| Procedura ZSZ<br>POLITYKA BEZPIECZENSTWA DANYCH OSOBOWYCH | | |
|---|---|---|
| SPZOZ<br>PARCZEW | **Zestaw standardów akredytacyjnych 2009**<br>**PN-EN ISO 9001**<br>**PN-EN ISO 14001**<br>**PN-EN ISO 45001** | **Q I-ZI 1.2 -02** |
| | **Wydanie nr 01**<br>**Obowiązuje od dnia 01.01.2014 r.** | **Wydanie nr 03**<br>**obowiązuje od dnia …17.08.2020 r.** |
| | ( tylko na str 1)<br>**Oryginał *** ☐<br>**Egzemplarz użytkowy *** ☐ | ( tylko na str 1)<br>**Kopia nr**** ☐<br>**Wersja elektroniczna** X |

* zaznaczyć x właściwie
** wpisać nr z tabeli rozdzielnika

# POLITYKA

# BEZPIECZEŃSTWA DANYCH OSOBOWYCH

*Niniejszy dokument jest wyłącznie dokumentem wewnętrznym stanowiącym własność administratora danych osobowych.

*Dokument zawiera zestaw praw, procedur i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych, wewnątrz jak i na zewnątrz SPZOZ.

*Polityka odnosi się całościowo do problemu zabezpieczenia danych przetwarzanych tradycyjnie – w formie papierowej, jak i danych przetwarzanych w systemach informatycznych.

*Celem polityki jest wskazanie działań jakie należy wykonać oraz stanowi zasady i reguły postępowania, które należy stosować aby właściwie wykonywać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych.

*Dokument stanowi tajemnicę SPZOZ i nie należy go publikować, lecz rozpowszechniać jedynie wśród pracowników SPZOZ.

## SPIS TREŚCI

## 1. DEFINICJE

**„przetwarzanie”** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

**„dane osobowe”** oznaczają 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;

**„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);

**„administrator - ADO”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

**„podmiot przetwarzający”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

**„inspektor – IOD”** oznacza osobę powołaną do pełnienia funkcji Inspektora Ochrony Danych w organizacji, inspektor odgrywa kluczową rolę w zakresie wspierania „kultury ochrony danych” oraz pomaga w implementacji niezbędnych elementów RODO w codziennej działalności organizacji. Administrator oraz podmiot przetwarzający zapewniają, by inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Inspektor bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Inspektor jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii oraz prawem państwa członkowskiego;

**„administrator systemu informatycznego – ASI”** oznacza osobę wyznaczoną przez administratora do zarządzania systemami informatycznymi, w których przetwarza się dane osobowe w organizacji;

**„osoba wykonująca zawód medyczny”** to osoba uprawniona na podstawie odrębnych przepisów do udzielania świadczeń zdrowotnych oraz osoba legitymująca się nabyciem fachowych kwalifikacji do udzielania świadczeń zdrowotnych w określonym zakresie lub w określonej dziedzinie medycyny, a także osoby wykonujące inne zawody wskazane w tabeli nr 1

załącznika nr 3 do rozporządzenia Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych;

**„pacjent”** oznacza każdą osobę zwracająca się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub osobę wykonującą zawód medyczny;

**„pracownik”** oznacza każdą osobę świadczącą pracę na rzecz administratora na podstawie umowy o pracę oraz innych form zatrudnienia, upoważnioną do przetwarzania danych osobowych w podmiocie, w tym osobę wykonująca zawód medyczny;

**„polityka – PBDO”** oznacza dokument Polityki Bezpieczeństwa Danych Osobowych, jest to zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych, wewnątrz określonej organizacji. Polityka odnosi się całościowo do problemu zabezpieczenia danych przetwarzanych tradycyjnie – w formie papierowej, jak i danych przetwarzanych w systemie informatycznym. Celem polityki jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować aby właściwie wykonywać obowiązki administratora w zakresie zabezpieczenia danych osobowych;

**„dokumentacja medyczna”** oznacza dokumentację medyczną, o której mowa w przepisach ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz wydanych na jej podstawie aktach wykonawczych, a także określona w przepisach odrębnych;

**„profilaktyka zdrowotna”** oznacza wszelkie działania mające na celu zapobieganie niekorzystnym zjawiskom w obszarze zdrowia Pacjenta;

**„świadczenie zdrowotne”** oznacza działania służące zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działania medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich wykonywania;

**„zgoda”** oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

**„naruszenie ochrony danych osobowych”** oznacza 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;

## 2. STRATEGIA I CELE SPZOZ

Głównym celem funkcjonowania Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Parczewie jest wykonywanie działalności leczniczej w rodzaju stacjonarnej i ambulatoryjnej opieki zdrowotnej polegającej na udzielaniu kompleksowych świadczeń zdrowotnych służących zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz innych działań medycznych wynikających z procesu leczenia lub przepisów odrębnych regulujących zasady ich wykonywania.

## 3. PODSTAWA PRAWNA

**Akty prawne:**

1. 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 Osobowych – RODO).

2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
4. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji
5. Ustawa z dnia 6 listopada 2008 r. o Prawach pacjenta i Rzeczniku Praw Pacjenta.
6. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
7. Rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

**Inne dokumenty:**

8. Norma PN-EN ISO 19011:2012.
9. Norma PN-EN ISO/IEC 27001:2017-06.
10. Norma PN-EN ISO/IEC 27002.
11. Wytyczne Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie przetwarzania danych osobowych
12. Bieżące wskazówki UODO oraz Ministerstwa Cyfryzacji.
13. Projekt Kodeksu Postępowania dla sektora ochrony zdrowia wydany zgodnie z art. 40 RODO dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających

## 4. DEKLARACJA STOSOWANIA KIEROWNICTWA

Zmieniająca się rzeczywistość prawna związana z obowiązywaniem RODO wymusiła na administratorze inwentaryzację zasobów danych osobowych i procesów ich przetwarzania. Z uwagi na pojawienie się nowych regulacji administrator deklaruje, że wdroży niezbędne procedury oparte na zasadach i podstawach przetwarzania zawartych w obowiązujących przepisach dotyczących ochrony danych osobowych.

Administrator świadomy wagi problemów i zagrożeń związanych z ochroną danych osobowych, w celu właściwej i skutecznej ochrony tych danych, wprowadza Politykę Bezpieczeństwa Danych Osobowych zwaną dalej „Polityką Bezpieczeństwa". Opracowanie niniejszego dokumentu wynika ze zrozumienia znaczenia bezpieczeństwa danych we współczesnym świecie. Polityka Bezpieczeństwa zawiera wypracowane reguły i procedury takie jak:

- reguły bezpiecznego przechowywania danych osobowych,
- procedura udostępniania danych osobowych (wewnątrz oraz na zewnątrz organizacji),
- procedura realizacji uprawnień wynikających z RODO,
- stosowanie zasady privacy by design, privacy by default.

Ponadto, administrator zobowiązuje się do prowadzenia nadzoru nad przestrzeganiem założeń niniejszego dokumentu. W tym celu ustala coroczny plan sprawdzeń oraz wprowadza obowiązek cyklicznych szkoleń podnoszących świadomość pracownika z zakresu ochrony danych osobowych oraz wprowadzonych w Szpitalu procedur bezpiecznego przetwarzania danych.

