WEWNĘTRZNA POLITYKA BEZPIECZEŃSTWA

w Zakładzie Lecznictwa Podstawowego i Specjalistycznego
MEDICOR Sp. z.o.o.
ul. Cichociemnych 14, 44-100 Gliwice

NIP: 6312298159

REGON: 276986910

Spis treści

I. Procedury z zakresu ochrony danych osobowych

Niniejszy dokument stanowi wewnętrzną politykę przetwarzania danych w podmiocie MEDICOR Sp. z.o.o. na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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 Ustawy z dnia 10 maja 2018 r.(Dz. U. 2018 poz.1000).

Dokument zawiera zbiór procedur z zakresu ochrony danych osobowych potrzebnych przy dostosowywaniu podmiotu do przepisów unijnych.

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, techniczne, w tym: oprogramowanie systemowe, aplikacje oraz użytkowników.

Wewnętrzna Polityka przetwarzania danych w **Zakład Lecznictwa Podstawowego i Specjalistycznego MEDICOR Sp. z.o.o** ul. Cichociemnych 14, 44-100 Gliwice (dalej oznaczane także jako: MEDICOR Sp. z.o.o.) ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj. :

a) naruszeń danych osobowych pacjentów, pracowników, zleceniobiorców rozumianych jako prywatne dobro powierzone MEDICOR Sp. z.o.o.;
b) naruszeń przepisów prawa oraz innych regulacji;
c) utraty lub obniżenia reputacji;
d) strat finansowych ponoszonych w wyniku nałożonych kar;
e) zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

II. Definicje

Przez użyte w niniejszych Procedurach określenia należy rozumieć:

1. **RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) General Data Protection Regulation - GDPR** 2016/679 z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
2. **Ustawa o Ochronie Danych Osobowych** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. Poz. 1000).
3. **Administrator** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
4. **Dane osobowe** informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna.
5. **Dane karne –** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.
6. **Dane dzieci** – oznaczają dane osób poniżej 16 roku życia.
7. **Osoba** – oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
8. **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; do danych o stanie zdrowia należą także informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, takie jak w szczególności: numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych;

9. **Zbiór danych osobowych** – „zbiór danych” oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
10. **Inspektor Ochrony Danych (Data protection officer (DPO) - IOD** – osoba wyznaczona przez administratora (administratorów-wspólny dla kilku podmiotów) lub podmiot przetwarzający, posiadająca kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań wynikających z zapisów RODO.
11. **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora, czyli działającym na jego zlecenie – instytucja powierzenia przetwarzania danych.
12. **Współadministratorzy** - co najmniej dwóch administratorów, którzy mają wspólny cel przetwarzania i wspólnie ustalają sposoby przetwarzania oraz uzgadniają, w sposób jasny i przejrzysty, zakresy swojej odpowiedzialności – to dwaj równorzędni administratorzy tego samego zbioru danych.
13. **Przetwarzanie danych** – 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.
14. **System tradycyjny** – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze.
15. **Zabezpieczenie danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
16. **Użytkownik** – rozumie się przez to upoważnionego przez administratora danych osobowych wyznaczonego do przetwarzania danych osobowych pracownika.
17. **ZLPiS MEDICOR**- Zakład Lecznictwa Podstawowego i Specjalistycznego MEDICOR Sp. z.o.o. ul. Cichociemnych 14, 44-100 Gliwice.

III. Zasady przetwarzania danych

Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Prezes Spółki, Zarząd Spółki, a w ramach upoważnienia wszyscy członkowie personelu. ZLPiS MEDICOR powinna też zapewnić zgodność postępowania kontrahentów Podmiotu z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez ZLPiS MEDICOR.

Niniejsza polityka ochrony danych osobowych jest dokumentem opisującym sposób przetwarzania danych osobowych oraz obowiązki podmiotu leczniczego działającego w charakterze Administratora danych, przetwarzanych w związku z prowadzoną działalnością leczniczą.

Ochrona danych osobowych w ZLPiS MEDICOR. Zasady ogólne

1. Filary ochrony danych osobowych :
   a) Legalność – ZLPiS MEDICOR dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

b) Bezpieczeństwo – ZLPiS MEDICOR zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.
c) Prawa jednostki – ZLPiS MEDICOR umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
d) Rozliczalność – ZLPiS MEDICOR dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

2. Zasady ochrony danych

ZLPiS MEDICOR przetwarza dane osobowe z poszanowaniem następujących zasad:
a) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
b) rzetelnie i uczciwie (rzetelność);
c) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
d) w konkretnych celach i nie „na zapas" (minimalizacja);
e) nie więcej niż potrzeba (adekwatność);
f) z dbałością o prawidłowość danych (prawidłowość);
g) nie dłużej niż potrzeba (czasowość);
h) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

3. System ochrony danych

System ochrony danych osobowych w ZLPiS MEDICOR składa się z inwentaryzacji danych. ZLPiS MEDICOR dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym przypadków przetwarzania danych szczególnych kategorii i danych karnych;

4. Rejestr.

ZLPiS MEDICOR opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania (Rejestr) który **stanowi zał. Nr 1** do niniejszego dokumentu. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Placówce.

5. Obsługa praw jednostki.

ZLPiS MEDICOR spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
a) obowiązki informacyjne. ZLPiS MEDICOR przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
b) możliwość wykonania żądań. ZLPiS MEDICOR weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;
c) obsługa żądań. ZLPiS MEDICOR zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane;
d) zawiadamianie o naruszeniach. ZLPiS MEDICOR stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

6. Minimalizacja.

ZLPiS MEDICOR posiada zasady i metody zarządzania minimalizacją (privacy by default), a w tym:

a) zasady zarządzania adekwatnością danych;
b) zasady reglamentacji i zarządzania dostępem do danych;
c) zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

7. Bezpieczeństwo.

ZLPiS MEDICOR zapewnia odpowiedni poziom bezpieczeństwa danych czyli stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

8. Przetwarzający.

ZLPiS MEDICOR posiada zasady doboru przetwarzających dane na rzecz Spółki, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

9. Eksport danych.

ZLPiS MEDICOR posiada zasady weryfikacji, czy ZLPiS MEDICOR nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Liechtenstein, Islandię, USA) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

10. Privacy by design.

ZLPiS MEDICOR zarządza zmianami wpływającymi na prywatność już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

11. Przetwarzanie transgraniczne.

ZLPiS MEDICOR posiada zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

12. Dane szczególnych kategorii i dane karne.

ZLPiS MEDICOR identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych ZLPiS MEDICOR postępuje zgodnie z przyjętymi zasadami w tym zakresie.

13. Profilowanie.

ZLPiS MEDICOR identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych, i utrzymuje mechanizmy zapewniające zgodność tego procesu z prawem. W przypadku zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji ZLPiS MEDICOR postępuje zgodnie z przyjętymi zasadami w tym zakresie.

14. Współadministrowanie.

ZLPiS MEDICOR identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

ZLPiS MEDICOR stosuje metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

ZLPiS MEDICOR dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza oraz ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Spółce, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu z Administratorem w tym celu.

IV. Podstawy prawne przetwarzania danych osobowych

1. Działalność administratora jako podmiotu leczniczego regulują w szczególności:

   - Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta z dnia 6 listopada 2008r
   - Ustawy o działalności leczniczej z dnia 15 kwietnia 2011r
   - Ustawa o służbie medycyny pracy z dnia 27 czerwca 1997r;
   - Ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;
   - Ustawa o zawodach lekarza i lekarza dentysty z dnia 5 grudnia 1996;
   - Rozporządzenie Ministra Zdrowia w sprawie rodzajów dokumentacji medycznej służby medycyny pracy, sposobu jej prowadzenia i przechowywania oraz wzoru stosowanych dokumentów;
   - Rozporządzenie Ministra Zdrowia z dnia 11 października 2019 r. zmieniające rozporządzenie w sprawie rodzajów dokumentacji badań i orzeczeń psychologicznych, sposobu jej prowadzenia, przechowywania i udostępniania oraz wzorów stosowanych dokumentów.

   wraz nowelizacjami.

   Jako podmiot leczniczy, administrator przetwarza dane osobowe w celach zdrowotnych na podstawie art. 9 ust. 2 lit. h Rozporządzenia.

2. Przez cele zdrowotne rozumie się:
   - **profilaktykę zdrowotną** - w szczególności poprzez informowanie pacjentów o możliwości pobierania świadczeń zdrowotnych, przekazywanie materiałów edukacyjnych,

   - **medycynę pracy oraz ocenę zdolności pracownika do pracy** – w szczególności poprzez sprawowanie zadań jednostki służby medycyny pracy, w tym poprzez badania wstępne, okresowe oraz kontrolne na podstawie umowy zawartej pomiędzy administratorem a pracodawcą,

   - **diagnozę medyczną oraz leczenie** - w szczególności poprzez udzielanie świadczeń zdrowotnych oraz prowadzenie dokumentacji medycznej,

- **zapewnienie opieki zdrowotnej oraz zarządzanie systemami opieki zdrowotnej** w szczególności poprzez: rejestrację pacjenta do usług administratora, odbieranie oraz archiwizację oświadczeń pacjentów wynikających z realizacji ich praw pacjenta, wykorzystywanie i utrzymywanie infrastruktury informatycznej służącej wspieraniu procesu leczenia, rozliczanie udzielonych świadczeń, wymianę danych osobowych pacjenta z innym podmiotem leczniczym w ramach zachowania ciągłości leczenia.

