Polityka Ochrony Danych Osobowych

MILTON ESSEX S.A.

Spis treści.

1) Deklaracja

1. Administrator danych mając świadomość, iż przetwarza dane wrażliwe deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.
2. Administrator deklaruje, że proces przetwarzania danych osobowych uwzględnia zasady, o których mowa w Motywie 39 RODO oraz artykule 5 ust. 1 ppkt a) – e) RODO.
3. Każdy pracownik upoważniony do przetwarzania danych, świadomy odpowiedzialności, zobowiązany jest postępować zgodnie z przyjętymi zasadami i minimalizować zagrożenia wynikające z błędów ludzkich.
4. W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.
5. Dane osobowe w Spółce przetwarzane są w sposób legalny, na podstawie art. 6 ust. 1 ppkt a) i b) oraz art. 9 ust. 2 ppkt h) RODO, a także w związku z art. 54 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa lub innych właściwych przepisów z zakresu prawa ubezpieczeń społecznych.
6. W przypadku konieczności pozyskania zgody na przetwarzanie danych osobowych, zgoda może zostać pozyskana w inny sposób, ale musi ona spełniać przesłanki, o których mowa w art. 7 ust. 1 RODO.
7. Zakres pozyskiwanych danych wynika z przepisów prawa i jest adekwatny do zdefiniowanych celów przetwarzania.
8. Okres czasu, przez jaki dane osobowe są przetwarzane wynika z przepisów prawa- zasady retencji danych znajdują się w Załączniku 17 Zasady retencji danych.

2) Definicje

1) **„dane osobowe”** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

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

3) **„ograniczenie przetwarzania”** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

4) **„profilowanie”** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

5) **„pseudonimizacja**” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi

uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

6) **„Zbiory danych”** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7) „**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; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

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

9) **„odbiorca”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane 4.5.2016 L 119/33 Dziennik Urzędowy Unii Europejskiej PL osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

10) **„strona trzecia”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

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

12) **„naruszenie ochrony danych osobowych”** oznacza naruszenie bezpieczeństwa

prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

13) **„dane genetyczne”** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

14) **„dane biometryczne”** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

15) **„dane dotyczące zdrowia”** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

16**) „przedstawiciel”** oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;

17) „**organ nadzorczy”** oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51; 4.5.2016 L 119/34 Dziennik Urzędowy Unii Europejskiej PL

18) **„organ nadzorczy, którego sprawa dotyczy”** oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ:

a)administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego;

b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub

c) wniesiono do niego skargę;

19) **„transgraniczne przetwarzanie”** oznacza:

a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo

b)przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;

3) Oznaczanie danych

dane osobowe – informacje dotyczące możliwej do zidentyfikowania osoby fizycznej. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

dane osobowe szczególnych kategorii –danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

4) Zasady dotyczące przetwarzania danych

1.Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane

dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i szczególność”).

5) Zasady przetwarzania danych

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

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

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której

dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

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

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

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

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

Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

6) Przetwarzanie szczególnych kategorii danych

Dane szczególnych kategorii można przetwarzać w przypadku wystąpienia poniższej sytuacji:

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

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

państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

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

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

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

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

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

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

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi

zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

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

7) Wykaz zbiorów osobowych

1. Dane osobowe przetwarzane przez ADO są zorganizowane są w zbiory, za pomocą których Administrator może ocenić ryzyko ich przetwarzania oraz ocenić konieczność przeprowadzenia procedury oceny skutków dla systemu ochrony danych, o którym mowa w art. 35 RODO. Wykaz zbiorów danych zawarty jest w dokumencie Rejestr Czynności Przetwarzania (plik REJESTR_RODO.xls.)- Załącznik 11.

8) Wykaz miejsc przetwarzania

1. Obszarem przetwarzania danych są wszystkie pomieszczenia, korytarze oraz obszar Podmiotu wyposażone w karty dostępowe.
2. Szczegółowy wykaz lokalizacji, w których przetwarzane są dane osobowe, ujęty jest w pliku **REJESTR_RODO.xls- załącznik 11** . Dla pomieszczeń, w których dane są gromadzone na czas nieobecności w nich osób upoważnionych opisano zastosowane środki ochrony technicznej, obejmujące system autoryzacji dostępu kartami elektronicznymi (czytnik systemu autoryzacji dostępu Fot.1).

