystnie wpływać na prawa i wolności innych osób.

## Prawo do sprzeciwu

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, gdy:

- przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie danych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, 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.

Administratorowi nie wolno już przetwarzać danych osobowych w sytuacji skorzystania z prawa do sprzeciwu, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

## IX. Procedura monitorowania sposobu używania sprzętu i oprogramowania

Celem niniejszej procedury jest określenie zasad korzystania ze sprzętu i oprogramowania, które administrator powierzył pracownikom, w celu niezbędnym do prawidłowego wykonywania powierzonych zadań.

1. Administrator wyposażył pracownika w sprzęt, w tym sprzęt komputerowy (dalej „Sprzęt) i oprogramowanie komputerowe (dalej „Oprogramowanie") niezbędne do prawidłowego wykonywania powierzonych zadań. Pracownik w trakcie wykonywania tych zadań może mieć dostęp do informacji stanowiących: tajemnicę, dane osobowe, dane poufne lub dane, co do których administrator zobowiązał się do ich zabezpieczenia przed nieuprawnionym ujawnieniem.

2. Pracownik może korzystać ze Sprzętu i Oprogramowania wyłącznie w celu wykonywania powierzonych obowiązków, zgodnie z obowiązującymi przepisami prawa. Powyższy obowiązek należy do podstawowych obowiązków pracowniczych z uwagi na konieczność dbałości o mienie administratora.

3. Pracownik jest zobowiązany do:
   a) niekorzystania z jakiegokolwiek oprogramowania komputerowego innego niż Oprogramowanie, w szczególności niedokonywania instalacji takiego oprogramowania na Sprzęcie;
   b) niekorzystania ze Sprzętu i Oprogramowania w celach prywatnych, w szczególności poprzez prowadzenie korespondencji e-mail niezwiązanej ze świadczeniem pracy, poprzez korzystanie z komunikatorów, portali społecznościowych, witryn www, innych niż konieczne do wykonywania obowiązków pracowniczych;
   c) niekorzystania z Oprogramowania w sposób mogący naruszyć prawa osób trzecich, w tym niekopiowania i nierozpowszechniania Oprogramowania;
   d) niezwłocznego udostępniania administratorowi, na każde żądanie, Sprzętu i Oprogramowania celem umożliwienia wykonania kontroli, o której mowa w pkt 4 niniejszej Procedury.

4. Administrator może przeprowadzić sprawdzenie należytego wykonania niniejszej polityki. Sprawdzenie może być wykonane przez wyznaczonego pracownika komórki właściwej ds. IT lub Inspektora poprzez:
   a) monitoring operacji wykonywanych na Sprzęcie;
   b) sprawdzanie wykazu połączeń telefonicznych;
   c) kontrolę zainstalowanego Oprogramowania i sposobu korzystania z niego;
   d) kontrolę czasu pracy przy wykorzystaniu Sprzętu i Oprogramowania;
   e) kontrolę aktywności w sieci Internet;
   f) kontrolę wysyłanej poczty służbowej.

5. Bezwzględnie zabronione jest wykorzystywanie Sprzętu lub Oprogramowania w celach niezgodnych z prawem lub zasadami obowiązującymi u administratora, a w szczególności w celach:
   a) korzystania z treści pornograficznych;
   b) naruszania praw autorskich (nielegalnego pobierania bądź udostępniania plików);
   c) infekowania sieci komputerowej wirusami pobieranymi z plikami z Internetu;
   d) korzystania ze służbowej poczty elektronicznej w sprawach prywatnych.

6. W związku z naruszeniem zasad niniejszej polityki pracownik może podlegać odpowiedzialności karnej, o której stanowi ustawa z dnia 6 czerwca 1997 r. Kodeks karny oraz odpowiedzialności karnej i cywilnej przewidzianej w ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie oprogramowania oraz odpowiedzialności karnej określonej w art. 51 ustawy.

7. Naruszenie przez pracownika jego obowiązków pracowniczych w zakresie wskazanym w niniejszej Polityce może stanowić podstawę do podjęcia przez Instytut przysługujących mu środków prawnych, a w szczególności może stanowić przyczynę uzasadniającą wypowiedzenie przez Instytut umowy o pracę łączącej Instytut z pracownikiem lub wymierzenie kary porządkowej przewidzianej przepisami ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.

## X. Procedura nadawania i odbierania upoważnień lub uprawnień

Celem niniejszej procedury jest określenie zasad nadawania upoważnień do przetwarzania danych osobowych oraz uprawnień w systemie informatycznym służącym do przetwarzania danych osobowych.

1. Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, użytkownikom nadaje komórka właściwa ds. IT.

2. Przed nadaniem użytkownikowi dostępu do systemu informatycznego, komórka właściwa ds. kadr odbiera od użytkownika oświadczenie o zachowaniu danych osobowych w poufności, którego wzór stanowi załącznik nr 4 do niniejszej Polityki.

3. Komórka właściwa ds. kadr przygotowuje dwa egzemplarze upoważnienia do przetwarzania danych, którego wzór stanowi załącznik nr 5 do niniejszej Polityki, w zakresie wynikającym z zajmowanego stanowiska.

4. Upoważnienia do przetwarzania danych podpisuje administrator lub osoba posiadająca odrębne pełnomocnictwo administratora.

5. Komórka właściwa ds. kadr prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi załącznik nr 6 do niniejszej Polityki.

6. Wyznaczony pracownik komórki właściwej ds. kadr jest obowiązany niezwłocznie odnotować fakt cofnięcia upoważnienia w ewidencji osób upoważnionych do przetwarzania danych osobowych.

7. Jeden egzemplarz upoważnienia zostaje przekazany pracownikowi za potwierdzeniem odbioru na drugim egzemplarzu, egzemplarz zawierający potwierdzenie odbioru wyznaczony pracownik komórki właściwej ds. kadr załącza do akt osobowych pracownika.

8. Bezpośredni przełożony, po podpisaniu upoważniania przez administratora danych, wypełnia wniosek o nadanie dostępu do systemów i grupy uprawnień, której wzór stanowi załącznik nr 7 do niniejszej Polityki, który niezwłocznie przekazuje komórce właściwej ds. IT.

9. Komórka właściwa ds. IT, niezwłocznie po otrzymaniu od bezpośredniego przełożonego wniosku o nadanie dostępu do systemów i grup uprawnień, przyznaje dostęp do systemu i grupy uprawnień, które zostały przypisane do stanowiska pracy zgodnie z rolą wskazaną we wniosku.

10. Nadanie uprawnień do systemu informatycznego polega na przydzieleniu unikalnego identyfikatora i hasła.

11. Komórka właściwa ds. IT prowadzi ewidencję użytkowników systemu informatycznego, której wzór stanowi załącznik nr 8 do niniejszej Polityki. Ewidencja zawiera w szczególności: identyfikator użytkownika systemu, datę i godzinę nadania oraz odebrania uprawnień.

12. Dostęp do systemów informatycznych służących do przetwarzania danych osobowych, możliwy jest wyłącznie po podaniu unikalnego identyfikatora i hasła. Nadane przez komórkę właściwą ds. IT hasło jest hasłem startowym, które użytkownik jest zobowiązany zmienić na hasło spełniające wymagania, o których mowa w rozdziale X pkt 10.

13. Użytkownik odbiera identyfikator i hasło startowe osobiście od komórki właściwej ds. IT - legitymując się dokumentem ze zdjęciem – potwierdzając tę czynność własnoręcznym podpisem na informacji o zatrudnieniu pracownika.

14. Procedurę nadania uprawnień stosuje się odpowiednio w przypadku zmiany uprawnień.

15. Zmiana uprawnień, w tym odebranie uprawnień może mieć charakter czasowy lub trwały.

16. Odebranie uprawnień następuje przez zablokowanie konta użytkownika.

## XI. Procedura dostępu do danych osobowych

Celem niniejszej procedury jest określenie zasad dostępu do danych osobowych przetwarzanych w systemie informatycznym oraz obowiązków związanych z rozpoczęciem, zawieszeniem i zakończeniem pracy.

1. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu indywidualnego identyfikatora i właściwego hasła. W identyfikatorze pomija się znaki diakrytyczne.

2. W przypadku trzech nieudanych prób uwierzytelnienia hasła, celem zabezpieczenia systemu przed próbą włamania, następuje automatyczne zablokowanie dostępu użytkownika do systemu. Odblokowanie dostępu użytkownika do systemu wymaga interwencji pracownika komórki właściwej ds. IT, który nadaje użytkownikowi nowe hasło startowe.

3. W systemie stosuje się uwierzytelnianie przynajmniej jednostopniowe: na poziomie dostępu do sieci lokalnej. Tam gdzie to możliwe stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji lub programu.

4. Identyfikator użytkownika w aplikacji lub programie (o ile działanie aplikacji lub programu na to pozwala) powinien być tożsamy z tym, jaki jest mu przydzielony w sieci lokalnej.

5. Hasło użytkownika powinno być zmienianie nie rzadziej niż co 90 dni.

6. Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po odebraniu uprawnień użytkownika w systemie informatycznym nie powinien być przydzielony innej osobie.

7. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł. Zabronione jest udostępnianie przez użytkownika swojego identyfikatora i hasła innym osobom, a także korzystanie z identyfikatora i hasła innego użytkownika. Zabrania się również przechowywania haseł w miejscach dostępnych innym osobom, np. pod klawiaturą, na monitorze lub w niezabezpieczonej szafce.

8. Hasło należy wprowadzać do systemu informatycznego w sposób, który uniemożliwia innym osobom jego poznanie.

9. W sytuacji, gdy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do samodzielnej zmiany hasła i powiadomienia o tym incydencie komórki właściwej ds. IT.

10. Hasło powinno składać się z zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika w

jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę itp.), ani jego imieniem lub nazwiskiem.

11. Niedozwolone jest stosowanie haseł, którymi użytkownik posługiwał się uprzednio w okresie minionego roku.

12. Kombinacja hasła nie powinna zwierać ogólnie dostępnych informacji o użytkowniku, np. imienia i nazwiska, numeru telefonu, numeru rejestracyjnego samochodu, marki samochodu lub przewidywanych sekwencji z klawiatury (np.: „QWERTY” i „12345” itp.).

13. Nie należy korzystać z opcji zapamiętywania hasła w systemie.

14. Komórka właściwa ds. IT jest odpowiedzialna za sprawdzenie, a następnie blokowanie zbędnych identyfikatorów użytkowników.

15. Komórka właściwa ds. kadr z chwilą powzięcia informacji o rozwiązaniu umowy z pracownikiem zobowiązana jest niezwłocznie - nie później niż tego samego dnia co jej rozwiązanie - przekazać komórce właściwej ds. IT informacje o zwolnieniu lub zmianie stanowiska, której wzór stanowi załącznik nr 6 do niniejszej Polityki. Informacja może zostać przesłane za pośrednictwem poczty elektronicznej.

16. Po otrzymania informacji o pracowniku o zwolnieniu lub zmianie stanowiska z komórki właściwej ds. kadr, komórka właściwa ds. IT z dniem rozwiązania umowy lub zmiany stanowiska z pracownikiem, odpowiednio odbiera lub zmienia uprawnienia w systemie informatycznym.

17. Hasło administratora systemu przechowywane jest w zamkniętej kopercie w szafie metalowej, do której mają dostęp wyłącznie: dyrektor Instytutu, zastępca dyrektora właściwego ds. administracyjnych oraz kierownik komórki właściwej ds. IT, lub w inny sposób, umożliwiający dostęp do niego wyłącznie dyrektorowi Instytutu, zastępcy dyrektora właściwego ds. administracyjnych oraz kierownika komórki właściwej ds. IT.

18. Rozpoczęcie pracy na stacji roboczej odbywa się po prawidłowym uwierzytelnieniu użytkownika.

19. Każdorazowe zaprzestanie pracy w systemie informatycznym, wymaga zabezpieczenia systemu przed nieuprawnionymm dostępem, np. poprzez zablokowanie stacji roboczej przy użyciu komendy „Ctrl+Alt+Del i Zablokuj Komputer”. Użytkownik jest zobowiązany wyłączyć monitor w sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć osoba nieuprawniona. Na komputerze użytkownika niewykonującego żadnych czynności przez 10 minut zostanie automatycznie uruchomiony wygaszacz ekranu.

20. Użytkownik przed wyłączeniem stacji roboczej i opuszczeniem stanowiska pracy powinien wylogować się z systemu informatycznego oraz sprawdzić, czy nie zostały pozostawione niezabezpieczone elektroniczne nośniki zawierające dane osobowe.

21. Użytkownik udostępniający stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązany jest wylogować się z systemu.

22. Przy przetwarzaniu danych osobowych na komputerach przenośnych stosuje się procedury określone powyżej. Użytkownicy korzystający z komputerów przenośnych zobowiązani są do ochrony ich przed kradzieżą i dostępem osób nieuprawnionych.

## XII. Procedura zabezpieczenia systemu informatycznego

Celem niniejszej procedury jest określenie zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz wirusami komputerowymi.

1. Na każdej stacji roboczej, komputerze przenośnym i serwerze musi być zainstalowane oprogramowanie antywirusowe, które sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

2. Każdy e-mail oraz załączniki muszą być sprawdzone przez program antywirusowy pod kątem obecności wirusów.

3. Definicje wzorców wirusów aktualizowane są nie rzadziej niż raz w miesiącu.

4. Jeżeli oprogramowanie antywirusowe pozwala, to należy ustawić harmonogram zadań tak, aby przynajmniej raz w tygodniu sprawdzał daną jednostkę komputerową pod kątem obecności wirusów.

5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.

6. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.

7. Przeprowadza się cyklicznie kontrole antywirusowe na wszystkich komputerach – minimum co 12 miesięcy.

8. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku stwierdzenia nieprawidłowości, zgłoszonych przez użytkownika, w funkcjonowaniu sprzętu komputerowego lub oprogramowania.

9. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wykryto wirusa, oraz wszystkie posiadane przez użytkownika nośniki.

10. Użytkownik jest obowiązany zawiadomić komórkę właściwą ds. IT o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

11. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.

12. Dostęp do Internetu możliwy jest na wszystkich stacjach roboczych, sieć wewnętrzna jest chroniona centralnym urządzeniem sprzętowym z wbudowanym Firewall.

## XIII. Procedura tworzenia kopii zapasowych

Celem niniejszej procedury jest określenie zasad tworzenia kopii zapasowych danych osobowych przetwarzanych w systemie informatycznym służącym do przetwarzania danych osobowych.

1. Odpowiedzialnym za tworzenie i przechowywanie u administratora kopii zapasowych danych osobowych przetwarzanych w zbiorach danych w sposób zgodny z przepisami prawa oraz poniższymi zasadami jest kierownik komórki właściwej ds. IT.

2. Kopie zapasowe danych osobowych wykonywane są codziennie, w sposób automatyczny i zawierają pełny obraz danych osobowych.

3. Kopie zapasowe przechowuje się odpowiednio zabezpieczone przed dostępem osób nieuprawnionych w innych pomieszczeniach niż serwerownia przez okres 30 dni.

4. Kopie zapasowe danych osobowych przetwarzanych po ustaniu ich użyteczności są bezzwłocznie usuwane.

5. Kopie zapasowe przetwarzanych danych osobowych, które uległy uszkodzeniu, podlegają natychmiastowemu zniszczeniu.

6. Dostęp do kopii zapasowych ma kierownik komórki właściwej ds. IT, Inspektor oraz inne osoby wskazane przez kierownika komórki właściwej ds. IT.

7. Użytkownicy stacji roboczej są zobowiązani do samodzielnego wykonywania kopii zapasowych danych osobowych zapisanych na dysku stacji roboczej. Kopie wykonywane są na nośniku danych typu pendrive.