3. W zakresie wykraczającym poza cele zdrowotne administrator przetwarza dane na podstawie:

   - zgody pacjenta (art. 6 ust. 1 lit. a Rozporządzenia) - w celach marketingowych
   - prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f Rozporządzenia) w celu dochodzenia roszczeń i obrony przed roszczeniami.

4. Zgoda, o której mowa w pkt 4 jest dobrowolna i jej wyrażenie jest świadomym działaniem pacjenta. Nieudzielenie zgody nie powoduje dla pacjenta żadnych negatywnych konsekwencji, w szczególności nie skutkuje odmową udzielenia świadczenia zdrowotnego ani nie warunkuje udzielenia tego świadczenia.

5. ZLPiS Medicor przetwarza również w ramach działalności gospodarczej dane Pracowników w związku z zatrudnieniem.

6. Jako Pracodawca, administrator przetwarza dane osobowe w celach zatrudnienia na podstawie art. 9 ust. 2 lit. b Rozporządzenia apPodstawą przetwarzania jest:
   - Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, m.in. art. 22 [1] i 22[2]
   - Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (t.j. Dz.U. z 2003 r. Nr 169, poz. 1650 z późn. zm.).
   - Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz. U. z 2018 r. poz. 217 z późn. zm.).
   - Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (t.j. Dz. U. z 2017 r. poz. 894).
   - Ustawa z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (t.j. Dz. U. z 2018 r. poz. 1270 z późn. zm.).
   - Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (t.j. Dz. U. z 2017 r. poz. 1778 z późn. zm.).
   - Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t.j. Dz. U. z 2018 r. poz. 1510 z późn. zm.).
   - Ustawa z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (t.j. Dz. U. z 2018 r. poz. 800 z późn. zm.).
   - Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (t.j. Dz. U. z 2018 r. poz. 1509 z późn. zm.).

ZLPiS Medicor przetwarza również dane w związku z zastosowaniem monitoringu wizyjnego w celach ochrony mienia podstawie art. 6 ust. 1 lit. f Rozporządzenia. Podstawą przetwarzania jest Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, m.in. art. 22.

V. Obowiązki personelu

1. Dostęp do danych osobowych pacjentów posiada personel medyczny (lekarze, pielęgniarki oraz rejestratorki) oraz inne osoby podczas wykonywania czynności pomocniczych niezbędnych przy udzielaniu świadczeń zdrowotnych, adekwatnie do ich obowiązków służbowych.

2. Personel administratora zobowiązany jest do:

    - zapoznania się oraz stosowania przepisów prawa w zakresie ochrony danych osobowych określonych w ZLPiS MEDICOR, w tym Rozporządzenia;
    - ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem do tych danych, ich nieuzasadnioną modyfikacją lub zniszczeniem;
    - niszczenia w bezpieczny sposób wszelkich nośników zawierających dane osobowe (w formie papierowej jak i elektronicznej);
    - korzystania z zasobów informatycznych oraz sprzętu w sposób zgodny z ich przeznaczeniem i w sposób bezpieczny, m.in. poprzez okresową zmianę haseł, zachowanie poufności loginów i haseł oraz niepozostawianie sprzętu bez nadzoru;
    - niezwłocznego informowania przełożonych o zaobserwowanych nieprawidłowościach, które mogą mieć wpływ na bezpieczeństwo przetwarzanych danych osobowych;
    - przechowywania dokumentacji zawierającej dane osobowe w przeznaczonych do tego miejscach, z ograniczonym dostępem osób trzecich, zwłaszcza dokumentacji medycznej pacjentów;
    - niepozostawiania stanowisk recepcyjnych/punktów rejestracji pacjenta bez nadzoru.

3. Personel ponosi odpowiedzialność za należyte wykonywanie swoich obowiązków i jest on pouczony przez administratora o sankcjach wynikających z nieprawidłowości w tym zakresie, w tym o odpowiedzialności karnej.

VI. Obszar przetwarzania danych osobowych

Dane osobowe przetwarzane są w budynku mieszczącym się przy ul. Cichociemnych 14, 44-100 Gliwice

VII. Opis środków bezpieczeństwa

1. ORGANIZACYJNE
    - do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora, bądź osobę przez niego upoważnioną;
    - ustalono zasady przetwarzania i bezpieczeństwa
    - ustalono zasad wydawania kluczy do pomieszczeń biurowych
    - stworzono wewnętrzną politykę przetwarzania danych;
    - stworzono procedurę postępowania w przypadku naruszeń;
    - osoba upoważniona do przetwarzania danych osobowych w systemie informatycznym została zaznajomiona z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;

- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
- przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
- przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych osobowych;
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
- wprowadzono zasadę „czystego biurka" i „białej kartki";
- dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych osobowych niemożliwa była identyfikacja osób;
- informacji telefonicznych nie udziela się, względnie udziela się po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych osobowych;
- powołano Administratora systemów informatycznych i określono jego obowiązki;
- powołano IOD oraz stworzono regulamin funkcjonowania Inspektora

2. TECHNICZNE
   - używane laptopy wyposażono w indywidualną ochronę antywirusową ESED NOD32 Antivirus™;
   - zastosowano wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika ok.3 min;
   - komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkownika;
   - określono procedury tworzenia kopii bezpieczeństwa;
   - serwis www. medicor.gliwice.pl posiada aktualny certyfikat SSL;
   - korzysta się zdalnych, autoryzowanych, bezpiecznych połączeń VPN;
   - konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych przechowywanych w systemie informatycznym wyłącznie za pośrednictwem używanych aplikacji;
   - komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła;
   - sieć zabezpieczono firewall na routerze;
   - skrzynka pocztowa na domenie;
   - zastosowano zasilanie awaryjne UPS w razie awarii zasilania;

3. FIZYCZNE
   - dokumentację zawierającą dane osobowe umieszcza się w zamykanych pomieszczeniach;
   - obszar, na którym przetwarzane są dane osobowe, chroniony jest poprzez zastosowanie:
     - zamykane pomieszczenia
     - zamykane szafy
     - monitoring wizyjny
     - stały nadzór Pracowników
   - pomieszczenie serwerowni zabezpieczony jest poprzez zastosowanie:
     - zamek szyfrowy
     - drzwi antywłamaniowe

- przeciwpożarowe
- czujka zalania

VI. Zasoby danych osobowych (czynności przetwarzania)

Nazwa zbioru danych osobowych/ czynność przetwarzania	Przetwarzanie danych osobowych w systemie informatycznym (wskazać nazwę)	Struktura
1. Dane Pracowników	e-nowa kadry i płace pakiet office bankowość elektroniczna Płatnik	Imię i nazwisko, adres zamieszkania, nr telefonu , imiona rodziców, data i miejsce urodzenia, numer ewidencyjny PESEL, wykształcenie, wykształcenie uzupełniające, przebieg dotychczasowego zatrudnienia, dodatkowe uprawnienia, umiejętności, zainteresowania, stan rodzinny, powszechny obowiązek obrony, seria i numer dowodu osobistego
2. Dane finansowo-księgowe- kontrola wydatków	e-nowa księgowość bankowość elektroniczna	Imię i nazwisko, adres i nazwa firmy, nr NIP i REGON, nr konta bankowego, nr faktury, data i miejsce wystawienia faktury, rodzaj usługi
3. Archiwum - archiwizacja dokumentów zgodnie z przepisami	Wszystkie systemy Papierowo, pakiet office	Imię i nazwisko, adres zamieszkania, nr telefonu , imiona rodziców, data i miejsce urodzenia, numer ewidencyjny PESEL, wykształcenie, wykształcenie uzupełniające, przebieg dotychczasowego zatrudnienia, dodatkowe uprawnienia, umiejętności, zainteresowania, stan rodzinny, powszechny obowiązek obrony, seria i numer dowodu osobistego, adres i nazwa firmy, nr NIP i REGON, nr konta bankowego, nr faktury, data i miejsce wystawienia faktury, rodzaj usługi, dokumentacja medyczna dotycząca podopiecznych(zlecenia lekarskie, wypisy, interwencje pogotowia), dane rodzin lub opiekunów prawnych
4. Dane z serwisu internetowego	www. medicor.gliwice.pl	
5. Zbiór danych osób ubiegających się o zatrudnienie- proces rekrutacji,	Papierowo, skrzynka email	Imię i nazwisko, adres zamieszkania, nr telefonu , data urodzenia, wykształcenie, wykształcenie uzupełniające, przebieg dotychczasowego zatrudnienia, dodatkowe uprawnienia, umiejętności, zainteresowania, stan cywilny, powszechny obowiązek obrony, seria i numer dowodu osobistego, wizerunek