Fot.1 czytnik systemu autoryzacji dostępu

9) Rejestr czynności przetwarzania

1. Dla zbiorów, w których przetwarzane są dane, o których mowa w art. 9 ust. 1 RODO prowadzony jest rejestr czynności przetwarzania.

2. Rejestr, o którym mowa w punkcie 1 niniejszego rozdziału może być również prowadzony dla innych zbiorów lub jedna czynność przetwarzania może obejmować kilka zbiorów danych osobowych.
3. Rejestr czynności przetwarzania winien zawierać co najmniej informacje, o których mowa w art. 30 RODO tj.:

a. Imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
b. cele przetwarzania;
c. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
f. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

10) Ewidencja osób upoważnionych do przetwarzania danych osobowych

1. Wprowadza się ewidencję osób upoważnionych do przetwarzania danych.
2. Ewidencja zawiera: imię i nazwisko osoby upoważnionej, stanowisko, datę nadania i ustania uprawnień oraz zakres, a w przypadku, kiedy dane są przetwarzane za pomocą programu komputerowego również identyfikator dostępowy do tego programu.
3. Rejestr osób upoważnionych znajduje się w pliku REJESTR_RODO.xls – **załącznik 11**
4. Opcjonalnie dopuszcza się by rejestr osób znajdował się w dziale administracji/Lab.

11) Środki organizacyjne ochrony danych osobowych

1. Przetwarzanie danych osobowych na terenie podmiotu może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień jest ściśle proporcjonalny do tych zadań.
2. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
3. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie wydane przez Administratora Danych Osobowych.
4. Unieważnienie upoważnienia do przetwarzania danych osobowych następuje na piśmie.
5. Każdy pracownik Podmiotu co najmniej raz na rok musi odbyć szkolenie z zakresu ochrony danych osobowych. Nowo przyjęty pracownik odbywa szkolenie przed przystąpieniem do przetwarzania danych.
6. Każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się oraz zrozumieniem wszystkich zasad bezpieczeństwa. Podpisany dokument „Zasady przetwarzania danych osobowych" jest dołączany do akt osobowych pracownika lub stanowi załącznik do zawartej umowy.
7. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.
8. Pomieszczenia stanowiące obszar przetwarzania danych są zamykane na zamek elektroniczny.
9. Po zakończeniu pracy, przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
10. W Spółce zabronione jest udzielanie wszelkich informacji zawierających dane osobowe osobom, których tożsamości nie można zweryfikować. Weryfikacja tożsamości może odbywać się poprzez żądanie okazania dokumentu tożsamości lub innego dokumentu zawierającego zdjęcie wnioskodawcy lub poprzez wykorzystanie informacji zawartej w dokumentacji, która jest znana jedynie wnioskodawcy. Do tego celu należy wykorzystać

metodę pytań bezpośrednich, w których wnioskodawca udzieli poprawnych informacji w co najmniej dwóch zapytaniach.

11. W Spółce niedopuszczalne jest przekazywania jakichkolwiek informacji zawierających dane osobowe podmiotom, instytucjom czy też organom, które nie mogą się wykazać prawidłową podstawą prawną dostępu do danych osobowych.
12. W przypadku konieczności wydania dokumentów zawierających dane osobowe (np. dane pracownika dot. zdrowia itp.) należy każdorazowo weryfikować tożsamość odbierającego za pomocą mechanizmu, o którym mowa w rozdziale 12, a w przypadku, kiedy odbierającym nie jest adresat dokumentu należy zażądać upoważnienia.
13. Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, parapetach itp.
14. Wydruki i inne dokumenty zawierające dane osobowe są przechowywane w pomieszczeniach do tego wyznaczonych. Na stanowiskach pracy mogą być dostępne jedynie dokumenty dotyczące danej sprawy/ danego klienta. Stosowana jest zasada tzw. czystego biurka.
15. Nie należy gromadzić w podręcznej dokumentacji danych osobowych. Wszystkie dane niezbędne do prawidłowej pracy powinny znajdować się w zbiorach.
16. Dokumenty zawierające dane osobowe niszczone są w niszczarkach min. DIN3 lub w przypadku dużej ilości dokumentów, ADO korzystać będzie z usług profesjonalnych podmiotów, zajmujących się utylizacją dokumentacji.
17. Wobec osób, których dane są przetwarzane wykonuje się obowiązek informacyjny, zgodnie z art. 12-14 RODO,
18. Obowiązek informacyjny wobec klientów wykonywany jest poprzez umieszczenie klauzuli informacyjnej na kierowanej do nich korespondencji.
19. Monitory komputerów, na których przetwarzane są dane osobowe zabezpieczone są hasłem uniemożliwiając wgląd osobom postronnym w przetwarzane dane.
20. Dokumenty w wersji elektronicznej, które zapisywane są na nośniki zewnętrzne, przenoszone poza obszary przetwarzania lub przesyłane pocztą elektroniczną, zabezpiecza się poprzez nadanie im haseł odczytu.