## 5. ZASADY PRZETWARZANIA DANYCH

Każdy upoważniony do przetwarzania danych osobowych w imieniu administratora jest zobowiązany do przestrzegania poniższych reguł:

1. Podstawą prawną przetwarzania danych osobowych Pacjentów w celach zdrowotnych przez Zakład są bezpośrednio właściwe przepisy RODO pozostające w związku z przepisami krajowego prawa medycznego.
2. Pracownik jest zobowiązany do przetwarzania danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.
3. Pracownik przed zebraniem danych osobowych od osoby fizycznej zobowiązany jest do umożliwienia zapoznania się z klauzulą informacyjną zawierającą wszelkie informacje dotyczące operacji przetwarzania oraz jej celach.
4. Pracownik czuwa by dane osobowe były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
5. Jeżeli pozyskane dane osobowe mają być wykorzystane w innym celu niż cel, w którym zostały zebrane, przed takim dalszym przetwarzaniem pracownik zobowiązany jest do poinformowania o tym zamiarze Inspektora Ochrony Danych.
6. Dane osobowe gromadzone przez pracownika w SPZOZ muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do realizacji celów, w których są przetwarzane.
7. Pracownik odpowiada za zakres przetwarzanych danych. Zakazuje się gromadzenia danych zbędnych dla osiągnięcia określonego celu przetwarzania danych tj. nadmiarowych.
8. Pracownik nadzoruje by dane osobowe były prawidłowe i w razie konieczności je uaktualnia.
9. Pracownik winien podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
10. Administrator odpowiada za wprowadzenie procedur wyznaczających terminy przechowania danych (okresy retencji) lub procedur określających terminy okresowych przeglądów danych, a pracownik zobowiązany jest do ich przestrzegania.
11. Pracownik ma obowiązek przetwarzać dane w sposób zapewniający odpowiednie bezpieczeństwo w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.
12. Jeżeli pracownik gromadzi dane na podstawie zgody to zobowiązany jest do prowadzenia ewidencji uzyskanych zgód od osób fizycznych, których dane dotyczą.

## 6. PROCEDURA REALIZACJI OBOWIĄZKU INFORMACYJNEGO

**W celu wypełnienia obowiązku informacyjnego wprowadza się następujące reguły:**

1. Przed podjęciem działań z danymi osobowymi należy umożliwić osobie, zapoznanie się z klauzulą informacyjną.
2. Informowanie powinno się dokonać bez prośby zainteresowanego.

3. Obowiązek informacyjny spełnia się poprzez:
    a. umieszczenie informacji na tablicach informacyjnych w przestrzeniach ogólnodostępnych, najczęściej wykorzystywanych przez Pacjentów,
    b. zamieszczenie treści klauzuli informacyjnej na stronie internetowej i w Biuletynie Informacji Publicznej,
    c. umieszczenie klauzul informacyjnych w regulaminie organizacyjnym Szpitala,
    d. umieszczenie klauzul informacyjnych w dokumentach przekazywanych Pacjentowi (w odniesieniu do Pacjentów, którym udzielane są świadczenia w miejscu wezwania).
4. Treść klauzuli należy skonsultować każdorazowo z Inspektorem w celu potwierdzenia zgodności z obowiązującymi przepisami prawa.

## 7. PROCEDURA OBSŁUGI PRAW WYNIKAJĄCYCH Z RODO

Obsługa uprawnień, które zostały zawarte w przepisach rozdziału III RODO stanowi gwarancję poszanowania praw i wolności osób fizycznych i jako podstawowe prawo realizowane jest poprzez wypełnienie poniższych reguł.

1. Administrator gwarantuje by wszelkie przekazywane informacje były sformułowane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
2. Administrator w miejscu ogólnodostępnym (w tym na stronie internetowej i Biuletynie Informacji Publicznej) zamieszcza informację, do kogo i w jakiej formie należy kierować żądanie realizacji praw.
3. Realizacja żądania osób fizycznych w zakresie realizacji praw wynikających z RODO (a w szczególności wskazanych w klauzuli informacyjnej) należy do obowiązków Inspektora.
4. Zgłoszenie żądania osoby fizycznej powinno zawierać:
    a. imię, nazwisko osoby której zgłoszenie dotyczy,
    b. opis zgłaszanego żądania wraz ze wskazaniem ewentualnych zastrzeżeń,
    c. podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
    d. pełnomocnictwo jeśli w imieniu zgłaszającego żądanie kieruje pełnomocnik,
    e. informacje o preferowanej formie odpowiedzi, jeżeli kanał odpowiedzi ma być inny niż zgłoszone żądanie.
5. Pracownik może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby składającej żądanie w przypadku, gdy ma co do niej uzasadnione wątpliwości.
6. Jeżeli zgłoszenie nastąpiło w formie ustnej, pracownik zobowiązany jest do sporządzenia notatki, zawierającej dane o których mowa w punkcie 4.
7. W przypadku skierowania żądania realizacji praw bezpośrednio pracownikowi, zobowiązany jest on najpóźniej w terminie 7 dni przesłać treść żądania inspektorowi.
8. Pracownik jest zobowiązany do udzielania inspektorowi informacji niezbędnych do realizacji żądania osoby fizycznej.
9. Wprowadza się obowiązek rejestracji każdego wniosku o realizację praw osób wpływający bezpośrednio do siedziby organizacji lub na skrzynki mailowe pracowników, poprzez wpisanie do rejestru obsługi praw osób fizycznych wraz ze wskazaniem daty otrzymania wniosku.

## 8. ŚRODKI ORGANIZACYJNE I TECHNICZNE

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

### 8.1. ŚRODKI ORGANIZACYJNE

1. Opracowano i wdrożono Politykę Bezpieczeństwa Danych Osobowych .
2. Opracowano i wdrożono Politykę Zarządzania Systemem Informatycznym.
3. Opracowano i wdrożono procedurę postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.
4. Powołano Inspektora Ochrony Danych.
5. Zastosowano upoważnienia adekwatne do zakresu przetwarzania zgodnego z zajmowanym stanowiskiem służbowym.
6. Upoważnienia do przetwarzania danych pracowników mających dostęp do zasobów systemu monitoringu tj. posiadającym dostęp do serwerowni, techniczną możliwość przeglądania/odtwarzania zapisów z monitoringu oraz pomieszczeń szczególnie chronionych, zawierają szczegółowe umocowania.
7. Wprowadzono ewidencję upoważnień pracowników.
8. W ewidencji upoważnień prowadzi się rejestr osób, które upoważniono do dostępu do pomieszczeń szczególnie chronionych oraz obsługi monitoringu.
9. Wprowadzono obowiązek odbierania oświadczenia pracowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi regulacjami bezpieczeństwa danych osobowych administratora wraz z obowiązkiem zachowania poufności wszelkich informacji uzyskanych w ramach wykonywanych obowiązków, również po ustaniu zatrudnienia.
10. Wprowadzono obowiązek bezpiecznego udostępniania danych osobowych podmiotom zewnętrznym poprzez zawieranie umów powierzenia (lub innych instrumentów prawnych) oraz zobowiązania do zachowania danych osobowych w poufności.
11. Wprowadzono obowiązek cyklicznego szkolenia pracowników z obowiązujących przepisów dotyczących ochrony danych osobowych jak i wewnętrznych regulacji bezpieczeństwa danych osobowych stosowanych przez administratora.
12. Wprowadzono obowiązek cyklicznego szkolenia pracowników w zakresie bezpiecznej obsługi urządzeń i programów służących do przetwarzania danych osobowych.

**Zabezpieczenia we własnym zakresie**

Pracownik zobowiązany jest do przestrzegania zasady czystego biurka i ekranu w szczególności poprzez:

13. Schowanie wszystkich dokumentów, nośników zawierających dane osobowe w miejsce niedostępne dla innych osób w trakcie pracy, w trakcie sprzątania pomieszczeń oraz po zakończeniu pracy.
14. Dbanie o porządek, poprzez pozostawienie na stanowisku pracy wyłącznie dokumentów, które są niezbędne do wykonywania czynności służbowych.