8. Niniejsza procedura nie ma zastosowania do systemu informatycznego służącego do przetwarzania danych osobowych z użyciem sieci publicznej, oraz których serwery zlokalizowane są poza siedzibą administratora. W takim jednak wypadku konfiguracja ww. serwerów powinna zapewniać wykonywanie kopii zapasowych.

## XIV. Procedura przechowywania elektronicznych nośników informacji

Celem niniejszej procedury jest określenie zasad przechowywania elektronicznych nośników informacji takich jak: pendrive, dyskietka, dysk magnetooptyczny, dysk twardy lub komputer przenośny.

1. Nośniki danych osobowych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieuprawnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).

2. Dane osobowe w postaci elektronicznej – zapisywane na dyskietkach, dyskach magnetooptycznych czy dyskach twardych nie są wynoszone poza siedzibę administratora. Nie dotyczy to komputerów przenośnych, które mogą być wynoszone poza siedzibę administratora.

3. Po zakończeniu pracy przez użytkowników systemu wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych.

4. Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania.

5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób mechaniczny uniemożliwiający ich odczytanie.

6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania danych osobowych, pozbawia się wcześniej zapisu tych danych.

7. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych.

8. W przypadku posługiwania się nośnikami danych pochodzącymi od podmiotu zewnętrznego, użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na swoim komputerze.

9. W przypadku konieczności przechowywania wydruków zawierających dane osobowe, należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym.

10. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

## XV. Procedura wykonywania przeglądów i konserwacji

Celem niniejszej procedury jest określenie zasad wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych.

1. Za bezawaryjną pracę systemu IT, w szczególności serwerów, stacji roboczych, aplikacji serwerowych, baz danych, poczty e-mail – odpowiada komórka właściwa ds. IT.

2. Przeglądu lub konserwacji systemu dokonuje doraźnie komórka właściwa ds. IT.

3. Przegląd lub konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonych przez producenta sprzętu.

4. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada komórka właściwa ds. IT.

5. Nieprawidłowości ujawnione w trakcie dokonywania przeglądu lub konserwacji powinny być niezwłocznie usunięte, a ich przyczyny powinny być przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Inspektora.

6. Przeglądu pliku zawierającego raport dotyczący działalności aplikacji, oprogramowania lub systemów serwerowych (log systemowy) komórka właściwa ds. IT dokonuje nie rzadziej niż raz na miesiąc.

7. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać na zasadach określonych w umowie zawartej pomiędzy administratorem a podmiotem zewnętrznym.

8. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nieposiadające upoważnień do przetwarzania danych osobowych (np. specjalistów z firm zewnętrznych), muszą być wykonywane wyłącznie pod nadzorem osób upoważnionych do przetwarzania danych osobowych.

## XVI. Procedura zarządzania systemem monitoringu wizyjnego

Celem niniejszej procedury jest określenie zasad korzystania i dostępu do systemu monitoringu wizyjnego rejestrującego obraz na terenie siedziby administratora.

1. Celem instalacji monitoringu wizyjnego na terenie siedziby administratora jest zapewnienie bezpieczeństwa osób i mienia.
2. Dyrekcja Instytutu decyduje o zakresie monitoringu wizyjnego oraz jego umiejscowieniu, biorąc pod uwagę między innymi przepisy prawa, ocenę bezpieczeństwa, jak również wnioski kierowników komórek organizacyjnych Instytutu.
3. Przed zainstalowaniem monitoringu wizyjnego, Dyrekcja Instytutu, dokonuje analizy potrzeb i celowości wprowadzenia systemu monitoringu wizyjnego oraz analizy rozmieszczenia kamer pod kątem ingerencji monitoringu w prawo pacjentów do prywatności.
4. Montaż elementów składających się na system monitoringu wizyjnego, przeprowadzony jest po przeanalizowaniu jego umiejscowienia pod kątem poszanowania godności, prywatności i intymności osób przebywających na terenie Instytutu, w szczególnie w czasie udzielania świadczeń zdrowotnych pacjentom.
5. Użytkownicy systemu monitoringu wizyjnego zobowiązani są zapewnić bezpieczeństwo oglądanych przekazów i uniemożliwić dostęp do nich osobom nieuprawnionym.
6. Monitoring wizyjny swym zasięgiem nie obejmuje drogi publicznej.
7. Czas przechowywania uzależniony jest od ilości wolnego miejsca na dyskach twardych rejestratora, jednakże nie przekracza okresu 14 dni.
8. Wykaz kamer systemu monitoringu, bez włączonej funkcji rejestracji, oraz z włączoną funkcją rejestracji obrazu prowadzi komórka właściwa ds. administracji. Wzór wykazu stanowi załącznik nr 18 do niniejszej Polityki.
9. W miejscach objętych monitoringiem zamieszczone są klauzule informacyjne o następującej treści:
   *„Monitoring wizyjny prowadzony jest przez Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa, w celu zapewnienie bezpieczeństwa i porządku publicznego oraz ochrony osób i mienia i obejmuje ….(dokładne wskazanie obszaru). Więcej informacji można uzyskać telefonicznie pod numerem telefonu …., lub drogą elektroniczną …. (podanie adresu poczty elektronicznej)”*

## XVII. Procedura udostępnienia danych

Celem niniejszej procedury jest określenie zasad udostępniania danych osobom, których dane dotyczą, a także organom publicznym, które wnioskują o udostępnienie danych osobowych w ramach prowadzonego przez te organy postępowania. Procedura nie ma zastosowania do udostępniania dokumentacji medycznej, które jest uregulowane odrębnymi przepisami wewnętrznymi.

10. Dane osobowe udostępnia się na pisemny wniosek, chyba że przepis innej ustawy stanowi inaczej.

11. W przypadku wniosku o udostępnienie danych, każda osoba, do której wpłynie taki wniosek, a która ma uzasadnione wątpliwości czy udostępnienie danych będzie zgodne z przepisami prawa, jest zobowiązana przekazać wniosek do Inspektora.

12. Inspektor rozpatruje przekazany wniosek oraz ustala czy wniosek o udostępnienie:
    a. jest sporządzony w formie pisemnej;
    b. wystarczająco identyfikuje osobę, której dane mają być udostępnione;
    c. wskazuje odpowiednią podstawę prawną udostępnienia danych;
    d. określa zakres danych osobowych, których wniosek o udostępnienie danych osobowych dotyczy.

13. Inspektor ocenia, czy można legalnie udostępnić dane osobowe i podejmuje decyzję, którą następnie administrator przekazuje odbiorcy wniosku.

14. W razie braków formalnych wniosku o udostępnienie danych osobowych, administrator zwraca się do wnioskodawcy o ich usunięcie we wskazanym terminie pod rygorem pozostawienia wniosku bez rozpoznania.

15. Po uzyskaniu pozytywnej opinii od Inspektora w przedmiocie dopuszczalności udostępnienia danych osobowych, administrator bez zbędnej zwłoki udostępnia dane osobowe.

16. Dane osobowe powinny być udostępnione w sposób zapewniający ich poufność wobec osób postronnych.

17. Po uzyskaniu negatywnej opinii od Inspektora w przedmiocie dopuszczalności udostępnia danych osobowych, administrator nie udostępnia danych osobowych.

18. Udostępnienie dokumentacji medycznej, o której mowa w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, odbywa się na podstawie odrębnych regulacji wewnętrznych.

## XVIII. Procedura udostępniania uczelni dokumentacji medycznej

Celem niniejszej procedury jest określenie zasad udostępniania uczelni lub instytutowi badawczemu dokumentacji medycznej Instytutu oraz przeprowadzania przez studentów, doktorantów lub słuchaczy badań ankietowych i testowych na terenie Instytutu.

1. Warunkiem udostępnienia szkole wyższej lub instytutowi badawczemu materiałów dokumentacji medycznej Instytutu jest złożenie wniosku Rektora, Dziekana lub uprawnionego przedstawiciela jednostki, zawierającego w szczególności:
   a) pieczęć jednostki,
   b) dane studenta, doktoranta lub słuchacza,
   c) wskazanie przeznaczenia udostępnionych danych,
   d) zakres wnioskowanych informacji,
   e) data i podpis Rektora, Dziekana lub uprawnionego przedstawiciela jednostki, wzór wniosku stanowi załącznik nr 15 do niniejszej Polityki.

2. Zgodnie z art. 26 pkt 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta udostępnienie dokumentacji następuje bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy.

3. W przypadku uzyskania przez studenta, doktoranta lub słuchacza upoważnienia do wglądu i wykorzystania dokumentacji medycznej udzielonego przez pacjenta, którego dokumentacja medyczna dotyczy lub przedstawiciela ustawowego pacjenta, którego dokumentacja dotyczy, dokumentacja udostępniania jest bezpośrednio na wniosek zainteresowanego wraz z załączonym upoważnieniem. Udostępnienie dokumentacji następuje z ujawnianiem nazwiska i innych danych umożliwiających identyfikację pacjenta, którego dokumentacja dotyczy, chyba że pacjent udzielający upoważnienia zastrzeże inaczej.

4. Udostępnienie dokumentacji może nastąpić w postaci kserokopii, odpłatnie – zgodnie z obowiązującym w Instytucie cennikiem. Udostępnienie dokumentacji następuje po podpisaniu przez studenta, doktoranta lub słuchacza oświadczenia, którego wzór stanowi załącznik nr 16 do niniejszej Polityki.

5. W przypadku udostępnienia dokumentacji do wglądu konieczne jest podpisanie przez studenta, doktoranta lub słuchacza oświadczenia, którego wzór stanowi załącznik nr 17 do niniejszej Polityki.

6. Warunkiem udostępnienia danych statystycznych lub umożliwienia studentom, doktorantom lub słuchaczom przeprowadzenia badań ankietowych lub testów wśród personelu Instytutu, pacjentów lub ich rodzin, jest złożenie przez zainteresowanego wniosku zawierającego w szczególności:
   a) dane studenta, doktoranta lub słuchacza,

b) wskazanie przeznaczenia udostępnionych danych,
c) zakres wnioskowanych informacji,
d) potwierdzenie Rektora, Dziekana lub uprawnionego przedstawiciela jednostki, zgodności danych zawartych we wniosku, poprzez złożony na wniosku podpis opatrzony datą.

7. Instytut prowadzi rejestr wniosków dotyczących udostępniania dokumentacji medycznej oraz przeprowadzania badań ankietowych lub testów.

## XIX. Procedura powierzania przetwarzania danych osobowych

Celem niniejszej procedury jest określenie zasad i zapewnienie, że administrator korzysta z usług podmiotów przetwarzających, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.

1. Administrator dokłada należytej staranności, by przetwarzanie danych osobowych przez podmiot przetwarzający odbywało się na podstawie pisemnej umowy między administratorem a podmiotem przetwarzającym, której wzór stanowi załącznik nr 10 do niniejszej Polityki.

2. Podmiot przetwarzający, któremu administrator powierzył przetwarzanie danych osobowych, nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody administratora.

3. W umowie powierzenia przetwarzania danych osobowych należy zastrzec, że podmiot przetwarzający ma obowiązek poinformować administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

4. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy, która określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

5. Umowa powierzenia przetwarzania danych osobowych stanowi w szczególności, że podmiot przetwarzający:
   a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
   b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   c) podejmuje wszelkie środki by uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku;
   d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego;
   e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw;
   f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków nałożonych na administratora w RODO;
   g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo nakazuje przechowywanie danych osobowych;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w umowie oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

6. Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający na mocy umowy powinny zostać nałożone te same obowiązki ochrony danych jak w umowie między administratorem a podmiotem przetwarzającym.

7. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego powinna spoczywać na pierwotnym podmiocie przetwarzającym.

## XX. Procedura przeprowadzania szkoleń pracowniczych

Celem niniejszej procedury jest określenie zapewnienia realizacji zadania Inspektora Ochrony Danych jakim jest informowanie pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów z zakresu ochrony danych osobowych, a także na mocy niniejszej Polityki.

1. Każda osoba upoważniona do przetwarzania danych osobowych, przed dopuszczeniem do pracy, jest poddawana szkoleniu stanowiskowemu, które przeprowadza jego bezpośredni przełożony lub osoba wyznaczona przez bezpośredniego przełożonego.

2. Szkolenie stanowiskowe obejmuje zaznajomienie pracownika z regulacjami wewnętrznymi obowiązującymi u administratora, w tym z niniejszą Polityką, a także omówienie sposobu bezpiecznego postępowania z danymi osobowymi.

3. Przynajmniej raz w roku Inspektor przeprowadza szkolenia grupowe dla wszystkich pracowników, którzy przetwarzają dane osobowe. Szkolenie obejmuje swym zakresem omówienie obowiązków spoczywających na pracownikach przetwarzających dane osobowe na mocy RODO oraz innych przepisów z zakresu ochrony danych osobowych, a także na mocy niniejszej Polityki.

4. Administrator zapewnia odpowiednie warunki do przeprowadzenia szkoleń grupowych.

5. Pracownicy potwierdzają swój udział w szkoleniu własnoręcznym podpisem na liście obecności, którą przechowuje komórka właściwa ds. kadr.

## XXI. Procedura zgłaszania incydentów

Procedura definiuje katalog zagrożeń i incydentów mogących prowadzić do naruszenia bezpieczeństwa danych osobowych przetwarzanych przez administratora (również tych danych, które zostały powierzone na rzecz administratora przez inny podmiot) oraz sposób reagowania na ww. zagrożenia i incydenty.

Celem opracowania procedury jest ograniczenie skutków wystąpienia incydentów godzących w bezpieczeństwo przetwarzania danych osobowych oraz zmniejszenie ryzyka ich powstania w przyszłości.

Procedura dzieli się na:
1. Postępowanie wewnętrzne;
2. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu;
3. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

**Postępowanie wewnętrzne**

1. Każdy pracownik administratora, w przypadku stwierdzenia zagrożenia lub podejrzenia naruszenia zasad ochrony danych osobowych, zobowiązany jest do niezwłocznego zgłoszenia o ww. okolicznościach bezpośredniego przełożonego lub komórkę właściwą ds. IT. Bezpośredni przełożony lub pracownik komórki właściwej ds. IT w przypadku powzięcia powyższej informacji zobowiązany jest do jej niezwłocznego przekazania Inspektorowi.

2. Rodzaje najczęściej występujących zagrożeń bezpieczeństwa danych osobowych:
    a. niewłaściwe zabezpieczenie stacji roboczych, komputerów przenośnych, tabletów, smartphonów, nośników przenośnych oraz oprogramowania IT przed kradzieżą, zniszczeniem lub utratą danych osobowych;
    b. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń oraz dokumentów;
    c. nieprzestrzeganie przyjętych zasad ochrony danych osobowych przez upoważnione osoby.

3. Przykładowe incydenty naruszające zasadę bezpieczeństwa danych osobowych:
    a. incydenty losowe zewnętrzne np. pożar obiektu lub pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;
    b. incydenty losowe wewnętrzne np. awarie stacji roboczych, awarie serwera, awarie oprogramowania, utrata lub zgubienie danych zawartych na nośnikach przenośnych;
    c. incydenty umyślne np. ataki hakerskie, włamania do pomieszczeń, celowe i świadome zniszczenie dokumentów, szkodliwe oprogramowanie.

4. W przypadku podejrzenia wystąpienia zagrożenia lub incydentu Inspektor w porozumieniu z kierownikiem komórki właściwej ds. IT prowadzi postępowanie wstępne, w toku którego:

a. ustala zakres i przyczyny zagrożenia lub incydentu oraz jego ewentualne skutki;
b. inicjuje ewentualne postępowanie dyscyplinarne;
c. rekomenduje działania prewencyjne zmierzające do eliminacji podobnych zagrożeń lub incydentów w przyszłości;
d. dokumentuje prowadzone postępowanie;
e. przedstawia raport z przeprowadzonego postępowania administratorowi.