21. Zbiory osobowe przetwarzane elektronicznie zabezpiecza się poprzez wykonywanie kopii bezpieczeństwa.
22. Komputery, które przetwarzają zbiory osobowe, za wyjątkiem komputerów służących jedynie do edycji tekstu, należy wyposażyć w urządzenia podtrzymujące napięcie na wypadek braku zasilania.
23. Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jak kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczać stosując wytyczne zawarte w dokumencie Instrukcja Zarządzania Systemem Informatycznym.
24. W celu zapewnienia ochrony danych przetwarzanych elektronicznie, należy zapewnić logowanie do systemu operacyjnego i/lub bezpośrednio do programów przetwarzających dane.
25. Z wszystkimi współpracującymi podmiotami gospodarczymi podpisano, na mocy art. 28 RODO, umowy powierzenia przetwarzania danych osobowych lub w umowach podstawowych wprowadzono uregulowania odnoszące się do obowiązków zapewnienia przestrzegania przepisów RODO przez te podmioty.
26. W biurze Spółki oraz odpowiednio w dziale kadr księgowości prowadzona jest ewidencja osób/podmiotów, z którymi podpisano umowy dostępu i/lub powierzenia**.**

    Szczegółowe zasady postępowania ze zbiorami przetwarzanymi elektronicznie określa Instrukcja zarządzania systemem informatycznym.

12) Udostępnianie danych

1. Spółka udostępnia dane osobowe jedynie na podstawie obowiązujących przepisów prawa i w granicach prawa - **Załącznik 9** Procedura udostępniania dokumentacji medycznej **(badania kliniczne).**
2. Dane osobowe pacjentów, które znajdują się w dokumentacji medycznej są udostępniane na zasadach, w trybie i na sposób określony w przepisach art. 26 i 27 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

3. Ewidencja udostępnionej dokumentacji medycznej prowadzona jest na podstawie art. 27 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta i zawiera, co najmniej: imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna, sposób udostępnienia dokumentacji medycznej;, zakres udostępnionej dokumentacji medycznej, imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna, a w przypadkach, o których mowa w art. 26 *udostępnianie dokumentacji medycznej* ust. 3 i 4, także nazwę uprawnionego organu lub podmiotu, imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną, datę udostępnienia dokumentacji medycznej, podpis przyjmującego dokumentację medyczną.- **załącznik 11.**
4. Spółka udostępnia również dane, na podstawie innych przepisów prawa niż te, o których mowa w ustępie 2 niniejszego paragrafu jedynie na pisemny wniosek i za potwierdzeniem.
5. Spółka przekazując dane drogą pocztową przekazuje je listem poleconym za potwierdzeniem odbioru.
6. W przypadku udostępniania dokumentów za pomocą korespondencji mailowej podmiot ma obowiązek szyfrować przekazywane pliku.