Pracownik zobowiązany jest również do:

1. Powstrzymania się od spożywania napojów i płynnych posiłków oraz palenia papierosów w tym elektronicznych przy urządzeniach i nośnikach danych, w szczególności dokumentacji medycznej.
2. Nie wynoszenia materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów odpowiada w takim przypadku pracownik oraz jego bezpośredni przełożony.
3. Upewnienia się czy nie są widoczne ślady ingerencji osób trzecich, pożaru, zalania lub innego uszkodzenia przy pierwszym wejściu do obszaru przetwarzania w danym dniu.
4. Pilnego strzeżenia dokumentów w formie papierowej, płyt CD/DVD, pamięci i komputerów przenośnych, oraz wszelkich innych urządzeń przenośnych, na których mogą znajdować się dane osobowe.
5. Nadzorowania by nie korzystano z urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających, np. kamer w urządzeniach przenośnych, w obszarach przetwarzania danych chyba że osoba ma odpowiednie upoważnienie.
6. Nieużywania powtórnie dokumentów zadrukowanych jednostronnie.
7. Niszczenia w niszczarce lub chowania do szaf zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy.
8. Zamykania na klucz pomieszczeń w czasie chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu. Zakazane jest pozostawianie kluczy w zamku w drzwiach.
9. Dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

### 8.2. ŚRODKI TECHNICZNE

1. Dane osobowe przechowywane są w uporządkowanych zbiorach, które przechowywane są w sposób uniemożliwiający dostęp osób nieupoważnionych.
2. Pomieszczenia, w których przetwarza się dane są zabezpieczone przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
3. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów, uniemożliwiających ich odtworzenie.

## 9. SZKOLENIA

Kompetencje oraz świadomość personelu mają wpływ na zgodność osiąganych wyników pracy z wymaganiami dotyczącymi zapewnienia bezpiecznego przetwarzania danych osobowych oraz bezpieczeństwa informacji. W tym celu administrator zapewnia aby pracownicy mieli możliwość czynnego udziału w szkoleniach z zakresu bezpiecznego przetwarzania danych osobowych.

### 9.1. SZKOLENIA WSTĘPNE

Szkolenie wstępne, dla nowoprzyjętych pracowników Szpitala odbywa się przed udostępnieniem stanowiska pracy i przeprowadzane jest przez Kierownika Działu Zatrudnienia i Płac bądź osobę przez niego wskazaną. Tematyka szkolenia powinna obejmować m.in.:

1. Terminologię z zakresu ochrony danych osobowych,
2. podstawy prawne obowiązywania ochrony danych osobowych,

3. omówienie roli i odpowiedzialności osób uczestniczących w przetwarzaniu danych osobowych,
4. omówienie istniejących zagrożeń bezpieczeństwa danych osobowych,
5. stosowane przez Administratora środki zabezpieczenia danych osobowych i ochronę stanowiska pracy,
6. obowiązki pracownika w razie naruszenia ochrony danych osobowych, bezpieczeństwa informacji.

### 9.2. SZKOLENIA OKRESOWE

Szkolenie okresowe pracowników, w zakresie przetwarzania danych osobowych, przeprowadza Inspektor Ochrony Danych bądź osoba przez niego wskazana. Szkolenia osób zaangażowanych w proces przetwarzania danych osobowych powinny być prowadzone cyklicznie w związku ze zmieniającymi się zagrożeniami bezpieczeństwa danych osobowych i zmieniającymi się zabezpieczeniami. Szkolenia powinny być przeprowadzane **nie rzadziej niż raz na rok.** Szkolenia okresowe dotyczą również wprowadzanych zmian i aktualizacji systemu bezpieczeństwa danych osobowych.

Tematyka szkolenia obejmuje m.in.:
1. zagrożenia bezpieczeństwa danych osobowych,
2. aktualności o zagrożeniach, skutkach i zabezpieczeniach danych osobowych,
3. skutki naruszenia zasad bezpieczeństwa danych osobowych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, w tym odpowiedzialność prawna,
4. obowiązki pracownika w razie naruszenia ochrony danych osobowych,
5. wybrane elementy dokumentacji ochrony danych osobowych przyjętej u Administratora,
6. sposoby zabezpieczenia danych w systemie informatycznym oraz w formie papierowej w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

### 9.3. ORGANIZACJA SZKOLEŃ

**Planowanie szkoleń**

1. Szkolenia związane z podnoszeniem kwalifikacji oraz poszerzania wiedzy w zakresie bezpieczeństwa przetwarzania danych osobowych są traktowane jako jedno z priorytetowych zadań Szpitala i obowiązków każdego pracownika.
2. Plany szkoleń sporządzane są przez Administratora na podstawie zaistniałych potrzeb (nowi pracownicy) oraz zgłoszeń zapotrzebowania (np. po wystąpieniu incydentu, naruszenia bezpieczeństwa ochrony danych osobowych),
3. Zmiany i uzupełnienia planów szkoleń mogą być wprowadzane na podstawie zgłoszeń pracowników, oraz Administratora, a także Inspektora Ochrony Danych

**Realizacja szkoleń**

1. Szkolenia odbywają się w siedzibie Administratora po uprzednim uzgodnieniu terminu oraz miejsca szkolenia.
2. Szkolenia mogą również odbywać się za pomocą urządzeń takich jak platformy do tworzenia szkoleń online.
3. Kierownik komórki lub pracownik przez niego wyznaczony zobowiązany jest sporządzić listę osób uczestniczących w szkoleniu.

**Dokumentowanie szkoleń**

1. Po zakończonym szkoleniu prowadzący szkolenie zobowiązany jest przekazać do Pełnomocnika ds. ZSZ konspekt (program) przeprowadzonego szkolenia.
2. Dokumentem potwierdzającym odbyte szkolenie jest również podpisana lista obecności osób uczestniczących w szkoleniu przekazywana po zakończonym szkoleniu do Pełnomocnika ds. ZSZ
3. Pełnomocnik ds. ZSZ zobowiązany jest do prowadzenia rejestru szkoleń, w którym odnotowuje, każde przeprowadzone szkolenie z zakresu ochrony danych osobowych.

## 10. STRATEGIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA I FAZIE DOMYŚLNEJ

Uwzględniając koncepcje ochrony danych w fazie projektowania administrator już podczas planowania systemu ochrony danych osobowych wdraża takie środki, by od samego początku chronić przetwarzane dane oraz prywatność osób, których dane dotyczą. W tym celu administrator wprowadza następujące reguły:

1. Każde planowane przedsięwzięcie w SPZOZ musi zostać poprzedzone analizą wpływu planowanych zmian na bezpieczeństwo danych osobowych.
2. Jako planowane procesy, w których administrator zobowiązany jest wziąć pod uwagę bezpieczeństwo danych osobowych wyróżnia się w szczególności:
    a. przystąpienie do przetargu w ramach zamówień publicznych,
    b. przystąpienie do projektów realizowanych ze środków europejskich,
    c. przeprowadzenie nowych akcji marketingowych,
    d. zakup nowego systemu bądź aktualizacja obecnego systemu informatycznego,
    e. zakup nowych systemów ochrony fizycznej (systemy alarmowe, monitoring) jak i systemów bezpieczeństwa IT,
    f. wprowadzenie nowych technologii produkcyjnych i organizacyjnych,
    g. rozwój SPZOZ poprzez tworzenie nowych działów, oddziałów itp.
    h. restrukturyzacja SPZOZ,
    i. zatrudnienie nowych pracowników,
    j. zmiana celów przetwarzania.
3. Administrator bądź wyznaczony przez niego pracownik zobowiązany jest na etapie planowania procesu wdrożyć odpowiedne środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych, a w szczególności zobowiązany jest do stosowania:
    a. pseudonimizacji,
    b. szyfrowania,
    c. minimalizacji danych,
    d. prawidłowości i przejrzystości zbieranych danych,
    e. ograniczenia do niezbędnej ilości zbieranych danych osobowych,
    f. ograniczenia do niezbędnego zakresu przetwarzania danych,
    g. ograniczenia do niezbędnego okresu przechowywania danych,
    h. technik zapewniających odpowiedni poziom dostępności,
4. Na etapie planowania procesów administrator bądź wyznaczony przez niego pracownik zobowiązany jest również:

a. rozważyć na jakiej przesłance legalności zostanie oparty proces przetwarzania danych, przy czym jeśli będzie to zgoda należy przygotować odpowiednio wcześniej jej treść oraz ustalić sposób jej zbierania i odwołania,
b. opracować treść oraz sposób przekazania klauzul zawierających obowiązek informacyjny,
c. administrator zobowiązany jest poinformować inspektora o wszystkich planowanych przedsięwzięciach oraz umożliwić mu podjęcie wszelkich koniecznych działań niezbędnych do zapewnienia bezpieczeństwa przetwarzania danych osobowych,
d. przy wyborze kontrahenta, partnera biznesowego, kooperanta administrator powinien rozważyć, który z nich w najpełniejszy sposób realizuje zasadę bezpiecznego przetwarzania danych osobowych,
e. przy wyborze nowego systemu informatycznego, sytemu ochrony bądź wprowadzaniu zmian technologicznych administrator powinien kierować się również zapewnieniami producenta
dotyczącymi bezpieczeństwa przetwarzania danych osobowych oraz dostosowaniu do wymogów RODO.