5. W przypadku stwierdzenia poważnego incydentu lub powzięcia uzasadnionej informacji o podejrzeniu poważnego naruszenia zasad ochrony danych osobowych, Inspektor informuje administratora o konieczności zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

6. Oceny, czy występuje ryzyko naruszenia praw lub wolności człowieka, administrator dokonuje we współpracy z Inspektorem. Ocena powinna być oparta na obiektywnych kryteriach, jak dotychczasowe doświadczenie związane z podobnymi naruszeniami lub wiedza z zakresu bezpieczeństwa informacji, oraz na uwzględnieniu okoliczności samego naruszenia ochrony danych osobowych.

7. W toku dokonywania oceny, o której mowa w pkt. 6 administrator bierze pod uwagę wszelkie możliwe szkody, jak i krzywdy, które mogą wyniknąć dla osób fizycznych z danego naruszenia. Mogą one w szczególności polegać na:
   - utracie kontroli nad własnymi danymi osobowymi,
   - negatywnych konsekwencjach wizerunkowych,
   - możliwości zawierania przez inną osobę umów z wykorzystaniem danych osobowych innej osoby fizycznej,
   - stratach finansowych,
   - negatywnym odbiorze społecznym, który może być konsekwencją upublicznienia niektórych danych osobowych.

8. W przypadku stwierdzenia poważnego incydentu lub powzięcia uzasadnionej informacji o podejrzeniu poważnego naruszenia zasad ochrony danych osobowych Inspektor, niezależenie od pkt 5, niezwłocznie rozpoczyna audyt doraźny. W ramach czynności audytowych Inspektor:
   a. określa sposób dokumentowania audytu, a w jego ramach:
      - sporządza notatki z czynności audytowych, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
      - odbiera pisemne wyjaśnienia osoby, której czynności objęto audytem;
      - sporządza kopie okazanych dokumentów;

- sporządza kopię obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
- sporządza kopie zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

b. zabezpiecza ewentualne dowody związane z incydentem;
c. ustala osoby odpowiedzialne za powstanie incydentu;
d. wskazuje możliwe sposoby przywrócenia stanu zgodnego z prawem;
e. wnioskuje o wszczęcie postępowań dyscyplinarnych;
f. przygotowuje raport dla administratora.

9. Inspektor zawiadamia administratora o rozpoczęciu audytu doraźnego przed podjęciem pierwszej czynności w toku audytu.

10. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta powinna pozwolić organowi nadzorczemu na zweryfikowanie przestrzegania niniejszej Procedury.

11. Inspektor prowadzi rejestr incydentów, którego wzór stanowi załącznik nr 11 do niniejszej Polityki.

## Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. W sytuacji, gdy naruszenie dotyczy danych osobowych osób fizycznych, których Instytut nie jest administratorem, a podmiotem przetwarzającym, któremu na podstawie art. 28 RODO zostały dane powierzone, to po stwierdzeniu naruszenia ochrony danych osobowych Instytut, bez zbędnej zwłoki, zgłasza naruszenie podmiotowi, który dane Instytutowi powierzył.

3. Zgłoszenie, o którym mowa w pkt. 1, zawiera co najmniej:
   a) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorii i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b) imię i nazwisko oraz dane kontaktowe Inspektora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
d) opisy środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach opis środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

## Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych.

2. Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej następujące informacje i środki:
   a) imię i nazwisko oraz dane kontaktowe Inspektora lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   b) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
   c) opisy środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach opis środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

3. Zawiadomienie nie jest wymagane, w następujących przypadkach:
   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;
   c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku administrator wyda publiczny komunikat lub zastosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

## XXII. Procedura zarządzania ryzykiem

Procedura zarządzania ryzykiem to szereg skoordynowanych działań podejmowanych przez dyrekcję Instytutu, kierowników poszczególnych komórek organizacyjnych, jak i pozostałych pracowników oraz współpracowników Instytutu, którzy poprzez identyfikację i analizę ryzyka oraz określanie adekwatnych reakcji na ryzyko zwiększają poziom bezpieczeństwa przetwarzania danych osobowych w ramach poszczególnych procesów ich przetwarzania.

1. W ramach powyższych działań dla zidentyfikowanych procesów przetwarzania danych osobowych (tabela nr 1) zostaną wskazane, przeanalizowane i oszacowane:
   1) **Zasoby** – które będziemy chronić:
      a) sprzęt komputerowy przechowujący dane,
      b) dane osobowe przetwarzane w formie papierowej i elektronicznej,
      c) prawa i wolności osób fizycznych, których dane dotyczą,
      d) aplikacje, w których przetwarzane są dane osobowe,
      e) pomieszczenia, w których pracują osoby upoważnione do przetwarzania danych osobowych;
   2) **Zastosowane środki bezpieczeństwa** – zastosowane środki techniczne i organizacyjne, opisane w niniejszej Polityce;
   3) **Zagrożenia** – zdarzenia, które można wyróżnić ze względu na utratę poufności, dostępności, integralności i rozliczalności przetwarzanych danych osobowych mogące powodować wystąpienie incydentu;
   4) **Podatności** – słabości zasobów, które mogą być wykorzystane przez potencjalne zagrożenia;
   5) **Skutki** – wpływ jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych.

2. Mając na uwadze powyższe administrator zapewnia warunki pracy systemach informatycznych zapewniające poufność, dostępność, integralność i rozliczalność przetwarzanych danych osobowych.

3. Administrator jest zobowiązany dostosować środki bezpieczeństwa zarówno techniczne, fizyczne, jak i organizacyjne do wyników przeprowadzonej analizy ryzyka.

4. Zmiany związane z pkt. 3 należy każdorazowo zaktualizować w Polityce ochrony danych osobowych.

5. Administrator wykazał zidentyfikowane zagrożenia, podatności oraz skutki związane z utratą poufności, dostępności, integralności i rozliczalność przetwarzanych danych osobowych w tabeli nr 2 do niniejszej procedury. W powyższej klasyfikacji zostały uwzględnione zagrożenia wewnętrzne (np. działanie pracownika, awaria systemu spowodowana brakiem zasilania) i zewnętrzne (np. atak hakerski) mogące być następstwem działań (umyślnych lub nieumyślnych) człowieka lub wynikające z przyczyn naturalnych (środowiskowych).

6. Zidentyfikowane zagrożenia, podatności oraz skutki, o których mowa w pkt. 5, podlegają obiektywnej analizie mającej na celu oszacowanie tzw. istotności ryzyka. Na potrzeby niniejszej procedury poziomem istotności ryzyka (tabela nr 5, która obrazuje macierz ryzyka) jest iloczyn oceny prawdopodobieństwa wystąpienia danego ryzyka (tabela nr 3) oraz oceny jego skutku (tabela nr 4).

7. Istotność konkretnego ryzyka określa czy jego poziom jest akceptowalny (tabela nr 6). Ustala się, że ryzykiem:
   - akceptowalnym jest ryzyko na poziomie 3 i poniżej. Przy tym poziomie ryzyka podjęcie dodatkowych działań ograniczających wystąpienie zagrożenia może nastąpić w okresie dłuższym niż w ciągu roku, w zależności od możliwości i koniecznych nakładów finansowych.
   - nieakceptowalnym jest ryzyko na poziomie od 4 – 16. Przy tym poziomie ryzyka konieczne jest zastosowanie dodatkowych mechanizmów kontrolnych (wdrażane są adekwatne, skuteczne i efektywne działania zaradcze), z uwzględnieniem sposób postępowania określonych w pkt. 8 niniejszej procedury.

8. U administratora przyjmuje się następujące sposoby postępowania z ryzykiem:
   a) przeniesienie ryzyka – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta, przy czym należy pamiętać, że przeniesienie ryzyka nie eliminuje go,
   b) akceptacja ryzyka – świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu administratora, w szczególności gdy koszty podjętych ewentualnych działań mogą przekroczyć przewidywane korzyści,
   c) redukcja ryzyka – polega na obniżeniu poziomu ryzyka do poziomu akceptowalnego poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenia skutków jego wystąpienia np. poprzez zwiększenie mechanizmów kontroli (procedury, wytyczne, zasadny, nadzór),
   d) unikanie ryzyka – polega na unikaniu przez administratora działań, które powodują powstanie określonych zagrożeń np. w przypadku gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatnych do przewidywanych korzyści.

9. Identyfikację i analizę ryzyka przeprowadza się na bieżąco jako element systematycznego działania. Identyfikację i analizę ryzyka przeprowadza się okresowo, co najmniej raz w roku, w sposób udokumentowany, odnosząc się do obecnych oraz nowo zidentyfikowanych procesów przetwarzania danych osobowych.

10. Za każde zidentyfikowane ryzyko, w tym za sposób postępowania odnośnie tego ryzyka odpowiedzialna jest osoba mająca uprawnienia wystarczające do zapewnienia efektywnego zarządzania ryzkiem w ramach zidentyfikowanego procesu przetwarzania, tj. właściciel ryzyka.

11. Właściciel ryzyka w zakresie wykonywanych zadań ponosi odpowiedzialność za:
    - przeprowadzanie i dokumentowanie identyfikacji i analizy ryzyka,
    - podejmowane decyzje o zakresie i sposobie zarządzania ryzykiem,
    - bezzwłoczne zgłoszenie bezpośredniemu przełożonemu ryzyka, które nie jest akceptowane i które wymaga zastosowania dodatkowych mechanizmów kontrolnych oraz wskazania konkretnych działań zaradczych ograniczających wystąpienie ryzyka i jego skutków.

12. Inspektor w ramach niniejszej procedury odpowiada za:
    - nadzór nad przestrzeganiem procedury, a w szczególności nad dokumentowaniem identyfikacji i analizy ryzyka,
    - rozstrzyganie kwestii spornych w zakresie stosowanej metodyki zarządzania ryzykiem.

13. Podstawową dokumentację identyfikacji i analizy ryzyka stanowi arkusz ryzyk zagrażających bezpieczeństwu przetwarzania danych osobowych u administratora zwany dalej „arkuszem ryzyk" (tabela nr 7).

14. Formularz arkusza ryzyk przekazywany jest przez Inspektora do właścicieli ryzyk w postaci elektronicznej w terminach uzgodnionych z Dyrekcją Instytutu.

15. Wypełniony przez właściciela ryzyk arkusz ryzyk przekazywany jest Inspektorowi w postaci papierowej zawierającej datę sporządzenia i podpis właściciela ryzyka.

16. Inspektor konsoliduje wyniki analizy ryzyk i przedstawia je Dyrekcji Instytutu wraz z propozycją postępowania z ryzykiem.

17. Jeżeli na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka (patrz tabela nr 6), zgodnie z art. 35 RODO przeprowadza się dla danego procesu przetwarzania ocenę jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane. Przy czym podczas przeprowadzania oceny skutków dla ochrony danych bierze się pod uwagę nie interesy administratora, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.

18. Niniejsza procedura podlega raz na rok przeglądowi i w przypadku konieczności aktualizacji. Przeglądu i aktualizacji procedury dokonuje Inspektor przy współpracy z kierownikiem komórki właściwej ds. IT.

**Tabela nr 1 do Procedury zarządzania ryzykiem**

| PROCESY | CZYNNOŚCI |
|---|---|
| Proces rekrutacji pracowników i współpracowników | Czynności związane z przeprowadzeniem rekrutacji wraz z wyłonieniem kandydata |
| | Czynności związane z dopuszczeniem kandydata do pracy lub nawiązaniem współpracy |
| | Czynności związane z archiwizacją dokumentacji |
| Proces obsługi pracowników i współpracowników, w tym byłych pracowników i współpracowników | Czynności związane z nawiązaniem zatrudnienia lub podpisaniem umowy o współpracę |
| | Czynności związane z bieżąca obsługa pracowników |
| | Czynności związane z bieżąca obsługa współpracowników |
| | Czynności związane z bieżąca obsługa byłych pracowników |
| | Czynności związane z bieżąca obsługa byłych współpracowników |
| | Czynności związane z realizacją świadczeń socjalnych |
| | Czynności związane z archiwizacją dokumentacji |
| Proces realizacji dostawy usług świadczonych na rzecz administratora | Czynności związane z szacowanie wartości zamówienia |
| | Czynności związane z zawarciem umowy |
| | Czynności związane z realizacją umowy |
| | Czynności związane z dochodzeniem roszczeń |
| | Czynności związane z archiwizacją dokumentacji |
| Proces obsługi korespondencji i osób kontaktujących się z administratorem | Czynność rejestracji korespondencji przychodzącej i wychodzącej |
| | Czynności związane z obiegiem dokumentów |
| | Czynności związane z telefoniczną obsługą osób kontaktujących się |
| | Czynności związane z archiwizacją dokumentacji |
| Proces obsługi finansowej i księgowej | Czynności związane z realizacją zobowiązań finansowych |
| | Czynności związane z windykacją należności |
| | Czynności związane z archiwizacją dokumentacji |
| Udzielanie świadczeń zdrowotnych Pacjentom | Czynności związane z rejestracją pacjenta |
| | Czynności związane z przyjęciem pacjenta na oddział lub przyjęciem do poradni |
| | Czynności związane z pobraniem materiału do badań lub wykonaniem badania |
| | Czynności związane z odbiorem wyników badań |
| | Czynności związane z prowadzeniem dokumentacji medycznej pacjentów i byłych pacjentów |
| | Czynności związane z wypisaniem lub przeniesieniem pacjenta z oddziału |
| | Czynności związane z rozliczeniem pacjentów z NFZ |

| | |
|---|---|
| | Czynności związane z rejestracją wniosków o udostępnienie dokumentacji medycznej |
| | Czynności związane z przygotowaniem wnioskowanej dokumentacji medycznej do udostępnienia |
| | Czynności związane z wydanie dokumentacji medycznej lub wyników badań |
| Proces związany z zabezpieczeniem osób i mienia | Czynności związane z obsługą monitoringu wizyjnego |
| | Czynności związane z udostępnieniem zapisu z monitoringu wizyjnego |
| | Czynności związane z archiwizacją zapisu |

**Tabela nr 2 do Procedury zarządzania ryzykiem**

| | Zagrożenie | Podatności (słabości) | Skutki |
|---|---|---|---|
| **POUFNOŚĆ, DOSTĘPNOŚĆ, INTEGRALNOŚĆ LUB ROZLICZALNOŚĆ** | nieuprawniony dostęp do danych osobowych | • awaria sprzętu,<br>• atak wirusa,<br>• odcięcie zasilania,<br>• pożar,<br>• zalanie,<br>• kradzież nośników danych,<br>• nieprzestrzeganie wewnętrznych regulacji,<br>• przekroczenie uprawnień,<br>• brak umowy powierzenia,<br>• brak okresowych szkoleń z zakresu ochrony danych osobowych<br>• brak zabezpieczeń fizycznych,<br>• instalowanie nielegalnego oprogramowania,<br>• niefrasobliwość pracowników lub współpracowników,<br>• brak wyciągania konsekwencji za przekroczenie uprawnień,<br>• niestosowanie się do przyjętych regulacji,<br>• niewystarczającym poziom świadomości pracowników lub współpracowników,<br>• nieprzestrzeganie zasad czystego biurka i pulpitu,<br>• wynoszenie nośników danych poza siedzibę administratora, | • wyciek, utrata, zniszczenie lub uszkodzenie danych osobowych,<br>• straty wizerunkowe,<br>• straty finansowe,<br>• odpowiedzialność dyscyplinarna, karna lub kontraktowa,<br>• naruszenie praw i wolności osób, których dane dotyczą,<br>• przetwarzanie danych osobowych niezgodne z prawem,<br>• przetwarzanie nieaktualnych danych osobowych,<br>• naruszenie zasady minimalizacji danych; |
| | niepożądana modyfikacja danych osobowych | | |
| | udostępnianie informacji osobom nieuprawnionym | | |
| | zniszczenie danych | | |

| | | | |
|---|---|---|---|
| | utrata danych | • pozostawianie osób trzecich bez nadzoru,<br>• brak legalnego oprogramowania,<br>• brak odpowiedniego nadzoru nad oprogramowaniem,<br>• brak świadomości najwyższego kierownictwa,<br>• niewystarczające nakłady finansowe,<br>• nienależyte niszczenie dokumentacji;<br>• używanie sprzętu i oprogramowania do celów prywatnych,<br>• niewystarczający nadzór nad dokumentacją archiwalną,<br>• brak reakcji na żądanie sprostowania danych osobowych;<br>• uniemożliwienie dostępu do danych osobowych osobom, których dane dotyczą; | |
| | przetwarzanie danych osobowych nieadekwatnych do realizacji celu | | |
| | przetwarzanie danych osobowych po upływanie okresu niezbędnego do realizacji celu | | |

