Załącznik nr 1 do Zarządzenia Dyrektora ZOZ w Łowiczu nr 34/2020 z dnia 07.05.2020r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

w Zespole Opieki Zdrowotnej w Łowiczu

ROZDZIAŁ I
DEFINICJE I PODSTAWY PRAWNE

§ 1. Polityka ochrony danych osobowych, zwana dalej Polityką, opracowana została na podstawie art 24 ust 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO)

§ 2. Celem polityki jest zapewnienie bezpieczeństwa przetwarzania danych osobowych poprzez zastosowanie jednolitych zasad ich przetwarzania, zgodnych z RODO oraz przepisami szczegółowymi.

§ 3. Polityka określa zasady przetwarzania danych osobowych:

1) we wszystkich komórkach organizacyjnych ZOZ w Łowiczu,
2) w formie dokumentacji papierowej jak również zapisów w systemach informatycznych oraz przechowywanych na elektronicznych nośnikach danych,
3) przez wszystkie osoby przetwarzające dane w imieniu i na odpowiedzialność ZOZ, bez względu na ich formę zatrudnienia lub współpracy,
4) pojedynczych informacji osobowych,
5) w ramach zbiorów danych:
   a) dokumentacji medycznej pacjentów, o której mowa w przepisach ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz wydanych na jej podstawie aktach wykonawczych, a także określonej w przepisach odrębnych,
   b) dokumentacji pracowniczej, w tym pracowników i osób zatrudnionych na podstawie umów-zleceń, osób wykonujących w imieniu ZOZ świadczenia zdrowotne na postawie umów innych niż umowa o pracę, praktykantów, stażystów, kandydatów do pracy,
   c) usługodawców i usługobiorców oraz oferentów,
   d) dokumentacji finansowo-księgowej.

§ 4. Przez użyte w treści niniejszej Polityki określenia należy rozumieć:

1) ZOZ – Zespół Opieki Zdrowotnej w Łowiczu, ul. Ułańska 28,
2) dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie 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,
3) szczególne kategorie danych – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby,
4) dane osobowe dotyczące zdrowia - wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym, przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. zbierane podczas jej rejestracji do usług opieki zdrowotnej, podczas świadczenia jej usług opieki zdrowotnej, w tym numer, symbol lub oznaczenie przypisane danej osobie fizycznej, informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, których źródłem może być pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne,
5) podmiot danych – osoba fizyczna, której dane dotyczą,
6) administrator danych osobowych – Zespół Opieki Zdrowotnej w Łowiczu, reprezentowany przez Dyrektora Opieki Zdrowotnej w Łowiczu- zwany dalej ADO. Administratorem danych osobowych pacjentów nie jest osoba prowadząca jednoosobową działalność gospodarczą, lub też działająca w imieniu innego podmiotu, wykonująca zawód medyczny, w zakresie w jakim wykonuje swoje zadania w ramach działalności leczniczej prowadzonej przez ZOZ.

7) inspektor ochrony danych (IOD)-wyznaczona przez dyrektora ZOZ w Łowiczu osoba bezpośrednio nadzorująca i odpowiedzialna za realizację przepisów w zakresie ochrony danych osobowych w ZOZ w Łowiczu,
8) administrator systemu informatycznego (ASI) – wyznaczona przez dyrektora ZOZ w Łowiczu osoba odpowiedzialna za funkcjonowanie systemów i sieci informatycznych ZOZ w Łowiczu oraz za przestrzeganie zasad i wymagań bezpieczeństwa tych systemów i sieci w procesach przetwarzania informacji,
9) zbiór danych osobowych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub miejscowo,
10) 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,
11) 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,
12) usuwanie danych – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
13) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
14) osoba przetwarzające dane osobowe – pracownik ZOZ w Łowiczu oraz osoba działająca na rzecz i w imieniu ZOZ w Łowiczu na podstawie umów innych niż umowa o pracę, upoważniona przez ADO do przetwarzania danych zwana dalej - osobą przetwarzającą,
15) osoba wykonująca zawód medyczny - osoba uprawniona na podstawie odrębnych przepisów do udzielania świadczeń zdrowotnych, w tym m.in. lekarz, lekarz dentysta, pielęgniarka, położna, ratownik medyczny, diagnosta laboratoryjny, fizjoterapeuta, technik analityki medycznej i inne osoby wskazane w art. 6a ustawy o diagnostyce laboratoryjnej, farmaceuta, technik farmacji, psycholog, psychoterapeuta, fizjoterapeuta, a także osoby wykonujące inne zawody wskazane w tabeli nr 1 załącznika nr 3 do rozporządzenia Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych,
16) pacjent - osoba zwracająca się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub osobę wykonującą zawód medyczny, oraz osoba, która korzystała z takich świadczeń w przeszłości.
17) osoba postronna - każda osoba za wyjątkiem osoby wyznaczonej do przetwarzania danych, w wyznaczonym do tego pomieszczeniu i na danym etapie przetwarzania, w tym również inny pracownik ZOZ. Osobą postronną nie jest inny pracownik ZOZ wykonujący czynności zawodowe w pomieszczeniu współdzielonym, chyba że wymaga tego szczególny charakter czynności.
18) 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.