Administrator świadomy jest, że zasada ochrony danych w fazie projektowania nie ogranicza się jedynie do procesu planowania, gdyż z przepisów RODO jasno wynika, że ocena zgodności z przepisami dotyczy również etapu realizacji procesu. Wobec powyższego administrator wprowadza zasadę regularnego przeglądu funkcjonowania procesów przetwarzania danych oraz jego elementów składowych poprzez:

1. Audyty systemu informatycznego (uwzględniającego zasady cyberbezpieczeństwa).
2. Sprawdzenie poprawności metod zbierania i przechowywania zgód na przetwarzanie danych osobowych (w tym zasadność ich zbierania, możliwość ich wycofania oraz treści samej zgody).
3. Sprawdzenie realizacji wypełniania obowiązków informacyjnych.
4. Audyty procesów przetwarzania danych osobowych pod względem adekwatności ich przetwarzania oraz ograniczenia do niezbędnej ilości zbieranych danych. W tym celu administrator zobowiązuje:
   a. pracowników odpowiedzialnych za realizację postępowań o udzielenie zamówienia publicznego do przeglądu wszystkich aktualnie prowadzonych postępowań i dostosowanie treści ich ogłoszeń zgodnie z nowymi regulacjami dotyczącymi ochrony danych osobowych, poprzez umieszczenie stosownych klauzul informacyjnych dla zmawiającego oraz oświadczeń wymaganych od wykonawcy,
   b. pracowników odpowiedzialnych za umieszczenie informacji publicznych na stronie Biuletynu Informacji Publicznej (BIP) zobowiązuje do przeglądu umieszczanych na stronie treści pod kątem prawidłowej anonimizacji umieszczanych danych w następujący sposób: administrator zobowiązuje pracownika odpowiedzialnego za umieszczanie informacji publicznych na stronie BIP-u do czuwania nad aktualizacją umieszczanych tam treści.
   c. pracowników odpowiedzialnych za prowadzenie rekrutacji zobowiązuje do przestrzegania procedury rekrutacyjnej określonej w niniejszej Polityce Bezpieczeństwa,
   d. pracowników odpowiedzialnych za prowadzenie projektów realizowanych z funduszy unijnych zobowiązuje do czuwania nad realizacją obowiązków, które spoczywają na

SPZOZ jako administratorze danych przetwarzanych w projekcie (np. w zakresie spełnienia obowiązku informacyjnego),

e. pracowników do wykonywania cyklicznej inwentaryzacji zasobów poczty służbowej i usuwania wiadomości, które utraciły znaczenia dla wypełniania obowiązków służbowych.

f. pracowników upoważnionych do obsługi monitoringu do dokonania analizy obszaru, który obejmie system monitoringu wizyjnego do upewnienia się, czy swoim działaniem nie narusza on godności oraz innych dóbr osób objętych rejestracją.

Realizując zasadę ochrony prywatności i bezpieczeństwa jako właściwości domyślnych *(pivacy by default)* administrator bądź pracownik nadzorujący pracę systemu informatycznego zobowiązany jest do:

1. Konfiguracji systemu informatycznego w taki sposób, aby od momentu jego uruchomienia system zapewniał odpowiedni poziom ochrony według ustawień domyślnych.
2. Konfiguracja systemu informatycznego powinna zapewniać:
   a. aby system nie pozwalał na zbieranie nadmiernej ilości danych osobowych,
   b. aby system wskazywał bądź umożliwiał wprowadzenie danych dotyczących okresu przechowywania danych,
   c. aby system umożliwiał dostęp do danych jedynie upoważnionym w danym zakresie pracownikom.
3. Wprowadzenia zakazu dokonywania jakichkolwiek samodzielnych zmian przez pracowników w ustawieniach fabrycznych komputerów oraz w ustawieniach systemu informatycznego.

## 11. SZACOWANIE RYZYKA DLA DANYCH OSOBOWYCH I OCENA SKUTKÓW

Administrator powinien przeprowadzić ogólną ocenę ryzyka oraz szczegółową ocenę ryzyka, ukierunkowaną na skutki w zakresie naruszenia praw lub wolności osób fizycznych (tzw. ocenę skutków dla ochrony danych).

Ogólną ocenę ryzyka w zakresie bezpieczeństwa przetwarzania informacji, w tym danych osobowych, należy przeprowadzić, biorąc pod uwagę potencjalne negatywne skutki (straty materialne i niematerialne) zarówno dla Administratora, jak i osób, których dane dotyczą. Ocenę skutków dla ochrony danych przeprowadza się natomiast wtedy, gdy istnieje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą.

### 11.1. IDENTYFIKACJA I KLASYFIKACJA AKTYWÓW ORGANIZACJI

Zarządzanie aktywami, jest realizowane w celu zapewnienia wymaganego poziomu bezpieczeństwa ochrony danych osobowych. Należy zidentyfikować i sklasyfikować wszystkie aktywa SPZOZ, które wiążą się z przetwarzaniem danych osobowych. Aktywa to wszystko, co ma wartość dla SPZOZ, rozumieć przez to należy zarówno informacje, w tym dane osobowe, jak i inne zasoby SPZOZ, takie jak: posiadana wiedza, personel, sprzęt, oprogramowanie oraz inne środki techniczne i organizacyjne związane z przetwarzaniem danych osobowych. Identyfikacja i klasyfikacja aktywów w danej organizacji powinna być przeprowadzana na takim poziomie szczegółowości, aby zapewnić niezbędne informacje wymagane w procesie szacowania ryzyka. Posługując się schematem zaczerpniętym z normy ISO/IEC 27005, aktywa te można podzielić na podstawowe i wspierające. Aktywa podstawowe to procesy i działania biznesowe oraz informacje. Aktywa wspierające to sprzęt, oprogramowanie, sieć, personel, siedziba, struktura organizacyjna. Aktywa są chronione ze względu na wymagania wynikające zarówno z przepisów prawa oraz

regulacji wewnętrznych, z których wynika ochrona właściwych aktywów, a także z zasad bezpieczeństwa wymaganych przez SPZOZ.

### 11.2. ZASADY ZARZĄDZANIA AKTYWAMI

Zarządzanie aktywami w SPZOZ odbywa się zgodnie z poniższymi zasadami:

1. Ustalenie odpowiedzialności za aktywa: należy określić właścicieli wszystkich aktywów oraz przydzieloną im odpowiedzialność za utrzymanie odpowiednich zabezpieczeń. Wdrożenie określonych zabezpieczeń może być delegowane przez właściciela aktywów, jednak pozostaje on nadal odpowiedzialny za adekwatną ochronę aktywów.
2. Identyfikacji aktywów: w wyniku identyfikacji aktywów powinno się uzyskać listę aktywów istotnych z punktu widzenia zarządzania ryzykiem oraz listę procesów biznesowych, w których aktywa te są wykorzystywane. Kolejnym istotnym krokiem podczas identyfikacji aktywów jest określenie ich wartości.
3. Akceptowalnego użycia aktywów: w dokumentacji są określone i wdrażane przez administratora zasady dopuszczalnego korzystania z aktywów i zasobów związanych z przetwarzaniem danych osobowych,
4. Klasyfikacji aktywów (szczegółowy opis stosowanych zabezpieczeń): określona jest metoda oraz sposób klasyfikacji aktywów odzwierciedlający wymagania ich ochrony na odpowiednim poziomie.
5. Oznaczania aktywów: stosowane są regulacje wewnętrzne wyznaczające zasady oznaczanie aktywów informacji i postępowania z nimi.