13) Administrator systemu informatycznego

1. Przy rosnącej liczbie zbiorów danych osobowych, dla celów obsługi i zabezpieczenia tych danych w systemie informatycznym Administrator danych może powołać osobnego Administratora Systemu Informatycznego (ASI) i wyznacza mu mi.in. następujący zakres zadań:

a. prowadzenie monitoringu przetwarzania danych,
b. administrowanie systemem informatycznym,
c. stosowanie środków ochrony w ramach oprogramowania użytkowego, systemów operacyjnych, urządzeń teletransmisyjnych, programów antywirusowych oraz ochrony sprzętowej,

d. kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych,
e. kontrola systemu antywirusowego,
f. kontrola awaryjnego zasilania komputerów,
g. kontrola i wykonywanie kopii zapasowych,
h. konserwacja oraz uaktualnienia systemów informatycznych,
i. informowanie na bieżąco ADO o przypadkach awarii programowych wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem, nie przestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystywania sprzętu komputerowego,
j. przedstawianie Administratorowi danych, nie rzadziej niż raz na rok, kompleksowej analizy przetwarzania danych osobowych w systemem informatycznym oraz ewentualne potrzeby w zakresie zabezpieczeń.
k. przedstawianie Administratorowi Danych Osobowych comiesięcznego raportu o pracy sieci informatycznej oraz nośników danych z szczególnym uwzględnieniem zdarzeń niepożądanych, incydentów oraz pozostałych nieautoryzowanych działaniach w obrębie swojego obszaru kompetencyjnego.

14) Inspektor Ochrony Danych Osobowych

1. Z uwagi na fakt, że głównym obszarem działalności Spółki MILTON ESSEX S.A. nie jest przetwarzanie danych, o których mowa w art. 9 ust. 1 w Spółce nie wyznaczony został Inspektor Ochrony Danych Osobowych.
2. Do zarządzania dokumentacją medyczną pacjentów biorących udział w badaniach klinicznych lub innych czynnościach medycznych powołany został Administrator Danych Medycznych .
3. Administrator Danych Medycznych wspomaga ADO w zarządzaniu obszarem danych osobowych w Spółce MILTON ESSEX S.A.

15) Zarządzanie ryzykiem w MILTON ESSEX S.A.

1. W podmiocie przeprowadzana jest analiza ryzyka. Analiza ryzyka może odbywać się dla wszystkich wyodrębnionych zbiorów danych osobowych lub dla procesów przetwarzania.
2. Analiza ryzyka przeprowadzana jest w celu określenia, oceny i minimalizacji zagrożeń, których efektem ma być wdrożenie optymalnych i adekwatnych zabezpieczeń.
3. Analiza ryzyka przeprowadzona jest corocznie, nie później niż do dnia 31 marca dla wszystkich czynności przetwarzania lub w przypadku wprowadzenia nowych procedur lub rozwiązań organizacyjnych w Spółce, zgodnie z odrębną procedurą przyjętą przez Podmiot.

16) Ocena skutków dla ochrony danych osobowych

1. Dla zbiorów danych osobowych, w których znajdują się dane osobowe, których nieuprawnione ujawnienie wiąże się z wysokim ryzykiem uszczerbku dla osób, których dane dotyczą przeprowadzana jest ocena skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO – tzw. Procedura przeprowadzenia PIA.
2. Ocena skutków dla ochrony danych osobowych polega na:

a. opisie planowanych operacji i celów przetwarzania,
b. opisie i ocenie przez administratora czy planowane operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów,
c. ocenie ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
d. opisie środków planowanych w celu zaradzenia ryzykiem, w tym określeniu mechanizmów, zabezpieczeń i środków technicznych, mających zapewnić bezpieczeństwo procesu,

3. Ocena skutków dla ochrony danych odbywa się odrębną procedurą przyjętą przez Podmiot.
4. Za zarządzania ryzykiem oraz ocenę skutków dla ochrony danych osobowych odpowiada Administrator danych osobowych.

5. Analiza ryzyka i ocena skutków dla systemu ochrony danych może odbywać się przy udziale wyznaczonych pracowników przez ADO .
6. Wyznaczony pracownik ma obowiązek sporządzenia corocznego raportu związanego z ryzykiem w Spółce nie później niż do 30 kwietnia.

