# Upoważnienie nr ……/……..

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. wsprawie 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) (Dz.U.UE.L.2016.119.1), niniejszym upoważniam:

Pana/Panią *(imię i nazwisko)*……, odbywającego/odbywającą staż kierunkowy na podstawie porozumieniaz dnia ……..
do przetwarzania danych osobowych w tym szczególnych kategorii danych, o których mowa w art. 9 ust. 1 ogólnego rozporządzenia o ochronie danych w zakresie powierzonych do realizacji zadań na podstawie porozumienia oraz zgodnie z poleceniami administratora.

Upoważnienie ważne jest od dnia ……. do dnia ……

Jednocześnie informuję, że:

1. jest Pan/Pani zobowiązany do przetwarzania danych osobowych wyłącznie na polecenie administratora zgodnie z celami wynikającymi z powierzonych przez administratora danych osobowych zadań oraz zasadami zawartymi w Polityce ochrony danych,
2. jest Pan/Pani zobowiązany w trakcie realizacji powierzonych zadań oraz po zakończeniu ich realizacji do zachowania w tajemnicy danych osobowych oraz informacji o środkach technicznych i organizacyjnych służących ich ochronie, do których miał Pan/ miała Pani dostęp w trakcie wykonywania powierzonych zadań,
3. udostępnianie danych osobowych lub umożliwianie dostępu do danych osobowych osobom nieuprawnionym podlega odpowiedzialności cywilnej wobec podmiotu danych, karze grzywny oraz karze ograniczenia wolności,
4. niniejsze upoważnienie nie upoważnia do udzielania dalszych upoważnień i wygasa z dniem ukończenia stażu kierunkowego.

.....
(*data i podpis ADO)*

## Oświadczenie osoby upoważnionej

1. Zapoznałam/em się i rozumiem zasady dotyczące przestrzegania i ochrony danych, w szczególności wynikających z ogólnego rozporządzenia o ochronie danych, Polityki Ochrony Danych w Szpitalu w Ostródzie S.A. oraz wObowiązkach osób upoważnionych do przetwarzania danych osobowych i zobowiązuję się do ich przestrzegania pod rygorem odpowiedzialności dyscyplinarnej oraz przewidzianej przepisami prawa.
2. Zobowiązuję się do zgłaszania wszelkich podejrzeń o naruszeniu bezpieczeństwa danych osobowych przełożonemu lub wyznaczonej do tego osobie.
3. Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych oraz środków organizacyjnych i technicznych służących ich zabezpieczeniu, także po zaprzestaniu przetwarzania danych zakończeniu stażu zawodowego,
4. Zobowiązuję się do poszanowania praw i wolności innych osób w tym poszanowania ich życia prywatnego oraz dobrego imienia.
5. Zostałam/em poinformowany o możliwości monitorowania mojej pracy na komputerach służbowych.
6. Zobowiązuję się brać udział w organizowanych przez Szpital w Ostródzie S.A. szkoleniach stacjonarnych ie-learningowych w zakresie ochrony danych osobowych.

Upoważnienie otrzymałem

.....
*(data i podpis upoważnionego)*

## Obowiązki osób upoważnionych do przetwarzania danych osobowych

Podczas współpracy ze Szpitalem w Ostródzie S.A. (dalej: Szpital), każdy pracownik jest zobowiązany do stosowania niżej określonych zasad, które wynikają z przepisów obowiązującego prawa, w szczególności z 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) oraz z obowiązującej w Szpitalu Polityki Ochrony Danych.

### Obowiązkowe szkolenie

1. Przed rozpoczęciem pracy wypełnij online krótkie szkolenie dotyczące ochrony danych osobowych. Żeby się do niego zalogować wejdź na stronę:

   https://szkolenie-crm.edpo.pl

   i wpisz hasło:

   34_SzkolenieDaneOsobowe

2. Wykonanie szkolenia jest obowiązkowe dla wszystkich pracowników mających dostęp do danych osobowych niezależnie od formy zatrudnienia.