### 11.3. SZACOWANIE RYZYKA

1. Szacowanie ryzyka ma na celu określenie, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i jak dotkliwe straty mogą powstać. W ramach tego działania dla zidentyfikowanych procesów przetwarzania danych i występujących tam aktywów należy wskazać, przeanalizować i oszacować:
    a. występujące zagrożenia dla bezpieczeństwa przetwarzanych danych,
    b. zastosowane środki bezpieczeństwa,
    c. podatność przyjętych rozwiązań z uwzględnieniem zastosowanych środków bezpieczeństwa na urzeczywistnienie się zidentyfikowanych zagrożeń,
    d. potencjalne następstwa w przypadku zaistnienia określonych zagrożeń.
2. Proces zarządzania ryzykiem w bezpieczeństwie informacji realizuje się zgodnie z wytycznymi normy PN-ISO/IEC 27005:2014.
3. Wszyscy pracownicy podczas realizacji zadań biorą pod uwagę ryzyka związane z bezpieczeństwem przetwarzania danych.

Administrator zobowiązany jest do:

a. identyfikacji i klasyfikacji aktywów oraz zasobów informacyjnych na potrzeby analizy szacowania ryzyka,
b. identyfikacji scenariuszy wykorzystania podatności na zagrożenie,
c. szacowania strat dla zasobów użytych w realizacji procesów objętych przeglądem analizy ryzyka,
d. wykonania oceny skutków zgodnie z art. 35 RODO dla operacji przetwarzania danych osobowych ( jeżeli jest wymagana przepisami prawa)

e. wykonania analizy szacowania ryzyka i przeprowadzenia oceny skutków zgodnie z art. 35 RODO, w przypadku wdrożenia nowej technologii (np. nowego systemu informatycznego) w SPZOZ służącej do przetwarzania danych osobowych,
f. w razie potrzeby po dokonaniu oceny skutków, przeprowadzenia zgodnie z art. 36 RODO konsultacji z Urzędem Ochrony Danych Osobowych w sytuacji, gdy Administrator nie jest w stanie zminimalizować wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

4. Zadania inspektora oraz ASI:
   a. przygotowanie Procedury szacowania ryzyka
   b. przygotowanie wykazu aktywów SPZOZ wraz z ich klasyfikacją,
   c. przeprowadzenie analizy szacowania ryzyka i przygotowanie raportu (wyników) szacowania ryzyka w Rejestrze ryzyka,
   d. przygotowanie planu postępowania z ryzykami,
   e. ewentualne konsultowanie oceny skutków i wsparcie administratora w jej wykonaniu.
5. Zadania Administratora:
   a. zatwierdzenie wykazu aktywów SPZOZ (informacyjnych),
   b. zatwierdzenie rejestru ryzyka SPZOZ,
   c. zatwierdzenie planów postępowania z ryzykami,
   d. przeprowadzenie i zatwierdzenie oceny skutków (jeżeli została wykonana).

Ocena skutków jest wykonywana zgodnie z metodologią wskazaną przez Urząd Ochrony Danych Osobowych.

## 12. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH (WEWNĄTRZ SPZOZ)

SPZOZ realizując niniejszą Politykę Bezpieczeństwa w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie pracownikom (w niektórych przypadkach praktykantom, stażystom). Zezwolenie na przetwarzanie danych osobowych realizowane jest poprzez nadanie stosownego upoważnienia.

### 12.1. ZASADY NADAWANIA UPOWAŻNIENIA DO PRZETWARZANIA DANYCH

1. Wniosek do Administratora o nadanie upoważnienia nowemu pracownikowi, w formie elektronicznej lub papierowej kieruje kierownik komórki organizacyjnej.
2. Wniosek od kierownika komórki organizacyjnej zawiera zakres w jakim pracownik będzie mógł przetwarzać dane oraz termin na jaki upoważnienie zostaje przyznane.
3. Od pracownika odbiera się oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi regulacjami bezpieczeństwa danych osobowych administratora.
4. Pracownika zobowiązuje się do zachowania w poufności wszelkich informacji uzyskanych w ramach wykonywanych obowiązków, również po ustaniu zatrudnienia.
5. Fakt nadawania upoważnienia jest odnotowywany w rejestrze upoważnień.
6. W przypadku, gdy podmiot zewnętrzny deleguje swoich pracowników lub osoby świadczące u niego pracę w ramach cywilnoprawnych form zatrudnienia do świadczenia usług pod kontrolą i na fizycznym obszarze przetwarzania danych administratora, oraz jeżeli nie zachodzi relacja

uzasadniająca zawarcie umowy powierzenia, w/w pracownikom lub osobom nadawane jest na piśmie upoważnienie do przetwarzania danych osobowych i odbierane jest od nich pisemne oświadczenie o poufności.

7. Administrator informuje o nadaniu upoważnia do przetwarzania danych pracownikowi osobę administratora systemu informatycznego, który nadaje dostęp do systemu informatycznego poprzez przydzielenie loginu i hasła.
8. Przydzielony login odnotowuje się w rejestrze upoważnień.
9. Nadane przez administratora upoważnienia mogą być modyfikowane w trakcie ich obowiązywania. Modyfikacja może nastąpić w skutek zmiany zakresu wykonywanych prac przez osobę upoważnioną.
10. Ewidencja osób upoważnionych do przetwarzania danych podlega przeglądowi każdorazowo z przeglądem organizacyjnych i technicznych środków bezpieczeństwa, czyli nie rzadziej niż raz w roku.

### 12.2. ZASADY ODBIERANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH

Upoważnienie do przetwarzania danych w określonych sytuacjach może być odebrane pracownikowi przez administratora:

1. Gdy pracownik posługuje się danymi w sposób niewłaściwy, przetwarza je w zakresie wykraczającym poza nadane upoważnienie.
2. Rażącego naruszenia zasad Polityki Bezpieczeństwa.
3. Rozwiązania stosunku pracy bądź innego stosunku prawnego łączącego osobę upoważnioną z administratorem.
4. Zmiany stanowiska pracy, na stanowisko uzasadniające konieczność posiadania upoważnienia w innym zakresie.

W sytuacji odebrania upoważnienia do przetwarzania danych stosuje się niniejsze zasady:

1. Administrator lub osoba wyznaczona informuje pracownika o przebiegu przekazywania obowiązków
   i rozliczeniu się tej osoby z pobranego sprzętu, materiałów i dokumentów należących do pracodawcy według przyjętych procedur.
2. Administrator systemu informatycznego blokuje dostęp pracownika do poczty elektronicznej oraz systemu informatycznego.
3. Administrator lub osoba nadzorująca system informatyczny, zabezpiecza skrzynkę poczty elektronicznej, zasoby serwera lub dysku twardego przypisane do pracownika.
4. Po zablokowaniu dostępu do imiennej skrzynki poczty elektronicznej, osoba nadzorująca system informatyczny, zmienia ustawienia skrzynki poprzez ustawienie przekierowania poczty przychodzącej na adres osoby przejmującej obowiązki, a także uruchomienie komunikatu w formie (autorespondera) automatycznej odpowiedzi/informacji do nadawcy o przekazaniu niniejszej korespondencji do innego odbiorcy.
5. Pracownikowi odbiera się możliwość dostępu do budynków i pomieszczeń należących do organizacji (klucze, karty dostępu, piny…).
6. W przypadku zmiany stanowiska pracy powyższe reguły stosuje się odpowiednio.

7. Fakt odebrania upoważnienia odnotowuje się w rejestrze upoważnień wraz ze wskazaniem daty.

## 13. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH (NA ZEWNĄTRZ SPZOZ)

Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą administratora, dane osobowe mogą być udostępniane w następujących przypadkach:

a. na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów,
b. na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych,
c. na podstawie wniosku osoby, której dane dotyczą.