6. Dane osób z którymi są zawierane umowy cywilnoprawne (umowy zlecenia i umowy o dzieło) – zawarcie umów zlecenia i o dzieło	Papierowo i pakiet office,	Imię i nazwisko, adres zamieszkania, nr telefonu, e-mail, imiona rodziców, data i miejsce urodzenia, numer ewidencyjny PESEL, dodatkowe uprawnienia, seria i numer dowodu osobistego
7. Dane Pacjentów/ Opiekunów prawnych/ osób upoważnionych przez Pacjenta do odbioru dokumentacji/recept/	Program eWUŚ mMedica, ECGLAB, ABPM, pakiet office,	Imię i nazwisko, nr telefonu, PESEL lub numer D.O. dane dotyczące płatności, dane dotyczące zdrowia: diagnozy, orzeczenia, zlecenia lekarskie, wyniki badań diagnostycznych i kontrolnych, wykonane zabiegi, zlecenia leków, recepty, elektroniczne zwolnienia pacjentów, skierowania do poradni specjalistycznych, przebyte zabiegi i operacje,
8. Kontrahenci	pakiet office,	Imię i nazwisko, nr telefonu, dane dotyczące płatności, adres i nazwa firmy, nr NIP i REGON, nr konta bankowego,

VII. Regulamin ochrony danych osobowych

Realizując postanowienia ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000) jak i również Rozporządzenia 2016/679 wprowadza się zestaw reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.

Regulamin zawiera:

- Zasady bezpiecznego użytkowania sprzętu stacjonarnego IT
- Zasady korzystania z oprogramowania
- Zasady korzystania z poczty elektronicznej
- Ochrona antywirusowa
- Procedura rozpoczęcia, zawieszenia i zakończenia pracy
- Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe
- Postępowanie z danymi osobowymi w wersji papierowej
- Zapewnienie poufności danych osobowych
- Postępowanie dyscyplinarne

Zasady bezpiecznego użytkowania sprzętu stacjonarnego IT

Sprzęt IT służący do przetwarzania zbioru danych osobowych składa się z 2 laptopów oraz 24 komputerów stacjonarnych i innych nośników. Użytkownik zobowiązany jest korzystać ze Sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem. Zobowiązany jest także do zabezpieczenia Sprzętu IT przed dostępem osób nieupoważnionych, a w szczególności zawartości ekranów monitorów.
Obowiązkiem jest też natychmiastowe zgłoszenie zagubienia, utraty lub zniszczenia powierzonego mu Sprzętu IT. Samowolne otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

Zasady korzystania z oprogramowania

- Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi,
- nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Pracodawcę/Zleceniodawcę na swoje własne potrzeby ani na potrzeby osób trzecich.
- Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.
- Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Pracodawcę/Zleceniodawcę. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.
- Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.

W przypadku naruszenia któregokolwiek z powyższych postanowień Pracodawca /Zleceniodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

Zasady korzystania z poczty elektronicznej

- System Poczty Elektronicznej jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
- Przy korzystaniu z Systemu Poczty Elektronicznej, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
- Użytkownicy nie mają prawa korzystać z Systemu Poczty Elektronicznej dla celów prywatnych.
- Korzystanie z Systemu Poczty Elektronicznej dla celów służbowych, nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych, a także na wydajność Systemu Poczty Elektronicznej.
- Użytkownik jest świadomy, że wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem Systemu Poczty Elektronicznej przetwarzane są wyłącznie na jego własną odpowiedzialność. Użytkownik wyraża zgodę na prowadzenie kontroli tych wiadomości przez Pracodawcę/Zleceniodawcę. Pracodawca nie będzie w tej sytuacji odpowiadać za przypadkowe naruszenie dóbr osobistych Użytkownika w postaci naruszenia tajemnicy korespondencji.
- Użytkownicy nie mają prawa korzystać z Internetu w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
- Użytkownik nie ma prawa wysyłać wiadomości zawierających informacje poufne dotyczące Pracodawcy i jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej
- Zakazuje się uczestnictwa w tzw. „łańcuszkach szczęścia”
- Użytkownicy nie powinni otwierać przesyłek od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi.
- Użytkownicy nie powinni uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną.

- W przypadku przesyłania plików danych osobowych do podmiotów zewnętrznych, Użytkownik zobowiązany jest do ich spakowania i opatrzenia hasłem (8 znaków: duże i małe litery i cyfry lub znaki specjalne). Hasło należy przesłać odrębnym mailem lub sms.

Ochrona antywirusowa

Ochrona antywirusowa jest realizowana poprzez zainstalowanie odpowiedniego oprogramowania antywirusowego- ESED NOD32 Antivirus™.
W przypadku wykrycia wirusa komputerowego, użytkownik systemu zobowiązany jest do natychmiastowego poinformowania o tym fakcie osobę odpowiedzialną za nadzór nad naruszeniami.
System informatyczny podlega regularnej kontroli pod kątem obecności wirusów komputerowych.
Wykryte zagrożenia usuwa się niezwłocznie z systemu informatycznego.
Przed przystąpieniem do unieszkodliwienia wirusa, należy zabezpieczyć dane zawarte w systemie przed ich utratą.

Procedura rozpoczęcia, zawieszenia i zakończenia pracy.

Przed rozpoczęciem pracy w systemie informatycznym użytkownik zobowiązany jest do:
- zalogowania się do systemu z wykorzystaniem zastrzeżonych tylko dla siebie: identyfikatora i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym – hasło nie może zawierać mniej niż 8 znaków, osoba je tworząca obowiązana jest uczynić to w taki sposób, aby utrudnić jego ewentualne odczytanie, poprzez wprowadzenie do hasła: znaków szczególnych, cyfr, dużych liter itd.,
- sprawdzenia prawidłowości funkcjonowania sprzętu komputerowego,
- w razie stwierdzenia nieprawidłowości, do powiadomienia o tym fakcie bezpośredniego przełożonego oraz osobę nadzorująca przypadku naruszeń,
- w razie stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub stanu wskazującego na istnienie takiej możliwości, do podjęcia odpowiednich kroków stosownie do zasad postępowania w sytuacji naruszenia zabezpieczenia danych osobowych.

Przerywając przetwarzanie danych użytkownik powinien co najmniej: aktywować wygaszasz ekranu lub w inny sposób zablokować możliwość korzystania ze swego konta użytkownika przez inne osoby. W takich przypadkach zalecane jest:
- skorzystanie z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie wygaszacza ekranu z hasłem (hasło powinno być zbieżne z hasłem logowania do systemu),
- zakończenie pracy w systemie informatycznym – wylogowanie się z systemu.

Po zakończeniu przetwarzania danych osobowych w danym dniu, osoba upoważniona zobowiązana jest do:
- zakończenia pracy w systemie informatycznym,
- wyłączenia sprzętu komputerowego oraz zamknięcia szaf, w których przechowuje się nośniki, na których utrwalone są dane osobowe,

Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom nieuprawnionym.

Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

Elektroniczne nośniki, to: np. zewnętrzne dyski twarde, pendrive, karty SD itp.
Użytkownicy nie mogą wynosić na zewnątrz miejsca pracy wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora.
W razie konieczności nadane zostanie upoważnienie do przewożenia dokumentacji na nośnikach lub papierowo.
Dane osobowe wynoszone na nośnikach mobilnych poza miejsce pracy muszą być zaopatrzone hasłem dostępu a dyski szyfrowane.
Do miejsca przechowywania nośników informacji i kopii zapasowych dostęp mają tylko osoby upoważnione.
Likwidacja wydruków z systemu, zawierających dane osobowe odbywa się za pomocą niszczarki do dokumentów lub w inny sposób, trwale uniemożliwiający odczytanie danych.
Z urządzeń, dysków lub innych nośników informatycznych, które zostały przeznaczone do przekazania innemu podmiotowi, usuwa się zapisane na nich dane.

Kopie bezpieczeństwa

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych wskutek awarii zasilania lub zakłóceń w sieci zasilającej. Zabezpieczenie to powinno być tak skonstruowane, by umożliwiało zapisanie danych we wszystkich uruchomionych aplikacjach i wykonanie kopii bezpieczeństwa.
Tworzone kopie bezpieczeństwa powinny być opisane w sposób pozwalający na określenie ich zawartości.
Kopie bezpieczeństwa nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
Kopie bezpieczeństwa powinny być przechowywane w sejfie lub w przypadku braku takiej możliwości w zamkniętych szafach, znajdujących się w pomieszczeniach, które również są zamykane na klucz.
Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz bezzwłocznie usuwać po ustaniu ich użyteczności.
Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych w sposób uniemożliwiający ich odtworzenie.
Jeżeli pozbawienie zapisu nie jest możliwe, kopie są niszczone w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.

Postępowanie z danymi osobowymi w wersji papierowej

Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy) oraz pracownicy.
Dokumenty i wydruki zawierające dane osobowe w szczególności dokumentacja medyczna Pacjentów oraz Pracowników przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
Użytkownicy są zobowiązani do stosowania „polityki czystego biurka". Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.
Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

Zapewnienie poufności danych osobowych

Użytkownik zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez Pracodawcę/Zleceniodawcę.
Użytkownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem o ile nie są one jawne.
Użytkownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne.
Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.