17) Wykaz zabezpieczeń

1. Środki organizacyjne:

a. Opracowano i wdrożono politykę bezpieczeństwa.
b. Opracowano instrukcję zarządzania systemem informatycznym.
c. Powołano Administratora danych medycznych.
d. Przygotowano stanowisko Administratora Systemu Informatycznego.
e. Do przetwarzania danych dopuszczono wyłącznie osoby, które posiadają upoważnienia nadane przez Administratora Danych Osobowych.
f. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.
g. Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych.
h. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
i. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy;
j. Monitory komputerów, w których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.
k. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer.
l. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
m. 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.

n. Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.

o. W Spółce prowadzi się politykę czystego biurka i ekranu.

2. Środki ochrony fizycznej danych:

a. **Pomieszczenia biurowe -** Zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym zamykanymi drzwiami. Dostęp do pomieszczeń jest ograniczony. Wewnątrz pomieszczeń zbiory danych przechowywane są w zamykanych szafach.

b. **Serwerownia –** pomieszczenie specjalistyczne, zabezpieczone drzwiami z elektronicznym zamkiem szyfrowym. Pomieszczenie z monitorowanymi aspektami środowiskowymi i klimatyzacją w celu utrzymania odpowiednich warunków dla serwera fizycznego. Serwer umieszczony w zamykanej szafie.

Wejście do korytarza serwerowni jest monitorowane.

c. **Zabezpieczenia ogólne budynków -** Monitoring wizyjny, system alarmowy, instalacje ppoż , bramy zamykane na klucz, ochrona fizyczna.

d. Dokumenty zawierające dane osobowe po ustaniu przydatnościci są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

3. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

a. Zbiory danych osobowych przetwarzane przy użyciu komputerów stacjonarnych oraz laptopów.

b. Komputery do przetwarzania danych osobowych są połączone z lokalną siecią komputerową.

c. Zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.

d. Zbiory danych osobowych przetwarzane za pomocą komputerów zabezpieczono za pomocą hasła.

e. Dostęp do systemów operacyjnych stacji roboczych jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika/hasła.
f. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
g. Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.
h. Zastosowano zabezpieczenia kopii serwera w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
i. Użyto zabezpieczenie informatyczne typu Firewall oraz autoryzację dostępu w celu ochrony dostępu do sieci komputerowej.

4. Środki ochrony w ramach narzędzi programowych i baz danych

a. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
b. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
c. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
d. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
e. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
f. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

18) Naruszenie bezpieczeństwa

1) Wszelakie podejrzenia naruszenia bezpieczeństwa danych należy zgłaszać w formie ustnej lub za pośrednictwem poczty elektronicznej ADO lub Administratorowi zgodnie z Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

2) Każdy incydent jest odnotowywany w stosownej bazie danych, a ADO podejmuje stosowne kroki zaradcze.

19) Zasady postępowania w przypadku naruszenia systemu ochrony danych

1. Każda osoba, której Administrator wydał upoważnienie do przetwarzania danych osobowych, ma obowiązek natychmiastowego powiadamiania o występującym zagrożeniu lub wystąpieniu incydentu związanego z systemem ochrony danych osobowych w MILTON ESSEX S.A.
2. Powiadomienie to może mieć charakter ustny lub pisemny.
3. Adresatem takiego powiadomienia jest Administrator Danych.
4. Po otrzymaniu takiego powiadomienia Administrator Danych podejmuje niezwłocznie czynności w celu ustalenia stanu faktycznego.
5. W przypadku uzasadnionego podejrzenia wystąpienia incydentu lub naruszenia systemu ochrony danych osobowych podejmuje działania mające zapobiec dalszym skutkom oraz powiadamia administratora.
6. Po dokonaniu czynności zabezpieczających, Administrator Danych, ma za zadanie przeprowadzić postępowanie wyjaśniające, które:

a. ustali ostateczny zakres, przyczyny wystąpienia oraz skutki, zarówno dla Praktyki, jak i osób, których dane dotyczyły,
b. podejmuje niezbędne czynności mające na celu przywrócenie prawidłowości działania systemu ochrony danych osobowych w Spółce,
c. opracowuje działania naprawcze i zapobiegawcze, których zadaniem jest wyeliminowanie niepożądanych zdarzeń w przyszłości,

d. wskazuje osoby odpowiedzialne za wystąpienie sytuacji.