### 13.1. UDOSTĘPNIANIE DANYCH

1. W przypadku udostępniania danych osobowych na zewnątrz administrator dokonuje oceny sposobu przygotowania danych, a także analizuje sposób i prawidłowość przygotowania danych do udostępnienia.
2. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.
3. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru np. e-mailem, listem poleconym za potwierdzeniem nadania lub innym bezpiecznym sposobem, pozwalającym na udokumentowanie spełnienia prawa.
4. Udostępniając dane osobowe innym podmiotom należy odnotowywać informacje o udostępnieniu bezpośrednio w systemie informatycznym, z którego udostępniono dane lub w inny zatwierdzony sposób.
5. Administrator prowadzi ewidencję podmiotów, którym udostępniono przetwarzane dane. Odnotować należy: informacje o odbiorcy danych, dacie i zakresie udostępnionych danych osobowych.

### 13.2. POWIERZANIE PRZETWARZANIA DANYCH OSOBOWYCH

Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej (w tym elektronicznej) umowy lub innego instrumentu prawnego, określającej w szczególności przedmiot i czas trwania przetwarzania oraz charakter i cel przetwarzania danych. Umowa musi określać również obowiązki i zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy. Regulacje dotyczące sposobu przetwarzania danych oraz obowiązków ciążących na stronach umowy winny zawierać również regulujące dotyczące:

1. Zobowiązania o zachowaniu poufności przez podmiot przetwarzający oraz osoby biorące udział w przetwarzaniu.
2. Obsługi praw jednostki, w szczególności obowiązków informowania administratora o otrzymaniu zgłoszenia i sposobie jego realizacji.

3. Niezwłocznego zgłaszania administratorowi wszelkich podejrzeń o naruszeniu ochrony powierzonych danych.
4. Sposób przekazania danych po zakończeniu trwania przetwarzania.
5. Realizacji uprawnień kontrolnych.
6. Dalszego powierzania danych przez podmiot przetwarzający.

**Procedura zawarcia umowy powierzenia przetwarzania danych osobowych**

1. Pracownik informuje administratora lub inspektora o potrzebie powierzenia danych osobowych do przetwarzania.
2. Inspektor w porozumieniu z pracownikiem przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.
3. Pracownik w projekcie umowy określa procesy przetwarzania powierzonych danych osobowych oraz ich zakres.
4. Sporządzony projekt umowy przedkładany jest administratorowi do podpisu.
5. Zawarta umowa powierzenia odnotowywana jest w rejestrze umów powierzenia prowadzonym przez Kierownika Działu Metodyczno – Organizacyjnego.

## 14. PROCEDURA REJESTRACJI PACJENTÓW

Personel medyczny, a szczególnie pracownicy rejestracji, muszą chronić nie tylko dane osobowe pacjentów, ale również ich prawo do poszanowania intymności i godności. W tym celu przyjmuje się poniższe zasady:

1. W podmiocie wyznaczono miejsca do realizacji procesu rejestracji.
2. Obszar rejestracji został wyznaczony poprzez:
   a. naklejenie na podłodze przed stanowiskiem rejestracji taśmy w jaskrawych barwach wyznaczając obszar, w którym przebywa tylko osoba obsługiwana przez rejestrację,
   b. zamieszczenie komunikatu o konieczności przebywania przy jednym stanowisku rejestracyjnym tylko jednego Pacjenta.
3. We wskazanym obszarze może znajdować się wyłącznie obsługiwany Pacjent (oraz osoba towarzysząca, przedstawiciel ustawowy).
4. Rejestrator zobowiązany jest do czuwania by oczekujący w rejestracji Pacjenci przestrzegali powyższej zasady.
5. Rejestrator weryfikuje tożsamość Pacjenta.
6. Weryfikacji tożsamości Pacjenta dokonuje się poprzez kontrolę okazanego przez Pacjenta dokumentu potwierdzającego tożsamość zawierającego co najmniej zdjęcie, imię i nazwisko oraz PESEL lub w przypadku jego braku inny numer jednoznacznie identyfikujący Pacjenta. Dokumentem potwierdzającym tożsamość jest w szczególności: dowód osobisty, legitymacja studencka, legitymacja szkolna, prawo jazdy, paszport lub inny dokument urzędowy ze zdjęciem.
7. Jeżeli Pacjent odmawia okazania dokumentu weryfikującego tożsamość można poprosić go o podanie danych identyfikacyjnych tj. PESEL lub inny numer identyfikacji wskazany w przepisach prawa ustnie lub poprzez zastosowanie kartek/formularzy, na których Pacjent

wpisuje wymagane dane identyfikacyjne. Kartki/formularze muszą być niszczone zgodnie z procedurą niszczenia dokumentów utylizacją nośników.

### 14.1. ZASADY WYWOŁYWANIA PACJENTÓW

1. Wezwanie do gabinetu lekarskiego następuje z wykorzystaniem numeru nadanego podczas rejestracji lub po godzinie wyznaczonej wizyty.
2. Wezwanie po imieniu jest możliwe wyłącznie w sytuacji, gdy w kolejce oczekujących jest tylko jedna osoba o danym imieniu.
3. Dopuszcza się by wezwanie Pacjenta odbywało się poprzez wskazanie imienia oraz numerku/godziny wizyty.
4. Zastosowane rozwiązania nie mogą w żadnym zakresie zakłócać udzielania świadczeń opieki zdrowotnej ani narażać zdrowia lub życia Pacjentów.
5. Jeżeli istnieje zagrożenie zdrowia lub życia Pacjenta możliwe jest zastosowanie metody identyfikacji tożsamości z wykorzystaniem nazwiska bądź imienia i nazwiska oraz innych niezbędnych danych osobowych Pacjenta.
6. W przypadku Szpitalnych Oddziałów Ratunkowych oraz Izb Przyjęć pełniących funkcję SOR możliwe jest wywoływanie Pacjentów przez zastosowanie metody identyfikacji tożsamości z wykorzystaniem nazwiska bądź imienia i nazwiska.

## 15. ZASADY WYKONYWANIA OBCHODÓW LEKARSKICH

Osoba wykonująca zawód medyczny podczas udzielania świadczeń zdrowotnych ma obowiązek poszanowania intymności i godności osobistej Pacjenta, w szczególności w czasie udzielania świadczeń zdrowotnych. W celu zagwarantowania poszanowania praw Pacjenta przyjmuje się następujące reguły:

1. W czasie obchodu lekarskiego na sali chorych mogą przebywać jedynie uprawnione osoby tj. personel medyczny, opiekun faktyczny, opiekunowie ustawowi Pacjenta.
2. Drzwi od sali, jeżeli to możliwe powinny zostać zamknięte tak, aby osoby nieuprawnione nie mogły usłyszeć informacji przekazywanych podczas obchodu.
3. Na życzenie Pacjenta w trakcie udzielania świadczenia może być obecna osoba bliska z zastrzeżeniem, że w przypadku obchodu opuszcza salę chorych, jeżeli omawiany jest stan zdrowia innego Pacjenta.
4. Osoby biorące udziału w obchodzie inne niż udzielające świadczeń zdrowotnych np. inni lekarze, pielęgniarki, fizjoterapeuci, biorą udział w obchodzie bez zgody Pacjenta, jeżeli są osobami wykonującymi zawód medyczny, tylko wtedy, gdy jest to niezbędne ze względu na rodzaj świadczenia.

## 16. PROCEDURA REKRUTACYJNA

Przetwarzanie danych osobowych kandydatów do pracy odbywa się z należytym poszanowaniem prawa do prywatności wobec czego wprowadza się następujące zasady przy prowadzeniu rekrutacji:

1. Administrator (lub pracownik odpowiedzialny za rekrutację) zamieszczając ogłoszenie rekrutacyjne zobowiązany jest do zawarcia w jego treści klauzuli informacyjnej dotyczącej przetwarzania danych osobowych kandydata oraz oświadczeń tj.:
   - oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych zawartych w CV, liście motywacyjnym lub innych załączonych dokumentach (jeśli przekazane dane obejmują szczególne kategorie danych, bądź wykraczają poza dane, o których mowa w art. $22^1$ k.p.),
   - oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych w celu wykorzystania ich w kolejnych rekrutacjach prowadzonych przez organizację – o ile w danym przypadku administrator zdecyduje o woli pozostawienia dokumentów rekrutacyjnych osób niewybranych na potrzeby przyszłych rekrutacji.
2. W przypadku braku zawarcia stosownej zgody w dokumentach aplikacyjnych pracownik kontaktuje się z kandydatem w celu odebrania stosownego oświadczenia o wyrażeniu zgody. Jeżeli pracownik nie uzyska oświadczenia, zobowiązany jest do usunięcie dokumentów aplikacyjnych w sposób trwały.
3. Pracownik odpowiedzialny za rekrutację przechowuje dokumenty aplikacyjne w miejscu zabezpieczonym przed dostępem osób nieuprawnionych.
4. Administrator określił czas w jakim dokumenty aplikacyjne są przechowywane, tj. 9 miesięcy. Po jego upływie dokumenty są niszczone w sposób trwały – stosując procedurę niszczenia dokumentów i utylizacji nośników.