### Obowiązki związane z przetwarzaniem danych osobowych

1. Pamiętaj, że przetwarzanie danych osobowych *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*.
2. Pamiętaj, żeby gromadzić (zbierać) i przetwarzać tylko te dane, które wskazane zostały w przepisach prawa (np. dotyczących prowadzenia dokumentacji medycznej lub rozliczania procedur medycznych) lub są bezwzględnie niezbędne do realizacji celu, dla którego je zbierasz.
3. Pamiętaj, że możesz przetwarzać dane osobowe tylko w zakresie zadań, jakie zostały Ci zlecone w ramach porozumienia, umowy lub kontraktu. Każda zmiana celu przetwarzania (wykorzystanie zebranych danych do nowego zadania) rodzi skutki prawne. W takiej sytuacji koniecznie skontaktuj się z Inspektorem Ochrony Danych – dane kontaktowe na końcu dokumentu.
4. Zawsze sprawdzaj prawidłowość przetwarzanych danych oraz potwierdzaj tożsamość osób, z którymi rozmawiasz.
5. Zbierając dane osobowe od osób, których dane dotyczą pamiętaj o upewnieniu się, że właściciel danych otrzymał obowiązek informacyjny. W razie wątpliwości poinformuj, że znajduje się on na stronie www Szpitala (https://szpital-ostroda.pl/ochrona-danych-osobowych-informacja-o-przetwarzaniu-danych/) lub pokaż wydrukowaną treść takiego dokumentu wyświetl treść informacji jeżeli właściciel danych o to poprosi.
6. Po zakończeniu współpracy ze Szpitalem zwróć wszystkie arkusze, notatki i dokumenty zawierające dane osobowe bezpośredniemu przełożonemu.
7. Planując (jeszcze przed jego rozpoczęciem) nowe zadania, z którym wiąże się przetwarzanie danych osobowych skontaktuj się z Inspektorem Ochrony Danych w celu ustalenia zasad przetwarzania danych osobowych jeszcze przed jego rozpoczęciem.
8. Zawsze kiedy podczas realizacji zadań okaże się, że powinieneś udostępnić innemu podmiotowi lub osobie dane osobowe – pamiętaj, żeby przestrzegać przepisów prawa w tym zakresie. Koniecznie skontaktuj się w tym celu ze swoim bezpośrednim przełożonym, Inspektorem Ochrony Danych lub Radcą Prawnym Szpitala.

### Obowiązki związane z bezpieczeństwem danych osobowych

1. W celu ograniczenia dostępu do danych osobowych przez osoby nieuprawnione (czyli takie, które nie są właścicielem tych danych, nie zostały upoważnione przez właściciela danych lub nie są pracownikami Szpitala posiadającymi upoważnienie do przetwarzania danych osobowych) pamiętaj o poniższych zasadach:
   a. w sytuacji tego wymagającej zadbaj o zapewnienie poufności rozmów prowadzonych z pacjentami, członkami ich rodzin lub klientami/kontrahentami Szpitala w ten sposób, żeby treść tych rozmów nie mogła być usłyszana przez osoby nieuprawnione.
      Pamiętaj, że zgodnie z zaleceniami Prezesa Urzędu Ochrony Danych Osobowych i Rzecznika Praw Pacjenta nie ma konieczności zachowania poufności rozmów na tematy dotyczące ogólnych zasad wykonywania procedur

medycznych, procedur obowiązujących w szpitalu oraz innych ogólnie dostępnych informacji. Taką poufność należy natomiast bezwzględnie zachować omawiając indywidulane kwestie dotyczące wyłącznie danej osoby.

b. nie dopuszczaj do dostępu do danych osobowych i metod ich zabezpieczania przez osoby nieuprawnione, w szczególności:
   - przechowuj i przenoś dokumenty w taki sposób, aby osoby nieuprawnione nie mogły zapoznać się z ich treścią,
   - wykonuj bieżącą pracę tylko z dokumentami niezbędnymi do wykonania aktualnego zadania lub obsługi danego pacjenta,
   - po zakończeniu zadania odkładaj dokumenty do przeznaczonych do tego teczek, segregatorów, szaf lub szuflad (zasada czystego biurka),
   - zapewnij, aby osoby nieuprawnione nie mogły odczytać danych osobowych z monitora wykorzystywanego komputera, telefonu lub tabletu (zasada czystego ekranu),
   - jeżeli zajdzie taka potrzeba, niszcz wadliwe dokumenty, projekty dokumentów lub ich kopie oraz wszelkie wydruki w przeznaczonych do tego niszczarkach o klasie niszczenia nie niższej niż P-3, urządzenia takie dostępne są w Szpitalu,
   - nie udostępniaj dokumentów zawierających dane osobowe osobom nieuprawnionym,
   - nie pozostawiaj bez nadzoru osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe,
   - niezwłocznie odbieraj z drukarki wydrukowane arkusze zawierające dane osobowe,