7. Powyższe czynności są dokumentowane przez Administrator Danych za pomocą formularza zawartego w pliku REJESTR_RODO.xls.- **załącznik 11**
8. Rejestr formularzy, o których mowa w punkcie 7 niniejszego rozdziału prowadzi ADM.
9. Administrator Danych, na ile jest to możliwe, ma obowiązek przedstawienia raportu Administratorowi w czasie umożliwiającym Administratorowi powiadomienie o incydencie lub naruszeniu systemu ochrony danych osobowych organu nadzorczego nie później niż na 72 godziny od czasu jego wykrycia.

20) Kontrole wewnętrzne i audyty bezpieczeństwa

1. Kontrolą przetwarzania danych osobowych zajmuje się Administrator Danych.
2. Kontrole przeprowadzane są regularnie, w terminach ustalonych przez Zarząd wspólnie z Administratorem Danych, a w przypadku wystąpienia incydentu w podmiocie, kompleksową kontrolę obejmującą wszystkie aspekty działalności rozpoczyna się nie później niż 7 dni po zakończeniu działań związanych z incydentem, który wystąpił.
3. Kontrola przeprowadzana jest przy uwzględnieniu minimalnych wytycznych jakimi są: badanie pod względem zgodności z prawem, branżowymi standardami postepowania, normami i przepisami wewnętrznymi.
4. Administrator Danych może wykonywać kontrole osobiście, może, przy pisemnej zgodzie Członka Zarządu wyznaczyć do tego inną osobę lub podmiot.
5. Kontrole przeprowadzane są na podstawie programów kontroli, w których opisywany jest ich zakres, termin, cele oraz metody ich przeprowadzania oraz doraźnie- **załącznik 20**.
6. Jeśli podczas kontroli stwierdzone zostają nieprawidłowości zagrażające systemowi ochrony danych osobowych w podmiocie, kontroler musi niezwłocznie powiadomić o tym fakcie Administratora i Zarząd.
7. Wynik kontroli musi być udokumentowany i przekazany Zarządowi w ciągu 21 dni od jej zakończenia.

21) Realizacja praw osób których dane dotyczą

1. MILTON ESSEX S.A. ułatwia Osobom, których dane osobowe przetwarza realizację przysługujących praw na mocy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)

2. Spółka może wprowadzić ograniczenia w realizacji praw osób, których dane przetwarza i uznać wnioski za bezzasadne, szczególnie powołując się na przepisy m.in. Ustawy o działalności leczniczej, Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz w przypadku, gdy realizacja prawa niekorzystnie może wypłynąć na prawa i wolności innych osób (podmiotów danych).

3. Wszelką komunikację w zakresie realizacji praw Organizacja podejmuje po ustaleniu tożsamości osoby, której dane dotyczą.

4. Komunikacja w zakresie realizacji praw jest wolna od opłat.

5. W przypadku żądań podejmowanych ewidentnie nieuzasadnionych lub nadmiernych, Organizacja w szczególności ze względu na swój ustawiczny charakter, może pobrać dodatkową opłatę lub odmówić podjęcia działań (przy ustaleniu wysokości opłaty uwzględnia się administracyjne koszty udzielenia informacji).

6. Za ewidentnie nieuzasadnione lub nadmierne żądania, które uzasadniają pobranie opłaty bądź odmowę podjęcia działań uznaje się w szczególności skierowane do Spółki:

1) żądania o informacje częściej niż raz na 3 miesiące, jeżeli zakres danych przetwarzanych przez Organizacja bądź inne okoliczności związane z przetwarzaniem nie ulegały zmianie od czasu złożenia poprzedniego żądania;

2) żądania o informacje dzielone sztucznie na kilka lub kilkanaście żądań;

3) żądania szczególnego, niestandardowego formatu odpowiedzi;

4) żądania udzielenia odpowiedzi w języku innym niż polski.

7. Za ewidentnie nieuzasadnione lub nadmierne żądania osoby, które uzasadniają odmowę ich zrealizowania uznaje się w szczególności żądanie informacji, których przekazanie spowodowałyby nieuprawnione ujawnienie tajemnicy przedsiębiorstwa, tajemnicy prawnie chronionej lub danych osobowych innych podmiotów danych.