**Tabela nr 3 do Procedury zarządzania ryzykiem**

| SKALA OCEN PRAWDOPODOBIEŃSTWA | | OPIS (pomocniczo) |
|---|---|---|
| **NISKIE** | **1** | Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, ale **w ostatnim okresie nie wystąpiło.** |
| **ŚREDNIE** | **2** | Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, i **w ostatnim okresie wystąpiło raz.** |
| **WYSOKIE** | **3** | Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, i **w ostatnim okresie wystąpiło 2 lub 3 razy.** |
| **BARDZO WYSOKIE** | **4** | Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, i **w ostatnim okresie wystąpiło częściej niż 3 razy.** |

**Tabela nr 4 do Procedury zarządzania ryzykiem**

| SKALA OCEN SKUTKU | | OPIS |
|---|---|---|
| **NISKI** | **1** | Zagrożenie objęte ryzykiem **ma niewielki wpływ** na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka:<br>• w dłuższym okresie czasu może spowodować niewielkie straty materialne,<br>• nie powoduje strat lub powoduje minimalne straty lub koszty finansowe,<br>• nie wpływa na prawa i wolności osób fizycznych, których dane dotyczą,<br>• nie wpływa na wizerunek administratora. |
| **ŚREDNI** | **2** | Zagrożenie objęte ryzykiem **ma umiarkowany wpływ** na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka:<br>• może spowodować w okresie roku niewielkie straty materialne lub koszty finansowe,<br>• stanowi naruszenie wewnętrznych regulacji,<br>• ma znikomy wpływ na prawa i wolności osób fizycznych, których dane dotyczą,<br>• ma niewielki wpływa na wizerunek administratora. |
| **WYSOKI** | **3** | Zagrożenie objęte ryzykiem **ma duży wpływ** na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka:<br>• może spowodować w krótkim okresie czasu znaczące straty materialne lub koszty finansowe,<br>• stanowi naruszenie wewnętrznych regulacji,<br>• może stanowić naruszenie przepisów prawa, a brak reakcji może rodzić odpowiedzialność administracyjną lub cywilną,<br>• ma wysoki wpływ na prawa i wolności osób fizycznych, których dane dotyczą,<br>• może powodować zakłócenia w funkcjonowaniu administratora,<br>• ma duży wpływa na wizerunek administratora. |
| **BARDZO WYSOKI** | **4** | Zagrożenie objęte ryzykiem **ma bardzo duży wpływ** na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka:<br>• powoduje znaczące straty materialne lub koszty finansowe,<br>• stanowi naruszenie przepisów prawa, a brak reakcji rodzi odpowiedzialność administracyjną, karną lub cywilną,<br>• ma bardzo wysoki wpływ na prawa i wolności osób fizycznych, których dane dotyczą,<br>• destabilizuje pracę administratora,<br>• wywołuje zdecydowanie negatywną reakcje publiczną, w mediach w całym kraju. |

**Tabela nr 5 do Procedury zarządzania ryzykiem**

| | | | **SKUTEK** | | | |
|---|---|---|---|---|---|---|
| | | | Niski | Średni | Wysoki | Bardzo wysoki |
| | | | **1** | **2** | **3** | **4** |
| **PRAWDOPODOBIEŃSTWO** | Niskie | **1** | | | | |
| | Średnie | **2** | | | | |
| | Wysokie | **3** | | | | |
| | Bardzo wysokie | **4** | | | | |

**Tabela nr 6 do Procedury zarządzania ryzykiem**

| **Poziom ryzyka** | **Opis działania** |
|---|---|
| Niski **(N)** | Poziom ryzyka akceptowalny – działania może zostać przesunięte w czasie i nie wymaga monitorowania |
| Średni **(Ś)** | Poziom ryzyka nieakceptowalny – działania może zostać przesunięte w czasie, wymaga okresowego monitorowania |
| Wysoki **(W)** | Poziom ryzyka nieakceptowalny – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania |
| Krytyczny **(K)** | Poziom ryzyka nietolerowany – wymaga natychmiastowego działania |

**Tabela nr 7 do Procedury zarządzania ryzykiem**

| **Arkusz ryzyk zagrażających bezpieczeństwu przetwarzania danych osobowych** | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **Symbol komórki organizacyjnej** | **Proces przetwarzania** | **Czynność przetwarzania** | **Zagrożenia** | **Ocena prawdopodobieństwa** | **Ocena skutku** | **Poziom istotności** | **Sposób postępowania z ryzykiem** |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## XXIII. Procedura oceny skutków

Celem niniejszej procedury jest zapewnienie realizacji obowiązków wynikających z art. 35 RODO, tj. ustalenie zasad wykonywania oceny skutków dla ochrony danych osobowych.

1. Jeżeli na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka (patrz tabela nr 6 do Procedury zarządzani ryzykiem), zgodnie z art. 35 RODO przeprowadza się dla danego procesu przetwarzania ocenę jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane.

2. Przeprowadzając ocenę skutków dla ochrony danych bierze się pod uwagę nie interesy administratora, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.

3. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, przed rozpoczęciem tego przetwarzania dokonuje się oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

4. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z Inspektorem m.in. kwestie dotyczące:
   - konieczności przeprowadzenia oceny skutków dla ochrony danych;
   - metodologii przeprowadzenia oceny skutków dla ochrony danych;
   - decyzji, czy przeprowadzić wewnętrzną ocenę, czy też zlecić ją podmiotowi zewnętrznemu;
   - zabezpieczeń, w tym środków technicznych i organizacyjnych, stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
   - prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO, w szczególności czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy zastosować.

5. W sytuacji, gdy administrator nie zgadza się z zaleceniami Inspektora, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia tych zaleceń.

6. Ocenę skutków, której formularz stanowi załącznik nr 19 do niniejszej Polityki – z wyłączeniem oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą – dokonuje się także w razie:
   a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
   b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa; lub
   c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

7. Ocena skutków zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą; oraz
d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

8. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, Inspektor dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

9. Administrator ustala następujący sposób oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą:

1) Administrator wykazał zidentyfikowane możliwe skutki związane z naruszenia praw lub wolności osób, których dane dotyczą w tabeli nr 1 do niniejszej procedury.

2) Zidentyfikowane skutki podlegają obiektywnej analizie mającej na celu oszacowanie tzw. istotności ryzyka naruszenia praw w wolności osób, których dane dotyczą. Na potrzeby niniejszej procedury poziomem istotności ryzka jest iloczyn (tabela nr 4, która obrazuje macierz ryzyka) oceny prawdopodobieństwa wystąpienia danego ryzyka (tabela nr 2) oraz oceny jego skutku (tabela nr 3).

3) Istotność konkretnego ryzyka określa czy jego poziom jest akceptowalny (tabela nr 5). Ustala się, że ryzykiem:
   - akceptowalnym jest ryzyko na poziomie 3 i poniżej. Przy tym poziomie ryzyka podjęcie dodatkowych działań ograniczających wystąpienie zagrożenia może nastąpić w okresie dłuższym niż w ciągu roku, w zależności od możliwości i koniecznych nakładów finansowych.
   - nieakceptowalnym jest ryzyko na poziomie od 4 – 16. Przy tym poziomie ryzyka konieczne jest zastosowanie dodatkowych mechanizmów kontrolnych.

4) U administratora przyjmuje się następujące sposoby postępowania z ryzykiem związanym z naruszeniem praw i wolności osób, których dane dotyczą:
   a) przeniesienie ryzyka – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta, przy czym należy pamiętać, że przeniesienie ryzyka nie eliminuje go,
   b) akceptacja ryzyka – świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu administratora, w szczególności gdy koszty podjętych ewentualnych działań mogą przekroczyć przewidywane korzyści,
   c) redukcja ryzyka – polega na obniżeniu poziomu ryzyka do poziomu akceptowalnego poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub

zmniejszenia skutków jego wystąpienia np. poprzez zwiększenie mechanizmów kontroli (procedury, wytyczne, zasadny, nadzór),

d) unikanie ryzyka – polega na unikaniu przez administratora działań, które powodują powstanie określonych zagrożeń np. w przypadku gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatnych do przewidywanych korzyści.

5) Podstawową dokumentację identyfikacji i analizy ryzyka stanowi arkusz ryzyk zagrażających prawom i wolnościom osób, których dane dotyczą, zwany dalej „arkuszem ryzyk praw i wolności" (tabela nr 6).

10. Jeżeli wykonana ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

11. Konsultując się z organem nadzorczym administrator przedstawia mu:
    a) gdy ma to zastosowanie – odpowiednie obowiązki administratora;
    b) cele i sposoby zamierzonego przetwarzania;
    c) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z RODO;
    d) dane kontaktowe inspektora ochrony danych;
    e) ocenę skutków dla ochrony danych, oraz
    f) wszelkie inne informacje, których żąda organ nadzorczy.

12. Niniejsza procedura podlega raz na rok przeglądowi i w przypadku konieczności aktualizacji.

13. Przeglądu i aktualizacji procedury dokonuje Inspektor.

**Tabela nr 1 do Procedury oceny skutków**

| **Możliwe skutki związane z naruszenia praw lub wolności osób, których dane dotyczą** | |
|---|---|
| dyskryminacja | kradzież tożsamości |
| oszusta dotyczące tożsamości | strata finansowa |
| naruszenie poufności danych osobowych chronionych tajemnicą zawodową | |
| nieuprawnione odwrócenie pseudonimizacji | szkoda gospodarcza |
| pozbawienie praw i wolności | szkoda społeczna |
| pozbawienie możliwości sprawowania kontroli nad swoimi danymi osobowymi | |
| naruszenie dobrego imienia | uszczerbek fizyczny |

**Tabela nr 2 do Procedury oceny skutków**

| SKALA OCEN PRAWDOPODOBIEŃSTWA | | OPIS (pomocniczo) |
|---|---|---|
| **NISKIE** | **1** | Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, ale **w ostatnim okresie nie wystąpiło.** |
| **ŚREDNIE** | **2** | Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, i **w ostatnim okresie wystąpiło raz.** |
| **WYSOKIE** | **3** | Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, i **w ostatnim okresie wystąpiło 2 lub 3 razy.** |
| **BARDZO WYSOKIE** | **4** | Istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne, i **w ostatnim okresie wystąpiło częściej niż 3 razy.** |

**Tabela nr 3 do Procedury oceny skutków**

| SKALA OCEN SKUTKU | | OPIS |
|---|---|---|
| **NISKI** | **1** | Zagrożenie objęte ryzykiem **ma niewielki wpływ** na prawa i wolności osób, których dane dotyczą. |
| **ŚREDNI** | **2** | Zagrożenie objęte ryzykiem **ma umiarkowany wpływ** na prawa i wolności osób, których dane dotyczą. |
| **WYSOKI** | **3** | Zagrożenie objęte ryzykiem **ma duży wpływ** na prawa i wolności osób, których dane dotyczą. |
| **BARDZO WYSOKI** | **4** | Zagrożenie objęte ryzykiem **ma bardzo duży wpływ** na prawa i wolności osób, których dane dotyczą. |

**Tabela nr 4 do Procedury oceny skutków**

| | | | **SKUTEK** | | | |
|---|---|---|---|---|---|---|
| | | | Niski | Średni | Wysoki | Bardzo wysoki |
| | | | **1** | **2** | **3** | **4** |
| **PRAWDOPODOBIEŃSTWO** | Niskie | **1** | | | | |
| | Średnie | **2** | | | | |
| | Wysokie | **3** | | | | |
| | Bardzo wysokie | **4** | | | | |

**Tabela nr 5 do Procedury oceny skutków**

| **Poziom ryzyka** | **Opis działania** |
|---|---|
| Niski **(N)** | Poziom ryzyka akceptowalny – działania może zostać przesunięte w czasie i nie wymaga monitorowania |
| Średni **(Ś)** | Poziom ryzyka nieakceptowalny – działania może zostać przesunięte w czasie, wymaga okresowego monitorowania |
| Wysoki **(W)** | Poziom ryzyka nieakceptowalny – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania |
| Krytyczny **(K)** | Poziom ryzyka nietolerowany – wymaga natychmiastowego działania |

**Tabela nr 6 do Procedury oceny skutków**

| **Arkusz ryzyk zagrażających prawom i wolnościom osób, których dane dotyczą** | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **Symbol komórki organizacyjnej** | **Proces przetwarzania** | **Czynność przetwarzania** | **Możliwy skutek** | **Ocena prawdopodobieństwa** | **Ocena skutku** | **Poziom istotności** | **Sposób postępowania z ryzykiem** |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## XXIV. Procedura prowadzenia wykazu i rejestrów

Celem niniejszej procedury jest ustalenie zasad prowadzenia przez Inspektora wykazu podmiotów przetwarzających dane w imieniu administratora, rejestru czynności przetwarzania danych osobowych oraz ewentualnego rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, które są prowadzone w celu realizacji przez administratora zasady rozliczalności.

1. Inspektor prowadzi:
   a) wykaz podmiotów przetwarzających dane, którego wzór stanowi załącznik nr 12 do niniejszej Polityki;
   b) rejestr czynności przetwarzania danych osobowych zgodnie z art. 30 ust. 1 RODO, którego wzór stanowi załącznik nr 13 do niniejszej Polityki;
   c) rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora zgodnie z art. 30 ust. 2 RODO, które wzór stanowi załącznik nr 14 do niniejszej Polityki.

2. Wykaz i rejestry mają formę pisemną, w tym formę elektroniczną.

3. Inspektor tworzy i prowadzi wykaz oraz rejestry w oparciu o dane otrzymane od kierowników komórek organizacyjnych lub osób zajmujących samodzielne stanowiska pracy.

4. Kierownicy komórek organizacyjnych lub osoby zajmujące samodzielne stanowiska pracy są zobowiązani do bieżącego przekazywania danych potrzebnych do prowadzenia wykazu i rejestru, w szczególności są zobowiązani do niezwłocznego informowania Inspektora o każdej zmianie mającej wpływ na treść wykazu i rejestrów.

5. Administrator, w ramach współpracy z organem nadzorczym, udostępnia rejestr na żądanie tego organu nadzorczego w celu monitorowania przez organ operacji przetwarzania.