Zasady udzielania informacji za pomocą środków komunikacji

Pracownik może udostępnić Uprawnionemu ograniczone dane dotyczące Pacjentów za pośrednictwem środków komunikacji na odległość po zweryfikowaniu tożsamości poprzez:

a) weryfikację numeru telefonu,
b) żądanie podania numeru PESEL/daty urodzenia Pacjenta.

Informacji dotyczących danych szczególnej kategorii(dany wrażliwych) dotyczących zdrowia, wyroków Sądów nie udziela za pomocą środków komunikacji na odległość. Informacje te udziela się tylko i wyłącznie osobiście w siedzibie Spółki MEDICOR w Gliwicach przy ulicy Cichociemnych 14.

ZLPiS MEDICOR nie ponosi odpowiedzialności za jakiekolwiek działania Uprawnionego, który udostępni swoje dane osobom trzecim.

Postępowanie dyscyplinarne

Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie

z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

VIII. Upoważnienie do przetwarzania danych osobowych (wzór)

Administrator: - Prezes dnia ……... na podstawie art. 29 w zw. z art. 32 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/678 z 27 kwietnia 2016 roku 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) (Dz. Urz. UE L 119, s. 1), dalej jako „**RODO**", nadaje upoważnienie

……..…….
(imię i nazwisko pracownika)

do przetwarzania danych osobowych w celach związanych z wykonywaniem *obowiązków na zajmowanym stanowisku/zleconych zadań w okresie *zatrudnienia/trwania umowy zlecenia/umowy o dzieło/umowy współpracy/stażu/praktyki. Upoważnienie nadane jest celem realizacji obowiązków wynikających z powierzonych zadań. Wszelkie wcześniej nadane upoważnienia tracą moc z dniem nadania niniejszego.

Upoważnienie dotyczy przetwarzania danych osobowych w poniższych systemach informatycznych:

……
/podać nazwy systemów lub programów/

OŚWIADCZENIE UPOWAŻNIONEGO

Ja niżej podpisany/a, oświadczam, że zostałem/am zaznajomiony/a z powszechnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych, w tym RODO. Ponadto zapoznałem/am się z zasadami dotyczącymi ochrony danych osobowych panującymi w podmiocie.
Jednocześnie oświadczam że :

1. Zobowiązuję się do przetwarzania danych osobowych zgodnie z udzielonym upoważnianiem, przepisami prawa, w tym przepisami RODO oraz ustawy o ochronie danych osobowych, a także aktami wewnętrznymi *pracodawcy/zleceniodawcy, przy zachowaniu pełnej ochrony przetwarzanych danych osobowych, z zastosowaniem wdrożonych środków technicznych i organizacyjnych.
2. Natychmiast zgłoszę stwierdzenie próby lub faktu naruszenia zasad ochrony danych osobowych lub bezpieczeństwa systemy informatycznego, w którym przetwarzane są dane osobowe.
3. Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczeń, do których uzyskałem dostęp w trakcie współpracy z administratorem, jak i po jej zakończeniu

Upoważnienie wygasa w dniu rozwiązania umowy *o pracę/zlecenia/dzieło/współpracy/stażu/praktyki, chyba że wcześniej zostanie odwołane.

/podpis osoby upoważnionej/	/podpis Administratora lub osoby upoważnionej do nadania upoważnienia/

Upoważnienie odwołano dnia: ……

IX. Ewidencja osób posiadających upoważnienia do przetwarzania danych osobowych wraz z zakresem uprawnień w systemach informatycznych (wzór)

Lp.	**Nazwisko i imię, stanowisko**	**Data nadania**	**Data ustania**	**Dostęp do programów i aplikacji**
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

X. Obowiązki informacyjne

Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:

a) Swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
b) Gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
c) Cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
d) Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
e) Informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
f) Gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
g) Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
h) Informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
i) Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
j) Informacje o prawie wniesienia skargi do organu nadzorczego;
k) Informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
l) Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, 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.

XI. Przykłady klauzuli informacyjnej

a) Dla pracowników
b) Dla osób rekrutowanych
c) Dla Pacjentów
d) Dla Pracowników korzystających z kasy zapomogowo-pożyczkowej
e) Dla osób zatrudnionych na umowach cywilno-prawnych

Klauzula Informacyjna dla pracowników

1. **Zakład Lecznictwa Podstawowego i Specjalistycznego MEDICOR Sp. z.o.o** ul. Cichociemnych 14, 44-100 Gliwice jest Administratorem Pani/Pana danych osobowych.
   Inspektor Ochrony Danych: iod@medicor.gliwie.pl
2. Dane osobowe przekazane w przetwarzanie Administratorowi Danych będą przetwarzane na podstawie na podstawie art. 9 ust. 2 lit. b oraz art.6 ust.1 lit. b i c RODO w celu: zatrudnienie, cel kontaktowy, prowadzenie rejestru pracowników, akt pracowniczych i ewidencji czasu ich pracy, zgłoszenie pracowników i członków ich rodzin do ZUS, aktualizacja zgłoszeń i przekazywanie danych o zwolnieniach, prowadzenie rozliczeń z pracownikami, wypłata wynagrodzeń naliczanie obciążeń oraz naliczanie składek do ZUS, realizacja obowiązków podatkowych, archiwizacja.
3. Odbiorcą Pani/Pana danych osobowych będą organy uprawnione na mocy przepisów prawa (ZUS, Urząd Skarbowy, Sądy, Policja, Prokuratura, Komornicy, Organy Nadzorcze itp.) lub inne podmioty współpracujące z Administratorem z którymi zostały zawarte umowy powierzenia danych(obsługa księgowo-kadrowa);
4. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej;
5. Pani/Pana dane osobowe będą przechowywane przez okres wskazany na podstawie przepisów prawa czyli : 10 lub 50 lat [art. 51u ust. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.), 50 lat [art. 125a ust. 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]
6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania *(jeżeli przetwarzanie odbywa się na podstawie zgody)* Posiada Pani/Pan prawo wniesienia skargi do Urzędu Ochrony Danych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy Ogólnego Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych;
7. Podanie przez Panią/Pana danych osobowych jest warunkiem zawarcia umowy o pracę jak i wymogiem ustawowym. Jest Pani/Pan zobowiązana do ich podania. Podstawy prawne:
   - Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r., poz. 108 t.j.) w szczeg. art. 22 z ind. 1 i 2
   - Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych - art. 1, 6 oraz 6a
   - Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r. poz. 108 t.j.) Dział III - Wynagrodzenia; ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych - art. 1, 6 oraz 6a;
8. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.
9. Administrator Danych jak i Podmiot Przetwarzający (Procesor) zobowiązany jest dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą i spełnić wszystkie przesłanki wymogów ustawy o ochronie danych osobowych, jak i Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych dotyczących racjonalnych zabezpieczeń systemów informatycznych.

Klauzula Informacyjna dla osób rekrutowanych

1. **Zakład Lecznictwa Podstawowego i Specjalistycznego MEDICOR Sp. z.o.o,** ul. Cichociemnych 14, 44-100 Gliwice jest Administratorem Pani/Pana danych osobowych.
   Inspektor Ochrony Danych, iod@medicor.gliwice.pl
2. Dane osobowe przekazane w przetwarzanie Administratorowi Danych będą przetwarzane w celu: przeprowadzenia rekrutacji, kontaktu telefonicznego lub celu kontaktowym na podany adresu e-mail, archiwizacji;
3. Odbiorcą Pani/Pana danych osobowych będą organy uprawnione na mocy przepisów prawa: Sądy, Policja, Prokuratura, Komornicy, Organy Nadzorcze itp.)
4. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej;
5. Pani/Pana dane osobowe będą przechowywane przez okres 3 miesięcy od złożenia CV a następnie niszczone w sposób uniemożliwiający odczytanie;
6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania *(jeżeli przetwarzanie odbywa się na podstawie zgody)*
7. Posiada Pani/Pan prawo wniesienia skargi do Urzędu Ochrony Danych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy Ogólnego Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych;
8. Podanie przez Panią/Pana danych osobowych jest dobrowolne a odmowa podania danych może skutkować brakiem możliwości udziału w procesie rekrutacyjnym Podstawą przetwarzania jest: art. 6 ust. 1 lit. a, b (zgoda i podjęcie działań przed zawarciem umowy) - ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016), Podstawa prawna:
   Art. 22^1 § 1 Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. 1974 Nr 24 poz. 141z poźn zm)
9. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.
10. Administrator Danych jak i Podmiot Przetwarzający (Procesor) zobowiązany jest dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą i spełnić wszystkie przesłanki wymogów ustawy o ochronie danych osobowych, jak i Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych dotyczących racjonalnych zabezpieczeń