2. Posiadając dostęp do systemów informatycznych, koniecznie zapewnij ich bezpieczeństwo w szczególności poprzez:
   - zachowanie w poufności identyfikatorów i haseł dostępowych do systemów informatycznych i nieudostępnianie tych elementów innym osobom upoważnionym (np. innym pracownikom) i osobom nieuprawnionym,
   - nieprzechowywanie zapisanych identyfikatorów i haseł w obszarze stanowiska pracy lub łatwo dostępnych miejscach,
   - niedopuszczenie do możliwości odczytania wprowadzanego do systemu hasła przez inne osoby upoważnione lub osoby nieuprawnione,
   - dokonywanie samodzielnie, bez wezwania, zmian wszystkich wykorzystywanych haseł co 90 dni; pamiętaj, że hasła powinny posiadać co najmniej 10 znaków, w tym duże i małe liter, cyfry, oraz znaki specjalne,
   - niewprowadzanie zmian w udostępnionych systemach informatycznych bez poinformowania pracowników Komórki IT,
   - nieinstalowanie jakichkolwiek dodatków lub programów bez poinformowania pracowników Komórki IT,
   - nieudzielanie dostępu lub zdalnego dostępu do systemów informatycznych osobom nieuprawnionym,
   - korzystanie wyłącznie z programów udostępnionych przez Szpital w celu realizacji zadań,
   - korzystanie wyłącznie z zaufanych serwisów internetowych w celu realizacji zadań,
   - niekorzystanie w celach prywatnych z udostępnionych kont, poczty elektronicznej oraz innych programów i serwisów internetowych,
   - nieprzesyłanie na prywatne konta pocztowe lub do prywatnych zasobów sieciowych (np. chmury) jakichkolwiek dokumentów służbowych,
   - korzystanie wyłącznie wydanych przez Szpital z zaufanych nośników danych (pendrive, dysk przenośny itp.) zabezpieczonych hasłem dla celów służbowych,
   - stosowanie się do zaleceń osoby odpowiedzialnej za prawidłowe funkcjonowanie udostępnionego systemu informatycznego,
   - przesyłanie danych osobowych drogą mailową wyłącznie w formie zaszyfrowanej oraz przekazywanie hasła do zaszyfrowanego pliku inną drogą komunikacji,
   - przesyłanie maili do wielu odbiorców z wykorzystaniem opcji „UDW", czyli ukryte do wiadomości,
   - oznaczanie niechcianej poczty elektronicznej jako spam.

3. Wykorzystując udostępniony sprzęt komputerowy lub inne urządzenia przetwarzające dane osobowe, koniecznie zapewnij ich bezpieczeństwo w szczególności poprzez:
   - dbanie o powierzony przez Szpital do użytkowania sprzęt informatyczny, w tym nieudostępnianie go osobom nieuprawnionym (także osobom znanym i członkom rodzin) oraz niepozostawianie powierzonego sprzętu w miejscach dostępnych osobom nieuprawnionym, uniemożliwienie korzystania z udostępnionego sprzętu przez osoby nieuprawnione,
   - użytkowanie powierzonego sprzętu komputerowego, urządzeń medycznych, urządzeń mobilnych i przenośnych nośników danych poza siedzibą jednostki wyłącznie za zgodą Prezesa Zarządu Szpitala oraz w sposób zapewniający poufność danych, a także niepozostawianie tych urządzeń bez nadzoru, przewożenie ich w sposób uniemożliwiający kradzież lub uszkodzenie w wyniku działania czynników środowiskowych,
   - zwrot powierzonego sprzętu na żądanie Szpitala,

– stosowanie się do zaleceń pracowników Komórki IT,

4. Za niestosowanie powyższych zasad oraz naruszenia w zakresie bezpieczeństwa informacji pracownicy zatrudnieni na podstawie umowy o pracę ponoszą odpowiedzialność dyscyplinarną zgodnie z zasadami przyjętymi w Szpitalu, a w przypadku osób zatrudnionych na podstawie umów cywilnoprawnych odpowiedzialność cywilną zgodnie z przepisami prawa.