## 17. PROCEDURA MONITORINGU

Zapewniając ochronę wizerunku osób fizycznych objętych monitoringiem stosowanym przez SPZOZ wprowadza się następujące reguły.

1. Administrator zapewnia prawidłowe funkcjonowanie monitoringu mając na względzie by nie naruszał on prawa do prywatności osób fizycznych oraz czuwa by przetwarzanie danych odbywało się w granicach prawa.
2. Monitoring jest prowadzony w celu zwiększenia bezpieczeństwa i porządku publicznego na terenach obiektów szpitalnych oraz dla poprawy ochrony osób i mienia przebywających w budynkach szpitala. Ponadto, Szpital prowadzi monitoring w celu zapewnienia bezpieczeństwa pacjentów znajdujących się w stanie zagrożenia życia lub zdrowia, stałego nadzoru nad osobą z zaburzeniami psychicznymi przebywającą w pomieszczeniu przeznaczonym do izolacji oraz kontroli wykonania czynności związanych z tym rodzajem środka przymusu bezpośredniego.
3. Obowiązek informacyjny realizowany jest poprzez oznaczenie strefy objętej systemem monitoringu tabliczką zawierającą piktogram kamery wraz ze skróconym obowiązkiem informacyjnym.
4. Klauzula informacyjna zawierająca pełny obowiązek informacyjny jest udostępniona wewnątrz budynku(tablica ogłoszeń) oraz na stronie internetowej oraz BIP.
5. Regulamin użytkownika monitoringu wizyjnego udostępniony jest na stronie internetowej oraz BIP.
6. Przed rozpoczęciem pracy monitoringu wizyjnego administrator (lub wskazana przez niego osoba) dokonuje analizy obszaru, który obejmie system monitoringu wizyjnego upewniając się, iż swoim działaniem nie naruszy on godności oraz innych dóbr pracownika. Monitoring wizyjny

może obejmować jedynie obszar przylegający do SPZOZ i to w takim zakresie jakim nie narusza on prywatności osób postronnych.

7. System monitoringu działa całą dobę.
8. Rejestracji i zapisaniu na nośniku fizycznym podlega tylko obraz. System monitoringu nie rejestruje dźwięku.
9. Zapis z monitoringu przechowuje się przez okres 30 dni z wyjątkiem oddziału psychiatrycznego. Po upływie tego terminu dane są automatycznie nadpisywane.
10. W oddziale psychiatrycznym zapis z monitoringu przechowuje się przez okres co najmniej 12 miesięcy od dnia jego zarejestrowania, nie dłużej jednak niż przez 13 miesięcy od dnia jego zarejestrowania, o ile nie zostanie on zabezpieczony jako dowód w sprawie w przypadku toczącego się postępowania. Po upływie terminu przechowywania zapis usuwa się w sposób uniemożliwiający jego odzyskanie. Z usunięcia zapisu sporządza się protokół, w którym należy wskazać datę tej czynności oraz imię i nazwisko osoby, która dokonała usunięcia. Dopuszcza się niszczenie zapisu na urządzeniu monitorującym przez jego automatyczne nadpisanie w przypadku, gdy warunki techniczne tego urządzenia umożliwiają przechowywanie zapisu przez okres, o którym mowa w zdaniu pierwszym.- *art. 18 e. ustawy o ochronie zdrowia psychicznego*.
11. W uzasadnionych przypadkach, gdy urządzenia monitoringu wizyjnego zarejestrowały zdarzenie związane z naruszeniem bezpieczeństwa osób i mienia, okres przechowywania danych może ulec wydłużeniu o czas niezbędny do zakończenia postępowania, którego przedmiotem jest zdarzenie zarejestrowane przez monitoring wizyjny.
12. Rejestrator umieszcza się w pomieszczeniu, do którego dostęp mają tylko upoważnione osoby.
13. Dostęp do poglądu z kamer w czasie rzeczywistym ma pracownik upoważniony do tego procesu.
14. Zapis z systemu monitoringu może być udostępniony uprawnionym organom w zakresie realizowania przez nie ustawowych zadań np. policji, sądom, prokuraturom na ich pisemny wniosek.
15. Osoba zainteresowana zabezpieczeniem danych z monitoringu zwraca się pisemnie do administratora z prośbą o ich zabezpieczenie przed automatycznym usunięciem. Wniosek musi zawierać informacje takie jak:
    a. dane osoby zgłaszającej,
    b. opis zdarzenia wraz ze wskazaniem przybliżonego czasu i miejsca,
    c. cel wykorzystania nagrania.
16. Pracownik sporządza kopię nagrania z monitoringu wizyjnego za okres, którego dotyczy wniosek osoby zainteresowanej oraz oznacza ją w sposób trwały poprzez:
    a. numer porządkowy kopii,
    b. datę sporządzenia kopii,
    c. okres, którego dotyczy nagranie,
    d. źródła danych.
17. Nagrania są udostępniane w sposób nienaruszający wizerunku osób trzecich widocznych na nagraniu.
18. Kopia nagrania przechowywana jest 6 miesięcy.

19. Po upływie 6 miesięcy zabezpieczona na wniosek osoby zainteresowanej kopia nagrania podlega zniszczeniu.
20. Kopia nagrania podlega zaewidencjonowaniu w rejestrze kopii z monitoringu wizyjnego.
21. Rejestr zawiera następujące informacje:
    a. numer porządkowy kopii,
    b. datę sporządzenia kopii,
    c. okres, którego dotyczy nagranie,
    d. źródło danych,
    e. informację o udostępnieniu ze wskazaniem daty,
    f. informację o zniszczeniu kopii ze wskazaniem daty.
22. Nośnik z kopią nagrania przekazuje się wnioskodawcy za pokwitowaniem odbioru.

## 17. NISZCZENIE DOKUMENTÓW I UTYLIZACJA NOŚNIKÓW

Niniejsza procedura utylizacji dotyczy zarówno nośników w formie papierowej, jak i elektronicznej.

1. Nośniki przeznaczone do zniszczenia przechowywane są w wydzielonym i zabezpieczonym miejscu.
2. Dokumenty papierowe zawierające dane osobowe, niszczone są w niszczarce, w sposób uniemożliwiający ich odczytanie.
3. Wycofane z użytku nośniki elektroniczne (uszkodzone, wyeksploatowane) przeznaczone do utylizacji pozbawia się wcześniej zapisu danych lub w sposób mechaniczny pozbawia się możliwości ich odczytu.
4. Poprzez trwałe usunięcie danych rozumie się wykorzystanie specjalistycznego oprogramowania, uniemożliwiającego odtworzenie danych.
5. Pracownik niszczy dokumentację papierową samodzielnie, a niepotrzebne lub uszkodzone nośniki elektroniczne przekazuje administratorowi lub wyznaczonemu pracownikowi.
6. Utylizacja nośników elektronicznych odbywa się po uzyskaniu zgody administratora i zostaje potwierdzona protokołem zniszczenia.
7. Wzór protokołu zniszczenia ustala administrator. Protokół powinien zawierać w szczególności datę, przyczynę zniszczenia nośników oraz podpisy osób uprawnionych do zniszczenia nośników.
8. W przypadku korzystania z usług zewnętrznego podmiotu utylizującego dokumentację zawierającą dane osobowe niezbędne jest uprzednie zawarcie umowy powierzenia danych osobowych. Administrator lub wyznaczony pracownik zobowiązany jest do odebrania protokołu zniszczenia wystawionego przez podmiot zewnętrzny.