Klauzula Informacyjna Pacjentów

1. Zakład Lecznictwa Podstawowego i Specjalistycznego MEDICOR Sp. z.o.o, ul. Cichociemnych 14, 44-100 Gliwice jest Administratorem Pani/Pana danych osobowych.
   Inspektor Ochrony Danych, iod@medicor.gliwice.pl
2. Dane osobowe przekazane w przetwarzanie Administratorowi Danych będą przetwarzane celem
   a) **udzielania świadczeń zdrowotnych** na podstawie Art. 9 ust 2 pkt h RODO, oraz przepisów:
      - Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (tj. Dz. U. z .2017 r., poz. 1318 z późn. zm.)
      - Ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (tj. Dz. U. 2017 r., poz. 1938 z późn. zm.)
      - Ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (tj. Dz.U. 2017 r.,poz. 125 z późn. zm.)
      - Ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (tj. Dz.U. 2018 r., poz. 123 z późn. zm.)
      - Ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (tj. Dz.U. z 2018r , poz. 160 z późn. zm.)
      - Ustawa o zapobieganiu i zwalczaniu zakażeń oraz chorób zakaźnych u ludzi (Dz. U. Nr. 234 poz. 1570 z dnia 30 grudnia 2008 r.)
   b) **wywiązania się z obowiązków prawnych ciążących na Administratorze na podstawie obowiązujących przepisów prawa** m.in. w zakresie prowadzenia rachunkowości (wystawienie i przechowywanie faktur/rachunków oraz innych dokumentów księgowych), archiwizacji (podstawa prawna art. 6 ust 1 lit. c RODO),
   c) **ochrony mienia, obsługi reklamacji oraz ustalenia, obrony i dochodzenia ewentualnych innych roszczeń, ochrony mienia(monitorig)**. Podstawą przetwarzania jest prawnie uzasadniony interes Spółki (art. 6 ust. 1 lit. f RODO),
   d) **tworzenia zestawień, analiz, statystyk na potrzeby wewnętrzne Spółki MEDICOR** Podstawą przetwarzania jest prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO),
   e) **promocji i marketingu,** poprzez organizacje akcji profilaktycznych, darmowych badań, artykuły, fotografie, filmy reklamowe, zamieszczane w lokalnej prasie, na portalach internetowych oraz na stronie internetowej http://www.mediocor.pl/ Podstawą przetwarzania jest uzyskanie zgody (art. 6 ust.1 lit. a RODO).
3. Odbiorcą Pani/Pana danych osobowych będą organy uprawnione na mocy przepisów prawa: ZUS, KRUS, Narodowy Fundusz Zdrowia, Powiatowa Stacja Sanitarno-Epidemiologiczna, Sądy, Prokuratury, Policja, firmy ubezpieczeniowe z którymi Pani/Pan ma podpisaną zgodę na udostępnienie dokumentacji medycznej oraz Podmioty świadczący usługi informatyczne, firmom kurierskim i pocztowym.
4. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej;
5. Pani/Pana dane osobowe będą przechowywane przez okres wskazany na mocy przepisów prawa czyli art. 29 Ustawy o Prawach Pacjenta i Rzeczniku Praw Pacjenta;

6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania *(jeżeli przetwarzanie odbywa się na podstawie zgody*

7. Posiada Pani/Pan prawo wniesienia skargi do Urzędu Ochrony Danych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy Ogólnego Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych;

8. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.

9. Administrator Danych jak i Podmiot Przetwarzający (Procesor) zobowiązany jest dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą i spełnić wszystkie przesłanki wymogów ustawy o ochronie danych osobowych, jak i Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016r. w sprawie osób fizycznych dotyczących racjonalnych zabezpieczeń systemów informatycznych.

Klauzula Informacyjna dla osób korzystających z ZKZP

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego Rozporządzenia PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej) RODO informuję, że:

1. Przyzakładowa Kasa Zapomogowo-Pożyczkowa przy **Zakład Lecznictwa Podstawowego i Specjalistycznego MEDICOR Sp. z.o.o,** ul. Cichociemnych 14, 44-100 Gliwice jest Administratorem Pani/Pana danych osobowych.
   Inspektor Ochrony Danych, iod@medicor.gliwice.pl
2. Dane osobowe pracownika, o których mowa będą przetwarzane w celu realizacji praw i obowiązków wynikających z realizacją zadań związanych z prowadzeniem przyzakładowej pracowniczej kasy zapomogowo-pożyczkowej, przyjęciem wniosku o członkostwo, wypłaty pożyczek, poręczenia, cel kontaktowy, archiwizacji dokumentacji.
3. Odbiorcą Pani/Pana danych osobowych będą organy uprawnione na mocy przepisów prawa (Urząd Skarbowy, Sądy, Policja, Prokuratura, Organy Nadzorcze) lub inne podmioty współpracujące z Administratorem z którymi zostały zawarte umowy powierzenia danych(podmioty świadczące usługi informatyczne, serwisowe do oprogramowania, operatorzy pocztowi);
4. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej;
5. Pani/Pana dane osobowe będą przechowywane przez okres wskazany na podstawie przepisów prawa czyli : do czasu ustania członkostwa w PKZP, natomiast w przypadku udzielenia pożyczki przez okres 5 lat od spłaty ostatniej raty.
6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania *(jeżeli przetwarzanie odbywa się na podstawie zgody).* Posiada Pani/Pan prawo wniesienia skargi do Urzędu Ochrony Danych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy Ogólnego Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych;
7. Podanie przez Panią/Pana danych osobowych jest wymogiem ustawowym. Jest Pani/Pan zobowiązana do ich podania. Przetwarzanie odbywa się na podstawie art. 6.ust.1 lit a i c.
   - Ustawa z dnia 23 maja 1991r o związkach zawodowych(Dz. U. z 2019 r. poz. 263) art. 39.1
   - Rozporządzenie Rady Ministrów z dnia 19 grudnia 1992 r. w sprawie pracowniczych kas zapomogowo-pożyczkowych oraz spółdzielczych kas oszczędnościowo- kredytowych w zakładach pracy(Dz.U. 1992 nr 100 poz. 502)
   - Regulamin korzystania z Kasy Zapomogowo-Pożyczkowej
8. Pani/Pana dane nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.
9. Administrator Danych jak i Podmiot Przetwarzający (Procesor) zobowiązany jest dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą i spełnić wszystkie przesłanki wymogów ustawy o ochronie danych osobowych, jak i Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016r. w sprawie osób fizycznych dotyczących racjonalnych zabezpieczeń systemów informatycznych.

Klauzula Informacyjna dla osób na umowach-zlecenie

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego Rozporządzenia PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej) RODO informuję, że:

1. **Zakład Lecznictwa Podstawowego i Specjalistycznego MEDICOR Sp. z.o.o,** ul. Cichociemnych 14, 44-100 Gliwice jest Administratorem Pani/Pana danych osobowych.
   Inspektor Ochrony Danych: iod@medicor.gliwice.p
2. Pani/Pana dane osobowe przetwarzane będą celem:
   a) **zawarcia i wykonania umów zleceń/dzieła** w tym komunikacji związanej z realizacją umów. Podstawą przetwarzania jest niezbędność do wykonania umowy (art. 6 ust. 1 lit. b RODO),
   b) **wywiązania się z obowiązków prawnych ciążących na Administratorze na podstawie obowiązujących przepisów prawa** m.in. w zakresie prowadzenia rachunkowości (rozliczenia podatkowe i finansowe, archiwizacja (podstawa prawna art. 6 ust 1 lit. c RODO),
   c) **obrony i dochodzenia ewentualnych innych roszczeń**. Podstawą przetwarzania jest prawnie uzasadniony interes ZLPiS(art. 6 ust. 1 lit. f RODO) oraz Kodeks Cywilny.
3. Podane przez Panią/Pana dane osobowe będą udostępniane podmiotom uprawnionym do ich przetwarzania na podstawie przepisów prawa oraz zawartych umów powierzenia.
4. Pani/Pana dane osobowe będą przechowywane przez okres wynikający z przepisów prawa czyli 5 lat.
5. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem w granicach określonych w przepisach prawa.
6. Posiada Pan/Pani prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, jeżeli uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
7. Podanie przez Pana/Panią danych osobowych może być wymogiem ustawowym, warunkiem umownym, warunkiem zawarcia umowy lub dobrowolnie wyrażoną zgodą.
8. Pani/Pana dane będą nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania..

XII. Regulamin monitoringu i obowiązki z tym związane

§ 1

1. Regulamin określa zasady funkcjonowania systemu monitoringu wizyjnego w **Zakładzie Lecznictwa Podstawowego i Specjalistycznego MEDICOR Sp. z.o.o** miejsca instalacji kamer systemu na terenie podmiotu, reguły rejestracji i zapisu informacji oraz sposób ich zabezpieczenia, a także możliwość udostępniania zgromadzonych danych o zdarzeniach.
2. Infrastruktura podmiotu, która jest objęta monitoringiem wizyjnym, to:
   - ciągi komunikacyjne (korytarze i poczekalnie)
   - wejścia do budynku

§ 2

Celem monitoringu jest:

a) Zwiększenie bezpieczeństwa osób przebywających na terenie objętym monitoringiem.
b) Ograniczenie zachowań niepożądanych, destrukcyjnych, zagrażających zdrowiu, bezpieczeństwu.
c) Ochrona mienia.
d) Ustalanie sprawców czynów zabronionych.
e) Ograniczenie dostępu na terenu podmiotu osób nieuprawnionych i niepożądanych.