## XXV. Procedura przeprowadzania audytów zgodności

Celem niniejszej procedury jest określenie trybu i zasad monitorowania przez Inspektora przestrzegania RODO i innych przepisów o ochronie danych osobowych, a także polityk administratora w dziedzinie ochrony danych osobowych, w tym niniejszej Polityki ochrony danych osobowych poprzez przeprowadzanie audytów zgodności przetwarzania danych osobowych.

1. Audyt zgodności jest przeprowadzany w trybie:
   a) audytu planowanego – przeprowadzanego przynajmniej raz w roku;
   b) audytu doraźnego – w sytuacji powzięcia przez Inspektora wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takie naruszenia. Audyt doraźny przeprowadza się na zasadach opisanych w rozdziale: „Procedura zgłaszania incydentów".

2. Przynajmniej na 14 dni przed rozpoczęciem audytu planowanego Inspektor informuje administratora o przedmiocie, zakresie oraz terminie przeprowadzenia audytu.

3. Planując przeprowadzenie audytu Inspektor uwzględnia w szczególności: procesy przetwarzania danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych z:
   1) zasadami, o których mowa w art. 5, art. 12-23 i art. 28 RODO i w niniejszej Polityce;
   2) zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 32 RODO i w niniejszej Polityce;
   3) zasadami przekazywania danych osobowych, o których mowa w art. 44-49 RODO;
   4) obowiązkami wynikającymi z art. 33-36 RODO;
   5) zweryfikowanym stanem faktycznym w zakresie przetwarzania danych osobowych;
   6) zasadami i obowiązkami określonymi w niniejszej Polityce.

4. Inspektor dokumentuje czynności przeprowadzone w toku audytu, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych oraz do opracowania raportu.

5. Dokumentowanie czynności w toku audytu może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania danych osobowych lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonania wydruku tych danych oraz na:
   1) sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
   2) odebraniu wyjaśnień osoby, której czynności objęto audytem;
   3) sporządzeniu kopii otrzymanego dokumentu;
   4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania danych osobowych;
   5) sporządzaniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych.

6. W systemie informatycznym służącym do przetwarzania lub zabezpieczania danych osobowych czynności Inspektora mogą być wykonywane przy udziale osób zarządzającym tym systemem.

7. Osoba, której dotyczy audyt, bierze udział w audycie lub umożliwia Inspektora przeprowadzenia czynności w toku audytu.

8. Po zakończeniu audytu Inspektor przygotowuje raport zgodności sporządzony w postaci elektronicznej lub postaci papierowej.

9. Inspektor przekazuje administratorowi raport zgodności:
   1) z audytu planowanego – nie później niż w terminie 30 dni od zakończenia audytu;
   2) z audytu doraźnego – niezwłocznie, nie później niż w terminie 7 dni od zakończenia audytu.

10. Inspektor jest uprawniony, w każdym czasie, do przeprowadzania weryfikacji przestrzegania niniejszej Polityki, bez konieczności przeprowadzania audytu zgodności.

11. Inspektor jest uprawniony do ustnego pouczenia osoby nieprzestrzegającej zasad określonych w niniejszej Polityce lub pisemnego zawiadomienia administratora o nieprzestrzeganiu zasad przez wskazaną osobę.

## XXVI. Postanowienia końcowe

1. Polityka ochrony danych osobowych jest dokumentem wewnętrznym i osoby, które uzyskały wgląd w jej treść, zobowiązane są do zachowania jej w poufności.

2. Przypadki nieuzasadnionego zaniechania obowiązków określonych w niniejszym dokumencie traktowane będą jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

3. W sprawach nieuregulowanych w niniejszej Polityce ochrony 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 oraz inne przepisy prawa z zakresu ochrony danych osobowych, a także inne przepisy z zakresu ochrony danych osobowych.

## Załącznik nr 1

| WYKAZ KATEGORII OSÓB, KTÓRYCH DANE DOTYCZĄ ORAZ KATEGORII DANYCH OSOBOWYCH | | | | | |
|---|---|---|---|---|---|
| **Lp.** | **Kategoria osób, których dane dotyczą** | **Kategorie danych osobowych** | | **Zastosowany program** | **Wersja papierowa** |
| | | **Dane zwykłe** | **Dane szczególne** | | |
| 1 | **Potencjalni pracownicy i współpracownicy** | imię i nazwisko, wizerunek, data urodzenia, miejsce urodzenia, adres zamieszkania, adres do korespondencji, nr telefonu, adres poczty elektronicznej, przebieg kariery, informacje o zatrudnieniu u innego pracodawcy, informacje o statusie bezrobotnego, poziom wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia, umiejętności, stopień znajomości języków obcych, obsługa komputera, prawo jazdy, zainteresowania, numer prawa do wykonywania zawodu, data uzyskania prawa wykonywania zawodu, data wygaśnięcia prawa wykonywania zawodu | dane dotyczące zdrowia, dane dotyczące wyroków skazujących i naruszeń prawa | Poczta elektroniczna, Portal Ministerstwa Sprawiedliwości | Tak |
| 2 | **Pracownicy i współpracownicy, w tym byli pracownicy i współpracownicy oraz członkowie ich rodzin** | imię i nazwisko, wizerunek, nazwa miejsca pracy, funkcja lub stanowisko, seria i nr dowodu tożsamości, data i miejsce urodzenia, miejsce zameldowania, adres zamieszkania, nr NIP, nr PESEL, nazwisko rodowe, | dane dotyczące zdrowia, dane dotyczące wyroków skazujących i naruszeń prawa, dane dotyczące przynależności do | Poczta elektroniczna, Hipokrates, InfoMedica, Infinitt, Simple, Waran, Płatnik, | Tak |

| | | | | | |
|---|---|---|---|---|---|
| | | obywatelstwo, prywatny nr telefonu, prywatny adres poczty elektronicznej, służbowy nr telefonu, służbowy adres poczty elektronicznej, imiona rodziców, stan rodzinny, imię i nazwisko oraz data urodzenia współmałżonka, data urodzenia dziecka lun dzieci pracownika, imię i nazwisko, adres oraz nr telefonu osoby, którą należy poinformować w razie wypadku pracownika, stosunek do powszechnego obowiązku obrony, przebieg kariery, czas pracy, wysokość wynagrodzenia, nagrody, premie, kwoty udzielonych pożyczek, informacje o zatrudnieniu u innego pracodawcy, informacje o statusie bezrobotnego, informacje o oddziale NFZ, informacje o US, poziom wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia, umiejętności, stopień znajomości języków obcych, obsługa komputera, prawo jazdy, zainteresowania, numery rachunku bankowego, firma, adres siedziby firmy, godzina i data użycia karty dostępu, imię i nazwisko osoby zgłoszonej do ubezpieczenia zdrowotnego, numer prawa do wykonywania zawodu, data uzyskania prawa wykonywania zawodu, data wygaśnięcia prawa | związków zawodowych | BIP, ePUAP, SZOI, Portal Ministerstwa Sprawiedliwości, | |

| | | | | | |
|---|---|---|---|---|---|
| | | wykonywania zawodu | | | |
| 3 | **Potencjalni dostawcy oraz ich pracownicy i współpracownicy** | imię, nazwisko, nazwa firmy, adres e-mail, strona www, nr telefonu, dane z CEIDG, forma rozliczania, nr REGON, nr NIP, nr PESEL, seria i numer dowodu tożsamości | | Poczta elektroniczna, ePUAP | Tak |
| 4 | **Dostawcy oraz ich pracownicy i współpracownicy** | imię, nazwisko, nazwa firmy, adres siedziby, adres dostawy, termin odstawy, adres e-mail, strona www, nr telefonu, dane z CEIDG, forma rozliczania, nr REGON, nr NIP, nr PESEL, seria i numer dowodu tożsamości, historia dostaw | | Poczta elektroniczna, Waran, ePUAP | Tak |
| 5 | **Skargi, wnioski i petycje** | imię, nazwisko, numer telefonu, adres poczty elektronicznej, adres do korespondencji, adres zamieszkania, treść podania, nr PESEL | | Poczta elektroniczna, ePUAP | Tak |
| 6 | **Informacja publiczna** | imię, nazwisko, numer telefonu, adres poczty elektronicznej, adres do korespondencji, adres zamieszkania, treść podania, nr PESEL | | Poczta elektroniczna, ePUAP | Tak |
| 7 | **Rejestr korespondencji** | imię, nazwisko, nazwa firmy lub instytucji, adres zamieszkania, adres siedziby, informacja czego dotyczy pismo | | Poczta elektroniczna, ePUAP | Tak |
| 8 | **Osoby kontaktowe** | imię, nazwisko, adres poczty elektronicznej, nr telefonu, miejsce pracy | | Poczta elektroniczna, ePUAP | Tak |
| 9 | **Finanse i księgowość** | imię, nazwisko, nr NIP, nr PESEL, nr rachunku bankowego, nazwa banku w którym prowadzony jest rachunek bankowy, nr REGON, nr telefonu, kwota, tytuł płatności, wysokość zadłużenia, informacje o egzekucji | | Poczta elektroniczna, InfoMedica, Simple, Waran, ePUAP, System bankowy | Tak |
| 10 | **Pacjenci i byli pacjenci** | imię, nazwisko, identyfikator pacjenta, nr PESEL, nr NIP, płeć, data urodzenia, miejsce urodzenia, nazwisko rodowe, stan cywilny, imię ojca, imię | dane dotyczące zdrowia, dane biometryczne, dane genetyczne | Poczta elektroniczna, Hipokrates, SZOI, Infinitt, | Tak |

| | | | | | |
|---|---|---|---|---|---|
| | | matki, nr ubezpieczenia, nr RUM, kod wykształcenia, adres poczty elektronicznej, adres zamieszkania, nr telefonu, adres korespondencyjny, kod wykonywanego zawodu, imię i nazwisko opiekuna, miejsce zamieszkania opiekuna, grupa krwi, seria i numer dowodu tożsamości, nr PESEL opiekuna, data ważności dokumentu ubezpieczenia, miejsce zameldowania, nr identyfikacyjny w kraju UE, numer europejskiej kartu ubezpieczeniowej, miejsce pracy, liczba dzieci, nr telefonu opiekuna, miejsce pracy opiekuna, zwód opiekuna, informacja o placówce w której dziecko mieszka, instytucja do której dziecko uczęszcza, obywatelstwo, narodowość, nr karty Polaka, dane wojskowe, numer noworodka, stopień pokrewieństwa opiekuna | | Qris, ABC, Klif, AP Kolce, SMPT, Syngovia, eWUŚ | |
| 11 | **Darczyńcy** | imię, nazwisko, nazwa przedsiębiorcy, adres, adres poczty elektronicznej, nr PESEL, nr NIP, nr REGON, nr KRS, | | Poczta elektroniczna, ePUAP | Tak |
| 12 | **Osoby objęte monitoringiem wizyjnym** | Wizerunek | | System monitoringu wizyjnego | Tak |

## Załącznik nr 2

| **Wzór informacji podawanych w przypadku zbierania danych od osoby, której dane dotyczą** | |
|---|---|
| **Wzór informacji podawanej w przypadku zbierania danych od pacjentów** | |
| **Miejsce umieszczenia** | **Treść informacji** |
| • strona internetowa – zakładka „kontakt”, „bip / dane podstawowe”;<br>• formularz rejestracyjny pacjenta;<br>• tablica ogłoszeń. | *Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:*<br>*1) administratorem danych osobowych **Pacjentów** jest Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa;*<br>*2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: kancelaria@spartanska.pl;*<br>*3) administrator będzie przetwarzał Państwa dane osobowe na podstawie art. 9 ust. 2 lit. h) RODO, tj. w celu zapewnienia opieki zdrowotnej, co wynika z ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej;*<br>*4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. laboratorium zewnętrznym, kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);*<br>*5) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;*<br>*6) mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.*<br><br>*Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:*<br>*1) Państwa dane osobowe będą przechowywane przez okres wynikający z przepisów prawa, tj. z art. 29 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta;*<br>*2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;*<br>*3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji ww. celów. Konsekwencją niepodania danych będzie odmowa udzielenia świadczeń z zakresu opieki zdrowotnej;* |

| | |
|---|---|
| | *4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.* |

| **Wzór informacje podawanej w przypadku zbierania danych od pracowników** | |
|---|---|
| **Miejsce umieszczenia** | **Treść informacji** |
| • umowa o pracę;<br>• formularz osoby zatrudnionej;<br>• oświadczenie o zachowaniu danych w poufności. | *Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:*<br>*1) administratorem danych osobowych **Pracowników** jest Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa;*<br>*2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: kancelaria@spartanska.pl;*<br>*3) administrator będzie przetwarzał Państwa dane w celu niezbędnym do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej. Dane osobowe pracowników są przetwarzane na podstawie art. 9 ust. 2 lit. b) RODO w zw. z realizacją obowiązków wynikających z ustawy z dnia 26 czerwca 1974 r. Kodeks pracy, ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, ustawy z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa, ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych oraz ustawy z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy;*<br>*4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)*;<br>*5) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;*<br>*6) mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.*<br><br>*Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:*<br>*1) Państwa dane osobowe będą przechowywane do momentu upływu okresu przewidzianego w ustawie z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, w ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20* |

| | |
|---|---|
| | *października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;*<br>2) *przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego*;<br>3) *podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji celu ich przetwarzania. Konsekwencją niepodania danych osobowych jest brak możliwości realizacji umowy o pracę;*<br>4) *administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.* |

| **Wzór informacji podawanej w przypadku zbierania danych od osób ubiegających się o zatrudnienie** | |
|---|---|
| **Miejsce umieszczenia** | **Treść informacji** |
| • ogłoszenie o pracę,<br>• formularz osoby ubiegającej się o zatrudnienie, | *Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:*<br>*1) administratorem danych osobowych **osób ubiegających się o zatrudnienie** jest Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa;*<br>*2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: kancelaria@spartanska.pl;*<br>*3) administrator będzie przetwarzał Państwa dane w celu niezbędnym do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej. Dane osobowe pracowników są przetwarzane na podstawie art. 9 ust. 2 lit. b) RODO w zw. z realizacją przepisów wynikających z ustawy z dnia 26 czerwca 1974 r. Kodeks pracy;*<br>*4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);*<br>*5) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;*<br>*6) mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.*<br><br>*Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:*<br>*1) Państwa dane osobowe będą przechowywane przez okres prowadzenia naboru na wolne stanowisko pracy, nie dłużej niż przez okres 30 dni liczonych od dnia zakończenia procesu naboru;*<br>*2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;*<br>*3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do wzięcia udziału w naborze na wolne stanowisko pracy. Konsekwencją niepodania danych osobowych jest brak udziału w naborze na wolne stanowisko pracy;*<br>*4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu* |

| | |
|---|---|
| | *o Państwa dane osobowe.* |

| **Wzór informacji podawanej w przypadku zbierania danych od wykonawców lub zleceniobiorców** | |
|---|---|
| **Miejsce umieszczenia** | **Treść informacji** |
| • umowa;<br>• formularz oferty,<br>• formularz oświadczenia zleceniobiorcy do celów podatkowych i ubezpieczenia społecznego;<br>• formularz oświadczenia wykonawcy dzieła do celów podatkowych. | *Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:*<br>*1) administratorem danych osobowych **Wykonawców lub Zleceniobiorców** jest Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa;*<br>*2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: kancelaria@spartanska.pl;*<br>*3) administrator będzie przetwarzał Państwa dane osobowe na podstawie art. 6 ust. 1 lit. b) RODO, tj. przetwarzanie jest niezbędne w celu wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;*<br>*4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych)*;<br>*5) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;*<br>*6) mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.*<br><br>*Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:*<br>*1) Państwa dane osobowe będą przechowywane do momentu upływu okresu przedawnienia wynikającego z ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny;*<br>*2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przeniesienia danych oraz prawo do wniesienia skargi do organu nadzorczego*;<br>*3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do zawarcia umowy. Konsekwencją niepodania danych osobowych będzie brak realizacji umowy;*<br>*4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu* |

| | |
|---|---|
| | *o Państwa dane osobowe.* |

| **Wzór informacji podawanej w przypadku zbierania danych od osób składających skargi lub wnioski** | |
|---|---|
| **Miejsce umieszczenia** | **Treść informacji** |
| • strona internetowa – zakładka „skargi i wnioski”,<br>• formularz skargi i wniosku,<br>• tablica ogłoszeń. | *Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:*<br>*1) administratorem danych osobowych **osób składających skargi lub wnioski** jest Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa;*<br>*2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: kancelaria@spartanska.pl;*<br>*3) administrator będzie przetwarzał Państwa dane osobowe w celu rozpatrzenia skargi lub wniosku. Państwa dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit. c) RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze wynikającego z ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego;*<br>*4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);*<br>*5) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;*<br>*6) mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.*<br><br>*Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:*<br>*1) Państwa dane osobowe będą przechowywane przez okres przechowywania ww. dokumentów określony w ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;*<br>*2) przysługuje Państwu prawo dostępu do treści swoich danych, ich* |

| | |
|---|---|
| | *sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przeniesienia danych oraz prawo do wniesienia skargi do organu nadzorczego*;<br>*3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do zawarcia umowy. Konsekwencją niepodania danych osobowych jest brak możliwości rozpatrzenia skargi lub wniosku;*<br>*4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.* |