## Monitorowanie wykorzystywanych zasobów IT

1. Pamiętaj, że Szpital prowadzi monitoring służbowych skrzynek email pracowników, udostępnionych systemów informatycznych i urządzeń służących przetwarzaniu informacji oraz połączeń internetowych (dalej monitoring IT), w celu właściwego i zgodnego z przyjętymi w Szpitalu zasadami użytkowania udostępnionych pracownikowi narzędzi pracy.
2. Monitoring IT wykonywany jest za pomocą systemu nVision i polega na rejestrowaniu oraz przeglądaniu raportów aktywności pracownika na poszczególnych urządzeniach lub w ramach udostępnionych zasobów.
3. Dane pochodzące z monitoringu IT będą przechowywane nie dłużej niż 3 miesiące od daty ich zgromadzenia, lub do czasu prawomocnego zakończenia postępowania prowadzonego na podstawie prawa, w zakresie zarejestrowane informacje mogą stanowić dowód w tym postępowaniu.
4. Monitoringiem IT objęte są w szczególności:
    a. uruchamiane programy oraz czas ich wykorzystywania,
    b. odwiedzane witryny internetowe, bez wyświetlania treści prywatnych (np. treści maili lub haseł),
    c. monitorowanie wydruków (nazwy plików, ilość stron),
    d. monitorowanie zapisywania, kopiowania, usuwania plików zarówno w obrębie danego urządzenia jak i innymi urządzeniami podłączanymi do urządzenia monitorowanego,
    e. podłączanie urządzeń zewnętrznych do komputerów Szpitala lub bezpośrednio do sieci Szpitala.
5. Powyższe czynności mają na celu zapewnienie bezpieczeństwa informacji i spełnienie wymagań prawnych w zakresie krajowego systemu cyberbezpieczeństwa, krajowych ram interoperacyjności oraz ochrony danych osobowych.
6. W zakresie przetwarzania, w tym udostępniania danych osobowych pochodzących z prowadzonego monitoringu stosuje się zasady i procedury zawarte w przyjętej w Spółce dokumentacji dotyczącej ochrony danych osobowych (Polityka Ochrony Danych).

## Informowanie o incydentach

1. Incydent oznacza naruszenie bezpieczeństwa prowadzące do:
    a. przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania – np. kradzież, zgubienie, zniszczenie dokumentów, nośnika danych (pendrive, dysk przenośny, komputer itp.),
    b. przypadkowego lub niezgodnego z prawem zmodyfikowania – np. zaszyfrowanie danych, lub przypadkowa zmiana ich treści powodująca, że danych nie można odtworzyć,
    c. nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – np. ujawnienie treści dokumentu, przesłanie maila z danymi osobowymi na niewłaściwy adres, niestosowanie opcji UDW: wysyłając maila do wielu osób, jeżeli ujawnienie ich adresów kontaktowych nie jest zamierzone, a nawet ujawnienie danych członkom rodziny.
2. Jednym z obowiązków nałożonym przepisami prawa w związku z naruszeniami, jest ewidencjonowanie i ewentualne zgłaszanie przez Szpital wszelkich naruszeń dotyczących przetwarzania danych osobowych.
3. Jeżeli zauważyłeś naruszenie lub podejrzewasz, że miało ono miejsce koniecznie i niezwłocznie skontaktuj się z pracownikiem Komórki IT lub Inspektorem Ochrony Danych.