§ 3

1. Monitoring funkcjonuje całą dobę.
2. Podgląd bieżący możliwy jest w Informacji.
3. Rejestracji i zapisu na nośniku fizycznym podlega tylko obraz (wizja) z kamer systemu monitoringu. Nie rejestruje się dźwięku (fonii).

§ 4

1. System monitoringu składa się z:
   - kamer rejestrujących zdarzenia wewnątrz i na zewnątrz budynku Administratora;
   - urządzeń rejestrujących i zapisujących obraz na nośniku fizycznym;
   - monitora pozwalającego na podgląd rejestrowanych zdarzeń.
2. Do rejestracji obrazu służą urządzenia wchodzące w skład systemu rejestracji spełniającego wymogi określone Polską Normą PN-EN 50132-7 dla systemów dozorowanych CCTV.
3. Elementy monitoringu wizyjnego w miarę konieczności i możliwości finansowych są udoskonalane, wymieniane i rozszerzane.
4. Osoby przebywające na terenie obszaru monitorowanego są poinformowani o funkcjonowaniu systemu monitoringu wizyjnego.
5. Miejsca objęte monitoringiem wizyjnym są oznakowane tabliczkami informacyjnymi.
6. Czas przechowywania danych na nośniku: 14 dni.
7. Zapis na nośniku nie jest archiwizowany, nadpisuje się go. Firma serwisująca system.

§ 5

Zasady wykorzystania zapisów monitoringu wizyjnego:

1. Rejestrator wraz z monitorem umożliwiającym podgląd budynku i terenu przy ul. Cichociemnych 14 znajduje się w Informacji.
2. Osobą upoważnioną do obserwowania obrazu jest Prezes. Prezes może w razie konieczności upoważnić inne osoby.

3. Zapis może być udostępniony w formie oglądu tylko za zgodą Administratora., a osoby, które mają wgląd w obraz zarejestrowany przez monitoring wizyjny mają świadomość odpowiedzialności za ochronę danych osobowych.

§ 6

Zasady obowiązujące przy przekazywaniu płyty z materiałem archiwalnym organom ścigania:

1. Przedstawiciel organów ścigania pisemnie kwituje odbiór płyty.
2. W pokwitowaniu odbioru zaznacza znaki szczególne płyty: zawartość płyty (np. nagranie z dnia – dzień, miesiąc, rok).
3. Płyta zostaje zapakowana do koperty, którą należy opieczętować i podpisać przez osobę uprawnioną ze strony udostępniającego (Administrator).
4. Jeżeli materiał archiwalny jest kopiowany na inny nośnik, obowiązują takie same zasady, jak przy przekazywaniu płyty.
5. Do przegrywania materiału archiwalnego z rejestratora upoważnione są osoby wskazane przez Administratora.

§ 7

1. W sprawach nieuregulowanych niniejszym regulaminem ostateczną decyzję podejmuje Administrator.
2. Regulamin może ulec zmianie w zależności od zaistniałej sytuacji.
3. Obowiązujące zasady wykorzystania monitoringu wchodzą w życie z dniem 27.05.2019r.

§ 8

Informacje do zamieszczenia na tablicy informacyjnej o monitoringu wizyjnym:

- Administratorem systemu monitoringu jest **Zakład Lecznictwa Podstawowego i Specjalistycznego MEDICOR Sp. z.o.o**
- Monitoring stosowany jest w celu zapewnienia bezpieczeństwa oraz ochrony mienia na terenie monitorowanym. Nagrywany jest tylko obraz (bez fonii).
- Podstawą przetwarzania jest prawnie uzasadniony interes Administratora zgodnie z art. 6. ust. 1. lit. f Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016r.
- Dane osób zarejestrowany przez system monitorujący ma prawo dostępu do swoich danych i wniesienia skargi do organu nadzorczego.

XIII. Polityka kluczy

1. Ogólne zasady
   a) Polityka kluczy obejmuje obszary przetwarzania danych osobowych w ZLPiS MEDICOR ul. Cichociemnych 14
   b) Obszar podlega ochronie poprzez zastosowanie ochrony fizycznej:
      - zamykane pomieszczenia
      - zamykane szafy
      - kontrola wejść i wyjść
   a) klucze przechowywane są w Informacji

Wydawanie kluczy w trybie nadzwyczajnym upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą i wiedzą Prezesa Po wykorzystaniu klucze należy niezwłocznie zwrócić.

Bieżące postępowanie w trakcie dnia pracy
   a) Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
   b) W godzinach pracy klucze pozostają pod nadzorem Pracowników.
   c) Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu, chyba że pomieszczenie to zostanie zamknięte a klucz będzie znajdował się pod bezpośrednim nadzorem osoby upoważnionej.
   d) Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w szafce do tego przeznaczonej.

XIV. Powierzenie przetwarzania danych osobowych (wzór)

Wzór Umowy powierzenia przetwarzania danych osobowych

zwana dalej „Umową", zawarta w …… , dnia ..... r. pomiędzy: …….. , NIP:…….. reprezentowanym przy zawarciu niniejszej umowy przez ……. zwanym dalej **„Administratorem" - „Powierzającym"**

a
……., zwaną dalej **„Podmiotem przetwarzającym",** zwanymi łącznie **„Stronami".**

Mając na uwadze, iż Strony łączy Umowa z dnia ....., przedmiotem której jest ……. zwana dalej „Umową główną", w trakcie wykonywania której przetwarzane są dane osobowe, Strony zgodnie postanowiły, co następuje:

§ 1.
Przedmiot Umowy

1. Strony postanawiają, że w celu spełnienia obowiązków wynikających z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. zwanego dalej „Rozporządzeniem", Administrator powierza Podmiotowi przetwarzającemu do dane osobowe w celu realizacji Umowy głównej.

2. Zakres przetwarzania obejmuje ……... (np. wprowadzanie, wgląd, modyfikację, drukowanie, usuwanie, archiwizację, przesyłanie) danych osobowych Administratora.
3. Przetwarzane dane dotyczą: …….. np. danych pracowniczych
4. Przetwarzane dane obejmują: …… np. imię, nazwisko, pesel, adres

§ 2.
Obowiązki i prawa administratora

1. Administrator jest uprawniony do powierzenia przetwarzania danych Podmiotowi przetwarzającemu. Powierza mu gromadzone zgodnie z obowiązującymi przepisami prawa.
2. Administrator zobowiązany jest do przekazywania danych osobowych zachowując zasady bezpieczeństwa w celu zachowania poufności i integralności powierzanych danych osobowych.
3. Administrator nie zezwala na korzystanie z usług innego podmiotu przetwarzającego. W uzasadnionych przypadkach może nastąpić podpowierzenie tylko po uprzednio uzyskanej zgodzie do Administratora.
4. Administrator ma możliwość wyrażenia sprzeciwu wobec dodania lub zastąpienia innych podmiotów przetwarzających.
5. Administrator ma prawo samodzielnie lub za pomocą upoważnionych przez siebie audytorów przeprowadzić audyty lub inspekcje, których celem jest weryfikacja realizacji obowiązków wynikających z zapisów Rozporządzenia.

§ 3.
Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający przy przetwarzaniu powierzonych danych osobowych zobowiązany jest stosować przepisy Rozporządzenia, w tym:
   a) stosować środki techniczne i organizacyjne zapewniające bezpieczeństwo powierzanym danym, w stopniu adekwatnym do ryzyka występujących zagrożeń,
   b) powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, utratą, uszkodzeniem lub zniszczeniem,
   c) dopuszczać do przetwarzana danych osobowych wyłącznie osoby, które zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
2. Podmiot przetwarzający zobowiązuje się do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Administratora.
3. Podmiot przetwarzający zgłasza Administratorowi przypadki naruszeń ochrony danych osobowych w ciągu 24 godzin ze względu na obowiązek zgłaszania naruszeń do Urzędu Ochrony Danych.

§ 4.
Oświadczenie Podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązany jest do wykorzystania powierzonych danych osobowych wyłącznie w zakresie i celu niezbędnym do realizacji obowiązków wynikających z umowy współpracy.
2. W przypadku ogólnej pisemnej zgody na korzystanie z usług innego podmiotu przetwarzającego Podmiot przetwarzający poinformuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających.

3. W miarę możliwości Podmiot przetwarzający pomagać będzie Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.
4. W przypadku audytów lub inspekcji przeprowadzonych lub zleconych przez Administratora udostępnione będą wszelkie niezbędne informacje z zachowaniem czujności, czy żądane informacje nie naruszą zapisów Rozporządzenia.

§ 5.
Odpowiedzialność stron

1. Każda ze Stron odpowiada za szkody wyrządzone drugiej Stronie oraz osobom trzecim w związku z wykonywaniem niniejszej Umowy, zgodnie z przepisami Rozporządzenia i Kodeksu cywilnego.
2. W celu uniknięcia wątpliwości, Podmiot przetwarzający ponosi odpowiedzialność za działania swoich pracowników i innych osób, przy pomocy których przetwarza powierzone dane osobowe, jak za własne działanie i zaniechanie.