**Wzór informacji podawanej w przypadku zbierania danych od osób ubiegających się o świadczenie z Zakładowego Funduszu Świadczeń Socjalnych**

| Miejsce umieszczenia | Treść informacji |
|---|---|
| • regulamin Zakładowego Funduszu Świadczeń Socjalnych,<br>• wniosek o przyznanie świadczenia z ZFŚS. | *Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:*<br>*1) administratorem danych osobowych **osób ubiegających się o świadczenie z Zakładowego Funduszu Świadczeń Socjalnych** jest Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa;*<br>*2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: kancelaria@spartanska.pl;*<br>*3) administrator będzie przetwarzał Państwa dane osobowe w celu związanym z rozpatrzeniem i realizacją wniosku o przyznanie świadczenia z Zakładowego Funduszu Świadczeń Socjalnych. Państwa dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit. c) RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze wynikającego z ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych;*<br>*4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);*<br>*5) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;*<br>*6) mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.*<br><br>*Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:*<br>*1) Państwa dane osobowe będą przechowywane do momentu upływu okresu przewidzianego zgodnie z ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;*<br>*2) przysługuje Państwu prawo dostępu do treści swoich danych, ich* |

| | |
|---|---|
| | *sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przeniesienia danych oraz prawo do wniesienia skargi do organu nadzorczego*;<br>*3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do zawarcia umowy. Konsekwencją niepodania danych osobowych jest brak możliwości rozpatrzenia wniosku się o świadczenie z Zakładowego Funduszu Świadczeń Socjalnych;*<br>*4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.* |

| **Wzór informacji podawanej w przypadku zbierania danych od osób składających wniosek o udostępnienie informacji publicznej** | |
|---|---|
| **Miejsce umieszczenia** | **Treść informacji** |
| • strona internetowa – zakładka „informacja publiczna” | *Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:*<br>*1) administratorem danych osobowych **osób wnioskujących o udostępnienie informacji publicznej** jest Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa;*<br>*2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: kancelaria@spartanska.pl;*<br>*3) administrator będzie przetwarzał Państwa dane osobowe na podstawie art. 6 ust. 1 lit. c) RODO, tj. w celu wypełnienia obowiązku prawnego ciążącego na administratorze przewidzianego w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej;*<br>*4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);*<br>*5) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;*<br>*6) mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.*<br><br>*Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:*<br>*1) Państwa dane osobowe będą przechowywane przez okres przewidziany w przepisach prawa, tj. w ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;;*<br>*2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;*<br>*3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do* |

| | |
|---|---|
| | *realizacji ww. celów. Konsekwencją niepodania danych będzie nierozpatrzenie skargi lub wniosku;*<br>*4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.* |

## Załącznik nr 3

| **Wzór informacji podawanych w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą** | |
|---|---|
| **Wzór informacji podawanej w przypadku zbierania danych wykonawców z Internetu** | |
| **Miejsce umieszczenia** | **Treść informacji** |
| • treść wiadomości elektronicznej skierowanej do potencjalnego wykonawcy,<br>• formularz oferty wysyłany do potencjalnego wykonawcy. | *Zgodnie z art. 14 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:*<br>*1) administratorem Państwa danych osobowych jest Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa;*<br>*2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: kancelaria@spartanska.pl;*<br>*3) administrator będzie przetwarzał Państwa dane osobowe w celu związanych z oszacowaniem wartości zamówienia oraz ewentualnym zawarciem i realizacją umowy o współpracy na podstawie. Dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit. b) RODO, tj. przetwarzanie jest niezbędne w celu wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;*<br>*4) administrator przetwarza jedynie Państwa dane kontaktowe;*<br>*5) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);*<br>*6) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;*<br>*7) mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.*<br><br>*Dodatkowo zgodnie z art. 14 ust. 2 RODO informujemy, że:*<br>*1) Państwa dane osobowe będą przechowywane do momentu upływu okresu przedawnienia wynikającego z ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny;*<br>*2) przysługuje Państwu prawo dostępu do treści swoich danych, ich* |

| | |
|---|---|
| | *sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia sprzeciwu wobec przetwarzania, prawo do przeniesienia danych oraz prawo do wniesienia skargi do organu nadzorczego*;<br>*3) dane osobowe zostały pozyskane z publicznie dostępnego źródła, tj. z Internetu;*<br>*4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.* |

## Załącznik nr 4

Wzór oświadczenia o zachowaniu danych osobowych w poufności:

……., Warszawa

imię: _____
nazwisko: _____
stanowisko: _____
komórka organizacyjna: _____

**OŚWIADCZENIE**
o zachowaniu danych osobowych w poufności w
**Narodowym Instytucie Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher**
(dalej „administrator")

**TREŚĆ OŚWIADCZENIA**

W związku z dopuszczeniem do przetwarzania danych osobowych oświadczam, że:

- Zapoznałem się i zobowiązuję się do przestrzegania obowiązków wynikających z:
  - przepisów 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;
  - regulacji wewnętrznych administratora danych obowiązujących w obszarze przetwarzania danych osobowych, w tym w szczególności Polityki ochrony danych osobowych.
- Zapewnię bezpieczeństwo przetwarzanych danych osobowych poprzez ich ochronę przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem.
- Zachowam w tajemnicy dane osobowe oraz sposoby ich zabezpieczeń, do których uzyskam dostęp w trakcie współpracy z administratorem, jak i po jej zakończeniu.
- Będę wykonywać polecenia Inspektora Ochrony Danych oraz innych przedstawicieli administratora odpowiedzialnych za bezpieczeństwo danych osobowych, które będą związane z zachowaniem bezpieczeństwa danych osobowych i sposobów ich zabezpieczenia w poufności.
- W razie uzyskania nieuprawnionego dostępu do danych osobowych lub wykrycia incydentu godzącego w bezpieczeństwo danych osobowych, zobowiązuję się powiadomić o tym bezpośredniego przełożonego lub komórkę właściwą ds. IT.

- Znane mi są zasady monitorowania sposobu używania sprzętu służbowego, w tym m.in. telefonu komórkowego, komputerów, poczty elektronicznej, obowiązujące u administratora. Zostałem poinformowany o zakresie i sposobach prowadzenia ww. monitoringu.
- Znane mi są zasady odpowiedzialności prawnej za niezgodne z przepisami o ochronie danych osobowych przetwarzanie danych osobowych oraz mam świadomość, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać prawnie na podstawie regulacji wewnętrznych obowiązujących u administratora danych, kodeksu pracy, kodeksu karnego lub kodeksu cywilnego.

Oświadczam, że treść niniejszego oświadczenia jest mi znana i zobowiązuję się do jego przestrzegania.

Potwierdzam odbiór 1 egz. niniejszego oświadczenia.

…….

data i podpis składającego oświadczenie

## Załącznik nr 5

Wzór nadania upoważnienia do przetwarzania danych osobowych:

……., Warszawa

**UPOWAŻNIENIE nr ……**

do przetwarzania danych osobowych w

**Narodowym Instytucie Geriatrii, Reumatologii i Rehabilitacji**

**im. prof. dr hab. Eleonory Reicher**

**TREŚĆ UPOWAŻNIENIA**

Działając na podstawie Polityki ochrony danych osobowych, w celu zapewnienia realizacji postanowień 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, zwanego dalej „RODO", **administrator upoważnia**:

imię: _____

nazwisko: _____

stanowisko: _____

do przetwarzania danych osobowych, których administratorem w rozumieniu art. 4 pkt 7 RODO jest Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher lub które zostały powierzone Narodowemu Instytutowi Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher do przetwarzania.

Upoważnienie dotyczy przetwarzania danych osobowych w postaci papierowej oraz w ramach nadanych dostępów do systemów informatycznych służących do przetwarzania danych osobowych w zakresie zgodnym z zakresem powierzonych czynności.

Upoważnienie traci ważność z chwilą jego cofnięcia, wydania nowego upoważnienia lub ustania stosunku umownego wiążącego upoważnionego z Narodowym Instytutem Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher.

_____

Data, podpis i pieczątka Dyrektora Instytutu

Potwierdzam otrzymanie niniejszego upoważnienia.

_____

Data i podpis osoby upoważnionej

## Załącznik nr 6

Wzór cofnięcia upoważnienia do przetwarzania danych osobowych:

……., Warszawa

**COFNIĘCIE UPOWAŻNIENIE nr ……**
do przetwarzania danych osobowych w
**Narodowym Instytucie Geriatrii, Reumatologii i Rehabilitacji**
**im. prof. dr hab. Eleonory Reicher**

**TREŚĆ COFNIĘCIA UPOWAŻNIENIA**

Działając na podstawie Polityki ochrony danych osobowych, w celu zapewnienia realizacji postanowień 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, zwanego dalej „RODO", **administrator cofa upoważnienie**:

imię: _____
nazwisko: _____
stanowisko: _____

do przetwarzania danych osobowych, których administratorem w rozumieniu art. 4 pkt 7 RODO jest Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher lub które zostały powierzone Narodowemu Instytutowi Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher do przetwarzania.

Cofnięcie upoważnienia dotyczy przetwarzania danych osobowych w postaci papierowej oraz w ramach nadanych dostępów do systemów informatycznych służących do przetwarzania danych osobowych w zakresie zgodnym z zakresem powierzonych czynności.

_____
Data, podpis i pieczątka Dyrektora Instytutu

Potwierdzam otrzymanie niniejszego cofnięcia upoważnienia.

_____
Data i podpis osoby, której cofnięto upoważnienie

## Załącznik nr 7

Wzór wniosku o nadanie dostępu do systemów i grupy uprawnień:

### Wniosek o nadanie dostępu do systemów i grupy uprawnień

nadanie dostępu ☐ aktualizacja dostepu ☐

**Dane Pracownika, któremu nadajemy uprawnienia:**

| | | |
|---|---|---|
| 1. | Imię i nazwisko | |
| 2. | Nr pesel | |
| 3. | Stanowisko/Nr prawa wykonywania zawodu | |
| 4. | Jednostka organizacyjna | |
| 5. | Bezpośredni przełożony | |

**Wnioskuję o nadanie uprawnień dla Pracownika zatrudnionego na stanowisku:**

| | | |
|---|---|---|
| Lekarz | oddział ☐<br>poradnia ☐<br>radiologia ☐ | dyżurny ☐<br>podpis z-cy Dyrektora ds. Klinicznych |
| Pielęgniarz/ka | oddział/poradania/zakład/izba przyjęć ☐ | oddziałowa ☐ |
| Rejestrator/ka | zespół poradni ☐ | radiologia ☐ |
| Sekretarka medyczna | ☐ | |
| Statystyk | ☐ | |
| Laborant | wprowadzający badania ☐ | zatwierdzający badania ☐ |
| Aptekarz | ☐ | |
| Technik RTG / TK / MR | ☐ | |
| Administracja | ☐<br>(proszę o wpisanie systemów) | |
| Inne | ☐<br>(proszę o wpisanie systemów) | |
| Założenie skrzynki pocztowej, imiennej | ☐ | |

| | | | | |
|---|---|---|---|---|
| Nadanie uprawnień do folderów sieciowych | | | | |
| | (nazwa folderu) | (podpis właściciela folderu) | (nazwa folderu) | (podpis właściciela folderu) |

| | |
|---|---|
| Nadanie niestandardwych uprawnień do: | (proszę wpisać nazwy systemów) |
| Łączna liczba zaznaczonych/wpisanych uprawnień | |

**Wnioskuję o <u>odebranie:</u>**

| | |
|---|---|
| ☐<br>wszystkich uprawnień | (proszę wpisać nazwy systemów do których odebrać uprawnienia) |

**Akceptacja wniosku:**

| | |
|---|---|
| Data i podpis bezpośredniego przełożonego (osoba wnioskująca) | Data i podpis Pracownika Działu Spraw Personalnych |

**Informacje o wydanym dostępnie:**

Data wydania: _____ Przez: _____

Potwierdzam otrzymanie uprawnień: _____
(data i podpis użytkownika)

## Załącznik nr 8

| Nazwa administratora danych: | **Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher** |
|---|---|

**Ewidencja użytkowników systemu informatycznego**

| Lp. | Imię | Nazwisko | Identyfikator użytkownika | Data nadania dostępu | Godzina nadania dostępu | Data odebrania dostępu | Godzina odebrania dostępu |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## Załącznik nr 9

| Nazwa administratora danych: | **Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher** |
|---|---|

**Ewidencja osób upoważnionych do przetwarzania danych osobowych**

| Lp. | Imię | Nazwisko | Numer upoważnienia | Data nadania upoważnienia | Data odebrania upoważnienia |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## Załącznik nr 10

Wzór umowy powierzenia przetwarzania danych osobowych:

**UMOWA**
**POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH**

Niniejsza umowa została zawarta w Warszawie w dniu ……. …… r. roku przez:

**……**
**……**
zwaną dalej „**Administratorem**”,
reprezentowaną przez:

**……** – ……,

oraz

**……**
**……**z
waną dalej „**Podmiotem Przetwarzającym**”,
reprezentowaną przez:

**……** – …….

Administrator i Podmiot Przetwarzający będą dalej zwani łącznie „**Stronami**”, a każdy z osobna „**Stroną**”.

Zważywszy, że:

1. Administrator jest administratorem danych osobowych w rozumieniu art. 4 pkt 7 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, zwanego dalej „RODO”, wskazanych w załączniku nr 1 do umowy.
2. Administrator zamierza powierzyć Podmiotowi Przetwarzającemu przetwarzanie danych osobowych, a Podmiot Przetwarzający zamierza przyjąć powierzone mu dane osobowe do przetwarzania w imieniu Administratora, zgodnie z umową oraz z przepisami regulującymi przetwarzanie danych osobowych, wiążącymi Podmiot Przetwarzający i Administratora.

Strony postanowiły, co następuje:

§ 1
Przedmiot umowy

Administrator powierza Podmiotowi Przetwarzającemu przetwarzanie danych osobowych w imieniu Administratora, na zasadach określonych w Umowie oraz we właściwych przepisach regulujących przetwarzanie danych osobowych, w szczególności w RODO.

Rodzaj danych osobowych, kategorie osób, których dotyczą dane osobowe, jak również przedmiot, czas trwania, charakter i cel przetwarzania danych osobowych są wskazane w załączniku nr 1 do umowy.