## Kontakty i informacje dodatkowe

1. Inspektorem Ochrony Danych Osobowych jest **Pan Michał Cupiał**,
   nr telefonu: **881-266-777**
   email: **info@edpo.pl**
2. Kontakt do pracowników Komórki IT:
   nr telefonu: **662-110-251**
   email: **informatyk@szpital-ostroda.pl**
3. Wszelkie instrukcje i procedury dotyczące ochrony danych osobowych i bezpieczeństwa informacji dostępne są w formie drukowanej w sekretariacie Szpitala oraz w wersji elektronicznej w udostępnionym folderze sieciowym.

**Pamiętaj wszystkie te dokumenty są dokumentami poufnymi i nie wolno ich udostępniać podmiotom zewnętrznym.**

## ADMINISTRATOR DANYCH OSOBOWYCH

SZPITAL W OSTRÓDZIE S.A., ul. Wł. Jagiełły 1, 14-100 Ostróda, REGON 511398725, NIP 741-18-87-468, tel.: 89 646-06-00, e-mail: sekretariat@szpital-ostroda.pl, dalej „Szpital".

## CEL, CZAS I PODSTAWA PRAWNA PRZETWARZANIA DANYCH OSOBOWYCH

Dane osobowe przetwarzane są:

1. **na podstawie art. 6 ust. 1 lit. b** 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) (zwanym dalej RODO):
   a) **w celu organizacji i rozliczenia stażu kierunkowego na podstawie zawartego porozumienia,**
   b) przetwarzanie danych osobowych przez Szpital jest obowiązkowe w celu zawarcia, realizacji i rozliczenia porozumienia. Nieprzetwarzanie tych danych oznaczałoby brak możliwości odbycia stażu,
   c) przez okres trwania porozumienia oraz do końca okresu przedawnienia potencjalnych roszczeń z porozumienia, z uwzględnieniem przepisów dotyczących archiwizacji dokumentacji.
2. **na podstawie art. 6 ust. 1 lit. f RODO**:
   a) **w celu zapewnienia bezpieczeństwa pracowników, pacjentów oraz ochrony mienia poprzez prowadzenie monitoringu wizyjnego** za pomocą środków technicznych umożliwiających rejestrację obrazu, z wyłączeniem możliwości nagrywania dźwięku, co jest prawnie uzasadnionym interesem Szpitala.
   b) przez 7 dni od dnia nagrania, a następnie nagranie z monitoringu wizyjnego zawierające wizerunek zostanie usunięte. Jeżeli nagranie stanowi lub może stanowić dowód w sprawie, to przechowywane będzie do czasu zakończenia prawomocnego postępowania.

## INFORMACJA O ODBIORCACH DANYCH OSOBOWYCH

Dane osobowe stażystów mogą być ujawniane podmiotom realizującym zadania na rzecz Szpitala, takim jak:

- operator pocztowy - Poczta Polska,
- dostawcy systemów informatycznych w celu zapewnienia zgodnego z prawem i bezpiecznego przetwarzania danych osobowych,
- pracownik służby BHP, m.in. w celu przeprowadzenia szkoleń i wydania zaświadczeń,
- komisje ds. orzekania i zdarzeniach medycznych.

Każdorazowo ujawnianie danych realizowane jest zgodnie z obowiązującymi przepisami prawa, w tym na podstawie powierzenia przetwarzania danych osobowych podmiotom działającym w imieniu i na rzecz Szpitala.

## PRZYSŁUGUJĄCE PRAWA

W związku z przetwarzaniem danych osobowych stażyście przysługuje prawo żądania dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia ich przetwarzania. Stażysta posiada także prawo wniesienia sprzeciwu wobec przetwarzania, które odbywa się na podstawie art. 6 ust. 1 lit. f RODO, a także prawo do przenoszenia danych w zakresie w jakim są one przetwarzane w systemach informatycznych w celu realizacji porozumienia. A także prawo wniesienia skargi do organu nadzorczego Prezesa Urzędu Ochrony Danych Osobowych w Warszawie, ul. Stawki 2, 00-193 Warszawa.

## KONTAKT Z INSPEKTOREM OCHRONY DANYCH

Kontakt z Inspektorem Ochrony Danych możliwy jest pod adresem e-mail: iod@szpital-ostroda.pl lub na wskazany wyżej adres Szpitala.

.....

(data i podpis Stażysty)