8. Organizacja każdorazowo uzasadni i poda do wiadomości osoby zgłaszającej żądanie

przyczyny pobrania dodatkowej opłaty lub odmowy podjęcia działań poprzez wskazanie, dlaczego w jego ocenie żądania są ewidentnie nieuzasadnione lub nadmierne.

9. Organizacja bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udzieli osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem złożonym na podstawie art. 15–22 RODO.

10. Z uwagi na skomplikowany charakter żądania lub liczbę żądań termin może być przedłużony o kolejne dwa miesiące. W terminie miesiąca od otrzymania żądania Administrator poinformuje osobę, której dane dotyczą o przedłużeniu terminu, z podaniem przyczyn opóźnienia.

11. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba, że osoba, której dane dotyczą, zażąda innej formy.

12. Jeżeli Organizacja nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – poinformuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego, skorzystania ze środków ochrony prawnej przed sądem.

13. Organizacja udziela informacji na piśmie.

14. Żądania w zakresie realizacji praw na mocy art. 15-22 RODO można składać za pośrednictwem:

- poczty elektronicznej: office@miltonessex.eu
- poczty tradycyjnej na adres: ul. J.P. Woronicza 31/348, 02-640 Warszawa
- osobiście w biurze Spółki.

SPIS TREŚCI

1. Cel

Niniejsza procedura ma na celu ustalenie jednolitego sposobu udostępniania dokumentacji medycznej w MILTON ESSEX S.A. pacjentom, osobom upoważnionym, przedstawicielom ustawowym pacjenta oraz organom i przedmiotom uprawnionym na podstawie obowiązujących przepisów prawa.

2. Podstawy prawne procedury

- Ustawa z dnia 6 listopada 2008r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2018r. poz. 1115 z późn. zm.)
- Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. z 2018r. poz. 1000)

3. Dokumentacja medyczna jest udostępniana:

1) pacjentowi, którego ta dokumentacja dotyczy za okazaniem dowodu tożsamości (dowód osobisty, paszport, inny dokument ze zdjęciem)

2) przedstawicielowi ustawowemu pacjenta za okazaniem odpowiedniego dokumentu:

rodzicom do chwili ukończenia przez dziecko 18 lat, za okazaniem swojego dowodu osobistego i metryki urodzenia dziecka,

lub opiekunom ustanowionym przez sąd, za okazaniem stosownego orzeczenia (opieka nad dzieckiem małoletnim, opieka nad niepełnosprawnym lub ubezwłasnowolnionym, kurator itp.)

3) osobie upoważnionej przez pacjenta w pisemnym upoważnieniu poświadczonym podpisem upoważniającego

4) po śmierci pacjenta prawo do wglądu w dokumentację medyczną ma osoba upoważniona przez pacjenta za życia w pisemnym oświadczeniu.

4. Formy udostępniania dokumentacji medycznej

Dokumentacja jest udostępniana:

1) do wglądu na miejscu w biurze Spółki w obecności pracownika MILTON ESSEX S.A., dotyczy to zarówno dokumentacji papierowej jak i prowadzonej w formie elektronicznej

2) poprzez sporządzenie jej wyciągów, odpisów

3) w formie wydruku z dokumentacji elektronicznej

4) w formie skanów dokumentacji papierowej lub pliku dokumentacji elektronicznej:

- na informatycznym nośniku danych lub

- za pośrednictwem środków komunikacji elektronicznej (z zastrzeżeniem, że pacjent żądając w takiej formie wydania dokumentacji bierze na siebie odpowiedzialność za obieg danych w sieci),

5) poprzez wydanie oryginału za potwierdzeniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu, na żądanie organów władzy publicznej albo sądów powszechnych, a także w przypadku gdy zwłoka w wydaniu dokumentacji mogłaby spowodować zagrożenie życia lub zdrowia pacjenta. Wówczas wykonujemy kserokopię oryginału i pozostawiamy ją w dokumentacji Spółki.