§ 6.
Czas trwania i wypowiedzenie Umowy

1. Umowa zostaje zawarta na czas obowiązywania Umowy głównej. W celu uniknięcia wątpliwości, rozwiązanie Umowy głównej skutkuje rozwiązaniem niniejszej Umowy.
2. Strony postanawiają, iż po zakończeniu przetwarzania danych osobowych Podmiot przetwarzający zobowiązany jest do niezwłocznego usunięcia powierzonych mu danych osobowych (i wszelkich ich istniejących kopii) lub zwrotu Administratorowi w zależności od jego decyzji, o ile nie następuje konieczność dalszego przetwarzania danych osobowych wynikająca z przepisów odrębnych.
3. Administrator jest uprawniony do rozwiązania Umowy bez wypowiedzenia, jeżeli Podmiot przetwarzający nie podjął środków zabezpieczających powierzone dane lub nie stosował się do wymogów przewidzianych w Rozporządzeniu.
4. Każdej ze Stron przysługuje prawo rozwiązania niniejszej Umowy w trybie natychmiastowym, w przypadku naruszenia postanowień niniejszej Umowy przez drugą Stronę Umowy.

§ 7.
Postanowienia końcowe

1. Z tytułu wykonywania świadczeń określonych w niniejszej Umowie Podmiotowi przetwarzającemu nie przysługuje dodatkowe wynagrodzenie ponad to, które zostało określone w Umowie głównej.
2. Umowa wchodzi w życie z dniem jej podpisania przez Strony.
3. W sprawach nieuregulowanych niniejszą Umową zastosowanie mają powszechnie obowiązujące przepisy prawa polskiego.
4. Wszelkie zmiany lub uzupełnienia niniejszej Umowy wymagają zachowania formy pisemnej pod rygorem nieważności.
5. Sądem właściwym dla rozstrzygania sporów powstałych w związku z realizacją niniejszej Umowy jest sąd właściwy dla siedziby Administratora.
6. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Podpisy:

…….… ……..
Administrator Podmiot przetwarzający

XV. Rejestr podpisanych umów przetwarzania danych osobowych (wzór)

Lp.	Nazwa firmy	Zakres świadczonych usług	Nr umowy, data zawarcia, uwagi
1.	Kancelaria Prawna		
2.	Strona	Tworzenie strony www, serwis, aktualizacja	
3.	Obsługa BHP	Szkolenia BHP	
4.	SERWIS SYSTEMU CCTV		
5.	Informatyk		
6.	Serwis programu		

XVI. Rejestr incydentów przy przetwarzaniu danych osobowych

Procedury postępowania w przypadku naruszeń

§ 1

1. Każdy użytkownik w przypadku stwierdzenia incydentu lub zaistnienia okoliczności wskazujących na ingerencję w system ochrony zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie osoby odpowiedzialnej – Administratora lub osoby przez niego wyznaczonej.
2. W razie braku możliwości zawiadomienia osoby odpowiedzialnej, należy zawiadomić bezpośredniego przełożonego.
3. Do czasu przybycia na miejsce Administratora lub osoby przez niego wyznaczonej, użytkownik powinien:
   a) niezwłocznie podjąć czynności niezbędne do powstrzymania skutków incydentu (o ile to jest możliwe),
   b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia, na ile to możliwe należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia incydentów ochrony i udokumentowanie zdarzenia podjąć stosowne działania,
   c) podjąć, stosownie do zaistniałej sytuacji działania, które zapobiegną ewentualnej utracie danych osobowych,
   d) ustalić przyczynę i sprawcę incydentu ochrony oraz zapisać wszelkie informacje i okoliczności związane ze zdarzeniem,
   e) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia,
   f) zabezpieczyć dostęp do pomieszczenia lub urządzenia.
4. Dokonywanie zmian w miejscu wystąpienia incydentu ochrony jest dopuszczalne tylko w wypadku konieczności ratowania osób, mienia albo zapobiegania powstaniu innego niebezpieczeństwa.
5. W przypadku stwierdzenia przez użytkownika incydentu bezpieczeństwa danych osobowych w systemie informatycznym należy:
   a) odłączyć system od sieci komputerowej,
   b) wykonać kopie bezpieczeństwa danych na oddzielnym nośniku informacji,
   c) wyłączyć system aby zapobiec działaniu złośliwego oprogramowania lub hakera.

§ 2

1. Po przybyciu na miejsce wystąpienia incydentu bezpieczeństwa danych osobowych osoba odpowiedzialna za nadzór nad incydentami podejmuje następujące kroki:
   a) Zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy,
   b) Wysłuchuje relacji użytkownika lub osoby, która dokonała powiadomienia,
   c) Podejmuje niezbędne działania mające na celu uniemożliwienie dalszej ingerencji w bezpieczeństwo danych osobowych (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów, zbiorów danych itp.),
   d) Zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
   e) Dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
   f) Może zażądać dokładnej relacji z zaistniałego od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
   g) Nawiązuje kontakt ze specjalistami (jeśli zachodzi taka potrzeba),

h) Poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,
i) Proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych osobowych z zabezpieczeń, oraz terminu wznowienia przetwarzania danych osobowych); analiza ta powinna zawierać wszechstronną ocenę zaistniałego naruszenia bezpieczeństwa, wskazanie odpowiedzialnych, wnioski co do ewentualnych działań proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym incydentom w przyszłości,
j) Dokumentuje zaistniały przypadek incydentu bezpieczeństwa danych osobowych sporządzając raport, którego wzór stanowi **zał. nr 1** do niniejszego Rejestru.

2. W przypadku incydentu danych osobowych w systemie informatycznym osoba nadzorująca przetwarzanie danych osobowych w systemie informatycznym:
   a) Sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   b) W celu powstrzymania lub ograniczenia dostępu do danych osoby nieupoważnionej podejmuje odpowiednie kroki zmierzające do: fizycznego odłączenia urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do zbiorów danych osobie nieupoważnionej, wylogowania użytkownika systemu podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmiany hasła poprzez które uzyskano nielegalny dostęp, aby uniknąć ponownej próby włamania,
   c) Przywraca prawidłowy stan działania systemu,
   d) Sprawdza sposób działania programów (w tym obecność wirusów komputerowych),
   e) Sprawdza jakość komunikacji w sieci telekomunikacyjnej,
   f) Wyraża zgodę na ponowne uruchomienie komputera lub innych urządzeń.

§ 3

Osoba odpowiedzialna za nadzór nad incydentami podejmuje niezbędne działania w celu wyeliminowania incydentów dotyczących zabezpieczeń danych w przyszłości, a w szczególności:

1. Jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub inny atak sieciowy, jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie zleca przeprowadzenie przeglądów oraz konserwacji urządzeń i programów, ustalenie źródła pochodzenia wirusa komputerowego lub innego ataku sieciowego oraz wdrożenie skuteczniejszego zabezpieczenia antywirusowego, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych w celu usprawnienia systemu zabezpieczeń.
2. Jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób upoważnionych do przetwarzania danych osobowych, a wobec osób winnych zaniedbań wnioskuje o wyciągnięcie konsekwencji przewidzianych prawem.
3. Jeżeli przyczyną zdarzenia było włamanie, w celu nielegalnego pozyskania danych dokonuje szczegółowej analizy wdrożonych środków zabezpieczenia i proponuje wdrożenie skuteczniejszej ochrony fizycznej.
4. Jeżeli przyczyną zdarzenia był czyn zabroniony lub zachodzi jego uzasadnione podejrzenie, zawiadamia organy ścigania.

§ 4

1. Osoba nadzorująca przypadki incydentów prowadzi dziennik incydentów, który stanowi **zał. nr 2** do niniejszego Rejestru.
2. Osoba nadzorująca przypadki naruszeń dokonuje rocznej analizy przypadków incydentów, dokument do analizy naruszeń stanowi **zał. nr 3** do niniejszego Rejestru.

§ 5

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 właściwemu zgodnie z art. 55, 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. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
3. 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.