## 18. UTRZYMANIE CZYSTOŚCI

Pomieszczenia, w których znajdują się dane osobowe zarówno w postaci papierowej jak i elektronicznej, które przechowywane są na stacjach komputerowych bądź innych urządzeniach umożliwiających dostęp do danych, stanowią obszar przetwarzania danych osobowych. Dostęp do tych obszarów powinien być kontrolowany zwłaszcza w zakresie w jakim jest on udostępniany

osobom sprzątającym. Niezależnie od tego czy osoby sprzątające pomieszczenia, w których przetwarza się dane osobowe są zatrudnione wewnątrz struktury organizacyjnej administratora czy są to osoby świadczące usługi z zewnątrz, administrator wprowadza następujące reguły:

1. Wszystkie osoby sprzątające zobowiązane są do zachowania w tajemnicy danych osobowych znajdujących się w obszarze przetwarzania danych osobowych podczas wykonywania czynności.
2. Oświadczenie o zachowaniu w tajemnicy powinno być odbierane przez administratora przed przystąpieniem osoby sprzątającej do wykonywania czynności.
3. Oświadczenie o zachowaniu w tajemnicy danych osobowych może stanowić oddzielny dokument bądź zostać zawarte w treści umowy o pracę bądź innej podstawy świadczenia usług.
4. Przed rozpoczęciem sprzątania pracownicy zobowiązani są zastosować się do zasady czystego biurka oraz zasady czystego ekranu oraz umożliwić wejście i rozpoczęcie wykonywanych czynności przez osobę sprzątającą.
5. Osoby sprzątające pomieszczenia, w których przetwarzane są dane osobowe powinny wykonywać czynności sprzątania pod nadzorem i w obecności pracowników.
6. Administrator wprowadza zakaz opuszczania pomieszczeń w trakcie ich sprzątania i pozostawiania nawet na krótką chwilę osób sprzątających bez nadzoru w trakcie wykonywanych przez nią czynności.
7. W przypadku realizacji usług bez nadzoru pracownika, pracownik zobowiązany jest do zabezpieczenia obszaru przetwarzania poprzez umieszczenie dokumentacji/nośników w szafkach zamykanych na klucz oraz wylogowania z systemu informatycznego.
8. Powyższe zasady mają również zastosowanie do innych osób świadczących usługi np. remontowe, serwisowe.

## 20. POSTANOWIENIA KOŃCOWE

1. Administrator zobowiązany jest zapoznać z dokumentem wszystkie osoby przetwarzające dane osobowe.
2. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce Bezpieczeństwa może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
3. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy RODO oraz przepisy Ustawy.
4. Pracownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Bezpieczeństwa. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących w organizacji pracownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.
5. W sprawach nieokreślonych w niniejszym dokumencie należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
6. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą Polityką Bezpieczeństwa oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
7. Integralną częścią Polityki są jej załączniki, opisane w wykazie.

8. Zmiany treści Polityki i/lub załączników lub ich aktualizacja jest wprowadzana zgodnie z procedurą PZ/O/01 Nadzór na dokumentami.
9. Polityka wchodzi w życie z dniem podpisania.

## 21. WYKAZ ZAŁĄCZNIKÓW

Nr 1. Upoważnienie pracownika;

Nr 2. Oświadczenie o zachowaniu w poufności;

Nr 3. Oświadczenie o zachowaniu w poufności osoby nie przetwarzającej danych osobowych;

Nr 4. Procedura realizacji praw osób fizycznych;

Nr 6. Plik Excel – „Rejestry i ewidencje", zawierający rejestr kategorii przetwarzania danych, ewidencję upoważnień, ewidencję umów powierzenia, ewidencję naruszeń, rejestr realizacji praw osób, których dane dotyczą, ewidencję szkoleń.

Dokument opracowany we współpracy z **POLSKIM CENTRUM AUDYTU TELEKOMUNIKACJI**

| **Opracował** | **Sprawdził** | **Zatwierdził** | |
|---|---|---|---|
| IOD Agnieszka Czerniak<br><br>Podpis nieczytelny | IOD Agnieszka Czerniak<br><br>podpis nieczytelny | **Pełnomocnik ds. ZSZ**<br>Mgr Elżbieta Ludwińska<br>Data 06.08.2020 r.<br>podpis nieczytelny | **Dyrektor SPZOZ ( ADO)**<br>Mgr Janusz Hordejuk<br>Data 07.08.2020 r.<br>podpis nieczytelny |

ROZDZIELNIK do **POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH wydanie 03**

| Lp. | Dokument | Kto otrzymuje | Data | Podpis |
|---|---|---|---|---|
| 1. | Oryginał procedury | Pełnomocnik ds. ZSZ | 07.08.2020 r. | |
| 2. | Kopia nr 1 | ZKZSz | 10.08.2020 r. | Wersja elektroniczna |
| 3. | Kopia nr 2 | OIT | 10.08.2020 r. | Wersja elektroniczna |
| 4. | Kopia nr 3 | SOR | 10.08.2020 r. | Wersja elektroniczna |
| 5. | Kopia nr 4 | Blok operacyjny | 10.08.2020 r. | Wersja elektroniczna |
| 6. | Kopia nr 5 | O/ internistyczno – kardiologiczny | 10.08.2020 r. | Wersja elektroniczna |
| 7. | Kopia nr 6 | O/ ginekologiczno – położniczy | 10.08.2020 r. | Wersja elektroniczna |
| 8. | Kopia nr 7 | O/ chirurgiczny | 10.08.2020 r. | Wersja elektroniczna |
| 9. | Kopia nr 8 | O/ dziecięcy | 10.08.2020 r. | Wersja elektroniczna |
| 10. | Kopia nr 9 | O/ geriatryczny | 10.08.2020 r. | Wersja elektroniczna |
| 11. | Kopia nr 10 | O/ psychiatryczny | 10.08.2020 r. | Wersja elektroniczna |
| 12. | Kopia nr 11 | Dział rehabilitacji | 10.08.2020 r. | Wersja elektroniczna |
| 13. | Kopia nr 12 | Pracownia diagnostyki obrazowej | 10.08.2020 r. | Wersja elektroniczna |
| 14. | Kopia nr 13 | O/ rehabilitacyjny | 10.08.2020 r. | Wersja elektroniczna |
| 15. | Kopia nr 14 | Dział zatrudnienia i płac | 10.08.2020 r. | Wersja elektroniczna |
| 16. | Kopia nr 15 | Zespół Poradni specjalistycznych | 10.08.2020 r. | Wersja elektroniczna |
| 17. | Kopia nr 16 | Dział finansowo- księgowy | 10.08.2020 r. | Wersja elektroniczna |
| 18. | Kopia nr 17 | Dział zamówień publicznych | 10.08.2020 r. | Wersja elektroniczna |
| 19. | Kopia nr 18 | Dział metodyczno – organizacyjny | 10.08.2020 r. | Wersja elektroniczna |
| 20. | Kopia nr 19 | Inspektor bhp | 10.08.2020 r. | Wersja elektroniczna |
| 21. | Kopia nr 20 | Inspektor OC i ppoż | 10.08.2020 r. | Wersja elektroniczna |
| 22. | Kopia nr 21 | Kuchnia | 10.08.2020 r. | Wersja elektroniczna |
| 23. | Kopia nr 22 | Sterylizatornia | 10.08.2020 r. | Wersja elektroniczna |
| 24. | Kopia nr 23 | Apteka | 10.08.2020 r. | Wersja elektroniczna |
| 25. | Kopia nr 24 | Dział informatyczny | 10.08.2020 r. | Wersja elektroniczna |
| 26. | Kopia nr 25 | Dział utrzymania ruchu i gospodarczy | 10.08.2020 r. | Wersja elektroniczna |
| 27. | Kopia nr 26 | Pracownia endoskopowa | 10.08.2020 r. | Wersja elektroniczna |