Strony zobowiązują się wykonywać zobowiązania wynikające z umowy z najwyższą starannością, w celu prawidłowego zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron oraz osób, których dane osobowe dotyczą, w zakresie przetwarzania danych osobowych.

§ 2
Oświadczenie Podmiotu Przetwarzającego

Podmiot Przetwarzający oświadcza, że:

a) wdrożył środki techniczne i organizacyjne gwarantujące przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami, w sposób zapewniający ochronę praw osób, których dotyczą dane osobowe; oraz
b) dysponuje środkami, doświadczeniem, wiedzą oraz odpowiednio wyszkolonym personelem, umożliwiającymi prawidłowe przetwarzanie danych osobowych w zakresie i w celu określonych w umowie.

§ 3
Przetwarzanie danych osobowych

1. Z zastrzeżeniem ust. 2, przetwarzanie danych osobowych przez Podmiot Przetwarzający może następować wyłącznie w przypadkach wynikających z Umowy lub na podstawie odrębnych zleceń Administratora, wyrażonych w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej).
2. Podmiot Przetwarzający ma prawo przetwarzać dane osobowe, jeżeli obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot Przetwarzający. W takim przypadku Podmiot Przetwarzający jest zobowiązany poinformować Administratora o stosującym się do niego obowiązku prawnym co najmniej na 24 godziny przed rozpoczęciem przetwarzania, chyba że wiążące go przepisy zabraniają mu udzielania takiej informacji, z uwagi na ważny interes publiczny.
3. Przetwarzanie danych osobowych przez Podmiot Przetwarzający jest ograniczone do celu i zakresu wskazanych w załączniku nr 1 do umowy.
4. Podmiot Przetwarzający prowadzi rejestr czynności przetwarzania danych osobowych, zawierający informacje wymagane przez obowiązujące przepisy, chyba że zgodnie z obowiązującymi przepisami nie ma obowiązku prowadzenia takiego rejestru.

5. Podmiot Przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z art. 30 ust. 2 RODO, chyba że zgodnie z obowiązującymi przepisami nie ma obowiązku prowadzenia takiego rejestru.
6. Wszelkie zlecane przez Administratora operacje przetwarzania danych osobowych Podmiot Przetwarzający wykonuje niezwłocznie, w szczególności jeśli chodzi o usunięcie danych osobowych na żądanie osoby, której dotyczą.
7. Biorąc pod uwagę charakter przetwarzania danych osobowych, Podmiot Przetwarzający ma obowiązek współdziałania z Administratorem w celu wywiązania się z obowiązku odpowiadania na żądania osoby, której dane osobowe dotyczą, w zakresie wykonywania jej praw określonych w obowiązujących przepisach, wdrażając odpowiednie środki techniczne i organizacyjne.
8. Podmiot Przetwarzający zapewni, że osoby, które będą zaangażowane w czynności przetwarzania danych osobowych w ramach jego organizacji:
   a) otrzymają pisemne upoważnienia do przetwarzania danych osobowych;
   b) będą zaznajomione z obowiązującymi przepisami o ochronie danych osobowych (z uwzględnieniem ich ewentualnych zmian) oraz z odpowiedzialnością za ich nieprzestrzeganie;
   c) będą dokonywały czynności przetwarzania danych osobowych wyłącznie na polecenie Administratora, z zastrzeżeniem ust. 2; oraz
   d) zobowiążą się do bezterminowego zachowania w tajemnicy danych osobowych oraz stosowanych przez Podmiot Przetwarzający sposobów ich zabezpieczenia, o ile taki obowiązek nie wynika dla nich z odpowiednich przepisów.
9. Podmiot Przetwarzający prowadzi ewidencję udzielonych upoważnień do przetwarzania danych osobowych, o których mowa w ust. 8 lit. a).

§ 4

Dalsze powierzenia przetwarzania

1. Podmiot Przetwarzający ma prawo korzystać z podwykonawców przy przetwarzaniu danych osobowych (dalsze powierzenie przetwarzania), pod warunkiem, że przed powierzeniem podwykonawcy przetwarzania danych osobowych:
   a) uzyska na to zgodę Administratora, wyrażoną w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej);
   b) zawrze z podwykonawcą umowę powierzenia przetwarzania danych osobowych na warunkach nie gorszych niż warunki umowy;
   c) upewni się, że podwykonawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom obowiązujących przepisów.
2. Jeżeli podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, Podmiot Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za wypełnienie obowiązków podwykonawcy.

3. Wykaz podwykonawców, z których Podmiot Przetwarzający korzysta w dniu zawarcia umowy, i co do których Administrator wyraża zgodę na dalsze powierzenie przetwarzania danych osobowych, stanowi załącznik nr 2 do umowy.

§ 5
Bezpieczeństwo danych osobowych

1. Podmiot Przetwarzający stosuje środki techniczne i organizacyjne, odpowiednie do zagrożeń oraz charakteru, zakresu, kontekstu i celu przetwarzania danych osobowych, zapewniające bezpieczeństwo danych osobowych, w szczególności przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem.
2. Podmiot Przetwarzający zobowiązuje się stale monitorować stan stosowanych zabezpieczeń danych osobowych oraz występujących zagrożeń bezpieczeństwa, i w razie potrzeby aktualizuje stosowane środki techniczne i organizacyjne, tak, żeby zapewnić najwyższy osiągalny poziom ochrony danych osobowych.
3. Podmiot Przetwarzający, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, ma obowiązek współdziałania z Administratorem w wywiązaniu się z obowiązków określonych w art. 32–36 RODO.
4. Podmiot Przetwarzający niezwłocznie zawiadamia Administratora, przed podjęciem jakichkolwiek działań, o każdym przypadku:
   a) wystąpienia jakiegokolwiek organu z żądaniem udostępnienia danych osobowych, chyba że zakaz ujawnienia tej informacji wynika z obowiązujących przepisów;
   b) wystąpienia przez osobę, której dane osobowe dotyczą, z żądaniem dotyczącym przetwarzania danych osobowych lub ich treści.
5. Podmiot Przetwarzający niezwłocznie – w każdym wypadku nie później niż w ciągu 24 godzin od wykrycia – informuje Administratora o wszelkich wykrytych naruszeniach bezpieczeństwa danych osobowych, przekazując Administratorowi wszelkie dostępne Podmiotowi Przetwarzającemu informacje na temat naruszenia, w szczególności:
   a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane osobowe dotyczą, oraz kategorie i przybliżoną liczbę wpisów, których dotyczy naruszenie;
   b) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   c) możliwe konsekwencje naruszenia ochrony danych osobowych; oraz
   d) środki zastosowane lub proponowane przez Podmiot Przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Podmiot Przetwarzający współdziała z Administratorem przy ustalaniu szczegółów związanych ze zgłoszonym Administratorowi naruszeniem, w szczególności przyczyn i skutków jego wystąpienia oraz wdraża zalecane przez Administratora środki mające na celu złagodzenie ewentualnych niekorzystnych skutków naruszenia danych osobowych oraz środki naprawcze.

7. Podmiot Przetwarzający niezwłocznie informuje Administratora, jeśli jego zdaniem wydane mu przez Administratora polecenie dotyczące przetwarzania danych osobowych stanowi naruszenie obowiązujących przepisów.

§ 6
Prawo do kontroli

1. Administrator ma prawo kontrolowania sposobu wypełniania przez Podmiot Przetwarzający jego obowiązków określonych w umowie lub w obowiązujących przepisach. W szczególności Administrator może żądać udostępnienia określonych informacji lub dokumentów oraz może przeprowadzać – samodzielnie lub przez upoważnionego przez Administratora pracownika lub współpracownika – audyty, w tym inspekcje w miejscu przetwarzania danych osobowych przez Podmiot Przetwarzający.
2. Podmiot Przetwarzający ma obowiązek współpracować z Administratorem lub upoważnionym przez Administratora pracownikiem lub współpracownikiem w czasie przeprowadzanej kontroli, w sposób umożliwiający Administratorowi weryfikację prawidłowej realizacji obowiązków Podmiotu Przetwarzającego.

§ 7
Rozwiązanie umowy

1. Umowa wchodzi w życie z dniem podpisania i zostaje zawarta na czas określony do dnia rozwiązania lub wygaśnięcia ostatniej z umów łączących Strony, z których wynika konieczność przetwarzania danych osobowych przez Podmiot Przetwarzający.
2. W przypadku stwierdzenia naruszenia przez Podmiot Przetwarzający obowiązków wynikających z umowy, Administrator ma prawo rozwiązać wszystkie umowy zawarte z Podmiotem Przetwarzającym, z których wynika konieczność przetwarzania danych osobowych przez Podmiot Przetwarzający, ze skutkiem natychmiastowym.
3. Najpóźniej w dniu rozwiązania umowy Podmiot Przetwarzający ma obowiązek:
   a) usunąć wszelkie dane osobowe; albo
   b) zwrócić Administratorowi wszelkie nośniki zawierające dane osobowe oraz usunąć wszelkie istniejące kopie danych osobowych, chyba że obowiązujące przepisy wymagają od niego dalszego przechowywania części lub całości danych osobowych,
   c) zależnie od wyboru Administratora, zakomunikowanego Podmiotowi Przetwarzającemu w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej) co najmniej na 7 dni przed terminem rozwiązania Umowy.
4. W przypadku rozwiązania Umowy w trybie ust. 2 wybór Administratora będzie zakomunikowany Podmiotowi Przetwarzającemu w oświadczeniu o rozwiązaniu umowy ze skutkiem natychmiastowym.
5. Czynności wskazane w ust. 3 zostaną wykazane w pisemnym protokole, podpisanym przez przedstawiciela Podmiotu Przetwarzającego i dostarczonym Administratorowi w terminie 7 dni od dokonania wskazanych w nim czynności.

§ 8

Postanowienia końcowe

1. Podmiotowi Przetwarzającemu nie przysługuje wynagrodzenie za wykonywanie Umowy.
2. Umowa stanowi całość porozumienia pomiędzy Stronami i zastępuje w całości uprzednie lub równoczesne uzgodnienia poczynione przez Strony (w formie pisemnej lub ustnej) w przedmiocie regulowanym postanowieniami niniejszej Umowy.
3. Załączniki do Umowy stanowią jej integralną część.
4. Wszelkie spory między Stronami będą rozwiązywane na zasadzie polubownych negocjacji. W przypadku nieosiągnięcia przez Strony porozumienia, spór zostanie przekazany do rozstrzygnięcia sądowi powszechnemu właściwemu dla siedziby Administratora.
5. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
6. Umowa została sporządzona w dwóch egzemplarzach, po jednym dla każdej ze Stron.

Administrator: Podmiot Przetwarzający:

_____ _____

**Załącznik nr 1 – Dane osobowe**

| | |
|---|---|
| **Rodzaje danych osobowych** (np. imię, nazwisko, adres, numer PESEL, numer telefonu, e-mail, adres IP, dane o stanie zdrowia) | |
| **Kategorie osób, których dane osobowe dotyczą** (np. pracownicy, dostawcy, pacjenci, kontrahenci, klienci) | |
| **Zakres przetwarzania danych osobowych** (czynności dokonywane na powierzonych danych osobowych, np.: zbieranie, utrwalanie, organizowanie, porządkowanie, adaptowanie, przechowywanie, modyfikowanie, pobieranie, przeglądanie, udostępnianie, zmienianie, usuwanie) | |
| **Charakter przetwarzania** (np. systematyczny/sporadyczny) | |
| **Cel przetwarzania** (np. wykonanie umowy z dnia…) | |
| **Czas przetwarzania** (np. *okres obowiązywania umowy z dnia…)* | |

**Załącznik nr 2 – Podwykonawcy zatwierdzeni przez Administratora**

| Lp. | Nazwa | Adres | NIP |
|---|---|---|---|
| 1. | | | |
| 2. | | | |
| 3. | | | |

## Załącznik nr 11

Wzór rejestru incydentów:

| Rejestr incydentów | | | | | | |
|---|---|---|---|---|---|---|
| **Lp.** | **Data wystąpienia** | **Opis incydentu** | **Zgłaszający** | **Opis rozwiązania** | **Data rozwiązania** | **Działania naprawcze** |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

## Załącznik nr 12

Wzór wykazu podmiotów przetwarzających:

| Wykaz podmiotów przetwarzających dane osobowe w imieniu administratora | | | | | |
|---|---|---|---|---|---|
| **Lp.** | **Nazwa podmiotu** | **Adres** | **Kod pocztowy** | **Poczta** | **Informacje o umowie** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## Załącznik nr 13

Wzór rejestru czynności przetwarzania danych osobowych:

| **Rejestr czynności przetwarzania danych osobowych** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Nazwa administratora:** | | | | | **Dane kontaktowe administratora:** | | | | **Dane kontaktowe Inspektora Ochrony Danych:** | | | |
| | | | | | | | | | | | | |
| **Lp.** | **Proces** | **Czynność przetwarzania** | **Kategorie podmiotów danych** | **Kategorie danych** | **Szczególne kategorie danych** | **Cel przetwarzania** | **Planowany termin usunięcia danych** | **Kategorie odbiorców danych** | **Techniczne środki bezpieczeństwa** | **Organizacyjne środki bezpieczeństwa** | **Ostatnia aktualizacja pozycji rejestru** | **Uwagi** |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

## Załącznik nr 14

Wzór rejestru wszystkich kategorii czynności przetwarzania:

| **Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Nazwa podmiotu przetwarzającego:** | | | **Dane kontaktowe podmiotu przetwarzającego:** | | | **Dane kontaktowe Inspektora Ochrony Danych:** | | |
| | | | | | | | | |
| **Lp.** | **Administrator** | | **Dane Inspektora Ochrony Danych** | **Kategorie przetwarzań** | **Techniczne środki bezpieczeństwa** | **Organizacyjne środki bezpieczeństwa** | **Ostatnia aktualizacja pozycji rejestru** | **Uwagi** |
| | **Nazwa** | **dane kontaktowe** | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

## Załącznik nr 15

Wniosek o udostępnienie dokumentacji medycznej:

Warszawa, dnia …….

_____
(pieczęć jednostki)

**Dyrektor**
**Narodowym Instytut Geriatrii, Reumatologii**
**i Rehabilitacji im. prof. dr hab. Eleonory Reicher**
**w Warszawie**
ul. Spartańska 1
02-637 Warszawa

### Wniosek o udostępnienie dokumentacji medycznej

Zgodnie z art. 26 ust. 4 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta zwracam się z wnioskiem o udostępnienie dokumentacji medycznej zgodnie z poniższym:

| Dane studenta, doktoranta lub słuchacza* | |
|---|---|
| imię i nazwisko: | |
| numer telefonu: | |
| adres e-mail: | |
| Wskazanie przeznaczenia udostępnionych danych: | |
| [ należy wpisać rodzaj pracy oraz jej tytuł ] | |
| Zakres wnioskowanych informacji: | |

[ należy wskazać jakie dane mają zostać udostępnione ]

Jednocześnie upoważniam ww. studenta, doktoranta lub słuchacza* do prowadzenia korespondencji z Narodowym Instytutem Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher w przedmiotowej sprawie, uzyskania dokumentacji medycznej, wniesienia w imieniu wnioskodawcy opłaty za kserokopię dokumentacji medycznej oraz do innych związanych z tym czynnościami.