§ 6

1. Każdy użytkownik przetwarzający dane osobowe w zbiorach danych zobowiązany jest zapoznać się z niniejszym Rejestrem i stosować przepisy w nim zawarte na swoim stanowisku pracy.
2. Nieprzestrzeganie zasad wskazanych w niniejszym Rejestrze stanowi niewykonanie bądź nie należyte wykonanie obowiązków pracowniczych/obowiązków służbowych lub niewykonanie bądź nienależyte wykonanie innej niż umowa o pracę umowy stanowiącej podstawę zatrudnienia, co może wiązać się dla osoby zatrudnionej z odpowiedzialnością majątkową wobec administratora.
3. Nadużycie przez użytkownika postanowień niniejszego Rejestru może stanowić podstawę do pociągnięcia go do odpowiedzialności dyscyplinarnej lub karnej, w trybie i na zasadach przewidzianych przepisami prawa.

załącznik nr 1

Raport dotyczący incydentu z bezpieczeństwa danych osobowych (wzór)

Nr raportu ___/_____Data i godzina wystąpienia zdarzenia _____
Miejsce wystąpienia zdarzenia _____
Osoba zawiadamiająca _____
Opis zdarzenia i rodzaj incydentu

Przyczyny powstania zdarzenia

Zaistniałe skutki zagrożenia

Podjęte czynności naprawczo-zapobiegawcze

Osoby zaangażowane w wyjaśnienie zdarzenia

Podpisy:

……..…… ……..
Administrator/ lub wyznaczona osoba nadzorująca Osoba zgłaszająca

załącznik nr 2

Dziennik incydentów (wzór)

Lp.	Nr raportu	Incydent z dnia	Opis incydentu	Podpis Administratora/ osoby nadzorującej

załącznik nr 3

Roczna analiza incydentów (wzór)

Data sporządzenia analizy _____

Administrator/ Osoba nadzorująca _____

Ilość incydentów _____

1. Ocena wdrożonych zabezpieczeń zapobiegających wystąpieniu incydentów

_____

2. Ocena realizacji działań naprawczo-zapobiegawczych

_____

3. Zadania do realizacji w celu zapobiegania wystąpienia incydentów

_____

_____

_____

Podpisy:

……..……

Administrator/ lub wyznaczona osoba nadzorująca

XVII. Obowiązek zgłaszania (notryfikacji) naruszeń organowi nadzorczemu oraz osobom, których dane dotyczą.

Dotyczy nie wszystkich naruszeń, ale tych mogących powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dotyczą (tzw. poważnych naruszeń) np. wycieki na masową skalę lub naruszenia jednostkowe ale o doniosłych skutkach dla osoby, której dane dotyczą.

Administrator wykonuje obowiązek notyfikacji bez zbędnej zwłoki w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłoszenie dokonane później musi zawierać opis przyczyn opóźnienia.

XVIII. Prawa osób

Prawo do bycia zapomnianym – zasady ogólne

W związku ze specyfiką przetwarzania danych za pomocą nowoczesnych metod, w tym cyfrowych, RODO wprowadza nowe prawo do „bycia zapomnianym", które osoba fizyczna może wykorzystać, jeżeli zatrzymywanie jej danych narusza prawo. Prawo to ma znaczenie w przypadkach, gdy osoba, której dane dotyczą, wyraziła zgodę jako dziecko, gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, w szczególności z Internetu. Osoba, której dane dotyczą, powinna móc wykonywać to prawo, mimo że już nie jest dzieckiem.
Osoba, której dane dotyczą, powinna w szczególności mieć prawo do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane jeżeli:

- dane te nie są już niezbędne do celów, w których były zbierane
- dane te są przetwarzane w inny sposób,
- osoba, której dane dotyczą, cofnęła zgodę,
- osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących,
- przetwarzanie jej danych osobowych nie jest z innego powodu zgodne rozporządzeniem.

Dalsze zatrzymywanie danych osobowych powinno być uznane za zgodne z prawem, jeżeli jest niezbędne do:

- korzystania z wolności wypowiedzi i informacji,
- do wywiązania się z obowiązku prawnego,
- 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 lub do ustalenia, dochodzenia lub obrony roszczeń.

Prawo żądania usunięcia danych

W celu wzmocnienia prawa do „bycia zapomnianym" w Internecie, rozszerzono prawo do usunięcia danych zobowiązując administratora, który upublicznił te dane osobowe, do poinformowania administratorów, którzy przetwarzają takie dane osobowe o usunięciu

wszelkich łączy do tych danych, kopii tych danych osobowych lub ich replikacji. Do spełnienia tego obowiązku administrator powinien podjąć racjonalne działania.
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;
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania jej danych w celach marketingowych;
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, oferowanych dzieciom przed 16 rokiem życia.

Jeżeli administrator upublicznił dane osobowe, które ma obowiązek usunąć, 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.

Prawa Pacjenta

1. Administrator przetwarza dane osobowe z poszanowaniem praw pacjenta oraz praw osób, których dane dotyczą wynikających z Rozporządzenia.
2. Administrator prowadzi rejestr zgłoszonych żądań, przez osoby, których danych dotyczą.
3. Przed wykonaniem praw osoby, której dane dotyczą administrator dokonuje weryfikacji tożsamości osoby zgłaszającej żądanie, celem ustalenia, czy żądanie pochodzi od osoby uprawnionej.
4. Administrator zapewnia odpowiednie zaplecze techniczne oraz kadrowe w celu terminowej oraz rzetelnej realizacji praw osoby, której dane dotyczą. Zgłoszone żądania realizowane są przez administratora niezwłocznie, nie później niż w terminie miesiąca od otrzymania żądania. W przypadku niemożności wykonania żądania w w/w terminie, z uwagi na skomplikowany charakter sprawy, administrator kontaktuje się z pacjentem i informuje go o przyczynie wydłużenia tego terminu oraz przewidywanym terminie realizacji żądania pacjenta.

Prawo do informacji

1. Pacjenci są informowani przez administratora o sposobie przetwarzania ich danych osobowych oraz przysługującym ich uprawnieniach w formie klauzuli informacyjnej, z którą mogą zapoznać się w każdej chwili w siedzibie Administratora oraz na stronie internetowej.

2. Nota informacyjna jest sporządzona prostym językiem, w sposób przejrzysty i wyczerpuje wszystkie informacje zgodnie z art. 13 oraz 14 Rozporządzenia.

Prawo dostępu do danych

1. Na żądanie pacjenta administrator udziela mu informacji o sposobie przetwarzania jego danych osobowych.Na żądanie pacjenta administrator udostępnia mu nieodpłatnie pierwszą kopię jego danych osobowych, w tym zawierającą jego dokumentację medyczną; za każdą kolejną kopię administrator może pobrać opłatę w rozsądnej wysokości (w tym za wydanie kopii w formie papierowej pobierana jest opłata zgodnie z przepisami regulującymi stawki za każdą wydaną stronę dokumentacji medycznej).Jeżeli żądanie wydania kopii danych zostało złożone administratorowi w formie elektronicznej a pacjent nie zaznacza inaczej - kopia wydawana jest w tej samej formie.Administrator może udostępnić kopię w inny sposób, niż wybrany przez pacjenta, jeżeli ze względów technicznych nie jest to możliwe (np. ze względu na wagę pliku w wersji elektronicznej); o niemożności dostarczenia kopii w wybrany przez pacjenta sposób oraz proponowanym alternatywnym rozwiązaniu administrator niezwłocznie powiadamia pacjenta.**Prawo do sprostowania danych**

1. Administrator umożliwia pacjentowi niezwłoczne sprostowanie jego danych osobowych, jeżeli są one nieprawidłowe lub nieaktualne, lub ich uzupełnienie.

2. Administrator może żądać od pacjenta stosownych dokumentów w celu okazania, aby ustalić zasadność oraz zgodność z prawem dokonywanej zmiany danych osobowych.

Prawo do usunięcia danych (prawo do bycia zapomnianym)

1. Administrator usuwa bez zbędnej zwłoki dane osobowe pacjenta na żądanie pacjenta, jeżeli na administratorze nie spoczywają obowiązki nakazujące dalsze przetwarzanie danych osobowych.

2. Administrator odmawia realizacji prawa do bycia zapomnianym, jeżeli została wytworzona dokumentacja medyczna pacjenta i nie upłynął okres jej przechowywania wynikający z przepisów regulujących sposób oraz okres prowadzenia oraz przechowywania dokumentacji medycznej.

3. Odmowa realizacji prawa do usunięcia danych jest przekazywana przez Administratora pacjentowi wraz z uzasadnieniem przyczyny odmowy zawierającym podstawy prawne odmowy.

Prawo do ograniczenia przetwarzania

Z uwagi na fakt, iż realizacja prawa do ograniczenia przetwarzania danych znacznie utrudniłaby realizację celów zdrowotnych, o których mowa w pkt 3.3., pomimo zgłoszonego żądania ograniczenia przetwarzania danych, administrator jest uprawniony do ich przetwarzania w dalszym zakresie (w szczególności zawartych w dokumentacji medycznej lub innych danych, przetwarzanych w oparciu o art. 9 ust. 2 lit. h Rozporządzenia).

Prawo do przenoszenia danych

1. Dla danych osobowych przetwarzanych w oparciu o podstawę prawną - art. 9 ust. 2 lit. h, wobec Administratora będącego podmiotem leczniczym, prawo do przenoszenia danych nie znajduje zastosowania.

2. W sytuacji odmowy realizacji żądania prawa do przenoszenia danych, administrator informuje pacjenta o przyczynie odmowy i instruuje pacjenta jakie kroki może podjąć w celu przekazania dokumentacji medycznej do innego podmiotu leczniczego.

Prawo do sprzeciwu

Dla danych osobowych przetwarzanych przez Administratora będącego podmiotem leczniczym, w oparciu o podstawę prawną - art. 9 ust. 2 lit. h Rozporządzenia, prawo do sprzeciwu nie znajduje zastosowania.