5. Ogólne zasady udostępniania dokumentacji medycznej

1) W celu uzyskania wyciągu, odpisu lub kopii dokumentacji medycznej pacjent, jego przedstawiciel ustawowy lub osoba upoważniona przez niego, składa pisemny „wniosek o wydanie dokumentacji medycznej" (wzór- załącznik nr 1do niniejszej procedury)

2) W przypadku odbioru dokumentacji wymagane jest złożone przez pacjenta upoważnienia dostępu do informacji i dokumentacji medycznej.

3) Wnioski można składać w rejestracji od poniedziałku do piątku w godzinach pracy MILTON ESSEX S.A. .

4) Udostępnienie dokumentacji medycznej następuje bez zbędnej zwłoki w terminie ustalonym indywidualnie z pacjentem, nie dłuższym jednak niż 5 dni roboczych licząc od daty złożenia wniosku

5) Wniosek na udostępnienie dokumentacji można pobrać osobiście lub za pomocą zgłoszenia email na adres office@miltonessex.eu .

6) Do poświadczenia „za zgodność z oryginałem" kopii dokumentacji medycznej upoważniona jest osoba wykonująca kopię dokumentacji .

7) wydanie kopii dokumentacji medycznej musi być potwierdzone podpisem wydającego i odbierającego oraz datą wydania na złożonym wniosku. Wniosek wpinamy do segregatora, a w dokumentacji pacjenta dokonujemy adnotacji o fakcie jej wydania .

8) wydanie i udostępnienie dokumentacji medycznej odnotowuje się również w:

Dokumencie elektronicznym: „Rejestr udostępnionej dokumentacji medycznej”.

Rejestr zawiera następujące wpisy:

- imię i nazwisko pacjenta ,
- zakres udostępnianej dokumentacji
(daty udostępnienia dokumentacji od - do),
- sposób udostępnienia dokumentacji,
- data złożenia wniosku o udostępnienie dokumentacji,
- instytucja lub imię i nazwisko osoby wnioskującej o udostępnienie dokumentacji,
- data wydania dokumentacji
- imię i nazwisko osoby wydającej dokumentację – podpis wniosek ,
- podpis osoby odbierającej dokumentację medyczną – podpis wniosek

9) w przypadku braku możliwości udostępnienia dokumentacji medycznej z powodów uzasadnionych wydaje się pismo: „ załącznik nr 2 do procedury” o odmowie wydania dokumentacji podając w nim przyczynę odmowy

6. Zasady odpłatności

Za pierwszorazowe udostępnienie dokumentacji medycznej nie pobiera się opłat . Zgodnie z obowiązującymi przepisami prawa.

Za każde kolejne udostępnienie dokumentacji w należności od formy udostępnienia stosuje się następujące zasady opłat :

za kopię historii choroby - 60 zł

za odpis z historii choroby – 30 zł

za kopie na nośniku elektronicznym – 50 zł

7. Przechowywanie dokumentacji medycznej

MILTON ESSEX S.A. przechowuje dokumentację medyczną przez okres 20 lat, licząc od daty końca roku kalendarzowego, w którym dokonano w niej ostatniego wpisu z wyjątkiem:

1) Dokumentacji medycznej dotyczącej dzieci do ukończenia 2 roku życia, która jest przechowywana przez 22 lata

2) Skierowań na badania lub zleceń lekarza, które są przechowywane przez 5 lat licząc od końca roku kalendarzowego, w którym udzielono świadczenia będącego przedmiotem

skierowania lub zlecenia lub 2 lata od końca roku kalendarzowego w którym wystawiono skierowanie , ale które nie zostało zrealizowane .

3) Zdjęcia rentgenowskie spoza dokumentacji medycznej 10 lat .

Po upływie okresu przechowywania dokumentacja medyczna jest niszczona w sposób uniemożliwiający identyfikację pacjenta, którego dotyczyła. Pacjent, jego przedstawiciel ustawowy lub osoba upoważniona może zwrócić się z prośbą do Prezes Spółki o wydanie oryginału dokumentacji dopiero po upływie okresu przechowywania dokumentacji medycznej, lecz nie później niż do końca I kwartału roku następnego po tym okresie.

8. Załączniki

1) wniosek o wydanie dokumentacji medycznej

2) odmowa wydania dokumentacji medycznej