_____ _____

(podpis studenta, doktoranta, słuchacza) (podpis przedstawiciela jednostki)

## Załącznik nr 16

Wzór oświadczenia studenta, doktoranta lub słuchacza:

Warszawa, dnia ……

_____
_____
_____
(dane studenta, doktoranta lub słuchacza)

**OŚWIADCZENIE**

Oświadczam, że otrzymałam/em kserokopię dokumentacji medycznej, zgodnie z wnioskiem:

| Nazwa uczelni lub instytutu badawczego | | Wniosek z dnia: |
|---|---|---|
| | | |
| W celu napisania pracy: | | |
| [ należy wpisać rodzaj pracy oraz jej tytuł ] | | |
| Dokumentacja medyczna dotyczyła następujących pacjentów: | Z pobytu (nazwa oddziału) | W okresie (od … do …) |
| | | |
| Dokumentacja obejmowała: | | |
| | | |

Zobowiązuję się do zachowania w tajemnicy wszystkich powziętych z tej dokumentacji danych oraz wykorzystania danych z tej dokumentacji jedynie ww. pracy naukowej.

_____
(data i podpis)

## Załącznik nr 17

Wzór oświadczenia studenta, doktoranta :

Warszawa, dnia ……

_____
_____
_____
(dane studenta, doktoranta lub słuchacza)

### OŚWIADCZENIE

Oświadczam, że w dniach od ……. do ……. korzystałem/am z dokumentacji medycznej Narodowego Instytutu Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, zgodnie z wnioskiem o udostępnienie dokumentacji medycznej:

| Nazwa uczelni lub instytutu badawczego | | Wniosek z dnia: |
|---|---|---|
| | | |
| W celu napisania pracy: | | |
| [ należy wpisać rodzaj pracy oraz jej tytuł ] | | |
| Dokumentacja medyczna dotyczyła następujących pacjentów: | Z pobytu (nazwa oddziału) | W okresie (od … do …) |
| | | |
| Dokumentacja obejmowała: | | |
| | | |

Zobowiązuję się do zachowania w tajemnicy wszystkich powziętych z tej dokumentacji danych oraz wykorzystania danych z tej dokumentacji jedynie ww. pracy naukowej.

_____
(data i podpis)

## Załącznik nr 18

Wykaz kamer monitoringu wizyjnego:

| **Wykaz kamer systemu monitoringu bez włączonej funkcji rejestracji** | |
|---|---|
| **Lokalizacja** | **Określenie obszaru monitorowania** |
| | |
| | |
| | |
| | |
| | |
| **Wykaz kamer systemu monitoringu z włączoną funkcją rejestracji** | |
| **Lokalizacja** | **Określenie obszaru monitorowania** |
| | |
| | |
| | |
| | |
| | |

## Załącznik nr 19

Wzór formularza oceny skutków:

| **OCENA SKUTKÓW PLANOWANYCH OPERACJI PRZETWARZANIA DLA OCHRONY DANYCH OSOBOWYCH** | | |
|---|---|---|
| **I. Informacje ogólne** | | |
| Administrator danych osobowych: | | |
| Oceniane operacje przetwarzania[i]: | | [opis ocenianych operacji] |
| Data przeprowadzenia oceny: | | [data przeprowadzenia pierwszej oceny] |
| Daty aktualizacji oceny: | | 1. [ data pierwszej aktualizacji oceny]<br>2. [ data drugiej aktualizacji oceny]<br>3. [ data trzeciej aktualizacji oceny] |
| Powód aktualizacji oceny: | | 1. [ powód pierwszej aktualizacji oceny]<br>2. [ powód drugiej aktualizacji oceny]<br>3. [ powód trzeciej aktualizacji oceny] |
| **II. Opis planowanych operacji przetwarzania danych osobowych** | | |
| 1. Uwagi ogólne | | |
| 2. Charakter przetwarzania danych osobowych[ii] | | |
| 3. Zakres przetwarzania danych osobowych[iii] | | |
| 4. Kontekst przetwarzania danych osobowych[iv] | | |
| 5. Cele przetwarzania danych osobowych[v] | | |
| 6. Podmioty uczestniczące w przetwarzaniu | Podmioty przetwarzające dane | |
| | Osoby upoważnione | |
| 7. Okres przetwarzania | | |
| 8. Aktywa wykorzystywane do przetwarzania danych osobowych[vi] | | |
| 9. Stosowanie zatwierdzonych kodeksów postępowania[vii] | | |
| **III. Ocena niezbędności i proporcjonalności przetwarzania danych osobowych** | | |
| 1. Czy dane osobowe zbierane są w konkretnych, wyraźnych i prawnie | | |

| | | |
|---|---|---|
| uzasadnionych celach?[viii] | | |
| 2. Czy dane osobowe są przetwarzane zgodnie z prawem?[ix] | | |
| 3. Czy dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane? | | |
| 4. Czy okres przechowywania danych osobowych został stosownie ograniczony? | | |
| **IV. Ocena wdrożenia środków pozwalających na realizację praw podmiotów danych** | | |
| 1. Czy zapewnione są odpowiednie środki, aby udzielić podmiotowi danych osobowych wszelkich wymaganych przez prawo informacji? | | |
| 2. Czy zapewnione są odpowiednie środki, aby umożliwić podmiotowi danych osobowych realizację: | prawo dostępu do danych osobowych | |
| | prawo do przenoszenia danych osobowych | |
| | prawo do sprostowania danych osobowych | |
| | prawo do przenoszenia danych osobowych | |
| | prawo do sprzeciwu | |
| | prawo do ograniczenia przetwarzania danych osobowych | |
| 3. Czy ograniczono liczbę odbiorców danych osobowych?<br>4. Czy zapewniono odpowiednie relacje z podmiotami przetwarzającymi dane osobowe?[x] | | |

| | |
|---|---|
| 5. Czy zapewniono odpowiednie zabezpieczenia przy międzynarodowym przekazywaniu danych osobowych (z uwzględnieniem stopnia ochrony występującego w państwie, do którego przekazywane są dane osobowe)? | |
| 6. Czy przeprowadzono uprzednie konsultacje z organem nadzorczym? | |
| **V. Zaangażowanie zainteresowanych stron** | |
| 1. Czy administrator danych dostatecznie ograniczył zidentyfikowane ryzyko? Czy środki zaplanowane są wystarczające do ograniczenia ryzyka do dopuszczalnego poziomu? | |
| 2. Czy przetwarzanie danych odbywa się w celu wykonania zadania realizowanego w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym? | |
| 3. W przypadku odpowiedzi negatywnej na pytanie V.1 lub odpowiedzi pozytywnej na pytanie V.2, czy skonsultowano się z inspektorem ochrony danych w celu uzyskania zaleceń? | |
| 4. Czy udokumentowano decyzję inspektora ochrony danych i wprowadzono konkretne rozwiązanie do oceny skutków dla ochrony danych? | |
| 5. Czy skonsultowano się z użytkownikiem bądź jego przedstawicielem w celu zasięgnięcia opinii w zakresie planowanego przetwarzania danych? | |
| **VI. Monitorowanie i przegląd ryzyka** | |

| | |
|---|---|
| 1. Za pomocą jakich narzędzi prowadzone jest monitorowanie ryzyka? | |
| 2. Jaka jest częstotliwość przeglądu ryzyka? | |
| 3. W jaki sposób dokonuje się przeglądu ryzyka? | |
| 4. Czy po przeprowadzeniu monitoringu i przeglądu ryzyka miała miejsce zmiana klasyfikacji ryzyka? | |
| 5. Czy po zmianie klasyfikacji ryzyka opracowano odpowiednią strategię postępowania w celu jego ograniczenia? | |
| **Podpis osób odpowiedzialnych** | |
| | |
| imię i nazwisko - stanowisko | imię i nazwisko - stanowisko |

[i] Do operacji wymagających przeprowadzenia oceny skutków przetwarzania dla ochrony danych osobowych zalicza się w szczególności (lecz nie wyłącznie):

1. Ocena lub punktacja, w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą” (motyw 71 i 79 RODO).
2. Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku wobec osoby fizycznej (art. 35 ust. 3 lit. a RODO).
3. Systematyczne monitorowanie, tj. przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, w tym gromadzenie danych za pośrednictwem sieci lub systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie (art. 35 ust. 3 lit. c RODO).

   Grupa Robocza Art. 29 wskazuje, iż „systematycznie” uzyskuje jedno z następujących znaczeń:

   a) przeprowadzane w ramach określonego systemu;
   b) wcześniej zaplanowane, zorganizowane lub mające metodyczny charakter;
   c) odbywające się w ramach ogólnego planu gromadzenia danych;
   d) realizowane jako część strategii.

   Pojęcie „miejsca publicznie dostępne” interpretować należy jako miejsca otwarte dla każdego obywatela, np. plac, centrum handlowe, ulica, rynek, stacja kolejowa, biblioteka publiczna. Katalog miejsc publicznie dostępnych
   nie jest zamknięty.
4. Przetwarzanie danych wrażliwych lub danych o charakterze wysoce osobistym: w szczególności kategorii danych osobowych ujętych w art. 9 RODO oraz danych osobowych dotyczących wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10 RODO.

5. Przetwarzanie danych na dużą skalę. Przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, zaleca się wziąć pod uwagę następujące czynniki:
   a) liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;
   b) liczbę danych lub zakres poszczególnych przetwarzanych pozycji danych;
   c) czas trwania lub trwałość czynności przetwarzania danych;
   d) zakres geograficzny czynności przetwarzania.
6. Dopasowanie lub łączenie zbiorów danych, np. pochodzących z co najmniej dwóch operacji przetwarzania danych prowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.
7. Przetwarzanie danych dotyczących osób wymagających szczególnej opieki, pozbawionych przysługujących im praw i wolności oraz kontroli nad zarządzaniem ich danymi osobowymi. Do osób tych zaliczyć należy dzieci, pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl, osoby starsze, pacjenci). Uwzględnić tu należy każdą sytuację, w której można stwierdzić brak równowagi między stanowiskiem osoby, której danej dotyczą, a stanowiskiem administratora.
8. Innowacyjne wykorzystanie lub stosowanie przy przetwarzaniu danych nowych rozwiązań technologicznych lub organizacyjnych takich jak połączenie technologii rozpoznającej odcisk palca i twarzy w celu poprawienia fizycznej kontroli dostępu.
9. Przesyłanie danych poza granice Unii Europejskiej.
10. Przetwarzanie, które „uniemożliwia osobom, których dane dotyczą, wykonywanie lub korzystanie z usługi lub umowy" (art. 22 i motyw 91 RODO). Obejmuje operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu.

W przypadku, gdy operacja przetwarzania danych spełnia co najmniej dwa z ww. kryteriów, należy przeprowadzić
w odniesieniu do takiej operacji ocenę skutków dla ochrony danych. W niektórych przypadkach administrator danych może uznać, że operacja przetwarzania spełniająca tylko jedno z wymienionych powyżej kryteriów będzie wymagała przeprowadzenia oceny skutków dla ochrony danych.

Kategorie operacji <u>niewymagających przeprowadzenia oceny</u> skutków planowanych operacji przetwarzania dla ochrony danych:

1. Operacje, które nie „powodują ryzyka naruszenia praw lub wolności osób, których dane dotyczą".
2. Operacje, których zakres, kontekst i cele przetwarzania są bardzo podobne do operacji przetwarzania, w przypadku których przeprowadzono ocenę skutków dla ochrony danych.
3. Operacje, które zostały sprawdzone przez organ nadzorczy przed majem 2018 roku, w szczególnych warunkach, które nie uległy zmianie, tj. decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE (do czasu ich zmiany, zastąpienia lub uchylenia).
4. Operacje, które mają podstawę prawną w prawie UE lub w prawie państwa członkowskiego, które reguluje dane operacje przetwarzania, oraz jeżeli oceny skutków dla ochrony danych dokonano już z przyjęciem tej podstawy prawnej, chyba że państwo członkowskie uznało za niezbędne dokonanie oceny skutków dla ochrony danych przed rozpoczęciem operacji przetwarzania.
5. Operacje przetwarzania umieszczone w opcjonalnym wykazie (utworzonym przez organ nadzorczy) operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych.

[ii] Charakter przetwarzania danych osobowych – należy wskazać, czy dane osobowe są przetwarzane w sposób całkowicie, częściowo zautomatyzowany czy w sposób inny niż zautomatyzowany; jaka jest częstotliwość

przetwarzania, czy przetwarzanie ma charakter krótko- czy długoterminowy, systematyczny czy sporadyczny, na jaką skalę przetwarzanie jest prowadzone (charakter masowy, znikomy).

[iii] Zakres przetwarzania danych osobowych – należy zawrzeć w tym miejscu opis każdej z planowanych operacji przetwarzania, dokonywanych na danych osobowych.

[iv] Kontekst przetwarzania danych osobowych – w punkcie tym należy wskazać wszelkie okoliczności prawne i faktyczne planowanego przetwarzania – kategorie przetwarzanych danych, kategorie osób, których dane dotyczą, okoliczności zbierania i dalszego przetwarzania danych osobowych (wykonanie obowiązków informacyjnych, zebranie danych na potrzeby wykonania innych czynności prawnych np. zawarcia umowy), a także otoczenie i zagrożenie dla bezpieczeństwa i integralności danych.

[v] Cel przetwarzania danych – należy wskazać konkretne, wyraźne, jednoznaczne, ograniczone i legalne cele. O celach przetwarzania danych decyduje administrator danych. Przetwarzanie danych sprzeczne z celami, dla których zostały zebrane, jest niezgodne z prawem. Przetwarzanie danych w celach nieokreślonych lub określonych nieprecyzyjnie, tj. nieograniczonych i niejasnych powoduje niezgodność przetwarzania z prawem.

[vi] Kategorie aktywów – w tym miejscu należy wyszczególnić:

1. procesy i działania biznesowe – seria powiązanych ze sobą działań lub zadań, które realizują operacje przetwarzania danych osobowych lub prowadzą do osiągnięcia celu przetwarzania danych;
2. personel – wszystkie grupy osób zaangażowane w przetwarzanie danych tj.: decydenci, użytkownicy, personel eksploatacji/utrzymania, twórcy oprogramowania;
3. sprzęt – wszelkie urządzenia fizyczne w organizacji tj.: urządzenia przenośne, stacjonarne, peryferyjne, nośniki danych;
4. siedziba – wszelkie lokalizacje wykorzystywane do przetwarzania danych oraz środki fizyczne potrzebne do ich funkcjonowania tj. siedziba, strefy bezpieczeństwa, usługi komunalne i techniczne;
5. oprogramowanie – wszelkie programy uczestniczące w operacjach przetwarzania danych tj.: systemy operacyjne, aplikacje biznesowe, oprogramowania usługowe, utrzymaniowe lub administracyjne;
6. sieć – wszystkie urządzenia telekomunikacyjne używane do połączenia wielu fizycznie oddalonych komputerów lub elementów systemu informacyjnego, tj.: media i usługi wspierające, przekaźniki aktywne lub pasywne, interfejsy komunikacyjne;
7. kanały transmisji – wszelkie rodzaje mediów służących do przekazu informacji między nadawcą a odbiorcą.

[vii] W przypadku braku kodeksów postepowania regulujących zasady przeprowadzania opisywanej operacji przetwarzania danych należy uwzględnić te informację w odpowiedzi na pytanie.

[viii] Odpowiedź powinna być oparta na analizie i porównaniu odpowiedzi z punktu 2.5 dotyczącej celu przetwarzania danych osobowych ze stanem faktycznym.

[ix] Zgodność z prawem – zgodnie z art. 5 ust. 1 RODO dane powinny być przetwarzane zgodnie z prawem, tj. z ustawami i rozporządzeniami wydanymi na podstawie ustaw z uwzględnieniem interesów podmiotów danych.

[x] Podstawowe wymagania dotyczące treści porozumienia między administratorem a podmiotem przetwarzającym dane osobowe zostały określone w art. 28 RODO.