§ 5. Główne przepisy prawne stanowiące szczegółową podstawę przetwarzania danych w ZOZ w zakresie:

1. Świadczeń zdrowotnych
   1) Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej,

2) Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania,
3) Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych,
4) Rozporządzenie Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych,
5) Ustawa z dnia 12 kwietna 2019 r. o opiece zdrowotnej nad uczniami.
6) Ustawa z dnia 27 czerwca 1997 r. o służbie medycyny pracy,
7) Rozporządzenie Ministra Zdrowia z dnia 26 sierpnia 2014 r. w sprawie badań lekarskich kandydatów do szkół ponadgimnazjalnych lub wyższych i na kwalifikacyjne kursy zawodowe, uczniów tych szkół, studentów, słuchaczy kwalifikacyjnych kursów zawodowych oraz uczestników studiów doktoranckich.
8) Rozporządzenie Ministra Zdrowia z dnia 29 lipca 2009r. w sprawie rodzajów dokumentacji medycznej służby medycyny pracy, sposobów jej prowadzenia i przechowywania oraz wzorów stosowanych dokumentów.
9) Ustawa z dnia 22 sierpnia 1997 r. o publicznej służbie krwi
10) Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe,
11) Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi,
12) Ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego,

2. Realizacji innych obowiązków prawnych
   1) Ustawa z dnia 6 czerwca 1997 r. kodeks postępowania karnego
   2) Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach
   3) Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia
   4) Rozporządzenie Ministra Sprawiedliwości z dnia 23 lutego 2005 r. w sprawie poddawania badaniom lub wykonywania czynności z udziałem oskarżonego oraz osoby podejrzanej,
   5) Rozporządzenie Ministra Zdrowia i Ministra Spraw Wewnętrznych i Administracji z dnia 28 grudnia 2018 r. w sprawie badań na zawartość alkoholu w organizmie,
   6) Rozporządzenie Ministra Spraw Wewnętrznych z dnia 13 września 2012 r. w sprawie badań lekarskich osób zatrzymanych przez Policję;
3. Spraw pracowniczych
   1) Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy,
   2) Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych,
   3) Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych,
   4) Ustawa z dnia 23 maja 1991 r. o związkach zawodowych,
   5) Ustawa z dnia 1 lipca 2011 r. o samorządzie pielęgniarek i położnych,
   6) Ustawa z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych,
   7) Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych;
4. Spraw finansowych i współpracy z kontrahentami
   1) Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych
   2) Ustawa z dnia 29 września 1994 r. o rachunkowości

ROZDZIAŁ II
OGÓLNE ZASADY PRZETWARZANIA DANYCH

§ 6. 1. Dane osobowe są przetwarzane na podstawie ustawy i w zakresie określonym przez ustawę.

2. Dane są przetwarzane rzetelnie i w sposób przejrzysty dla podmiotu danych w konkretnych, wyraźnych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami, ograniczone do tego, co niezbędne do celów, w których są przetwarzane oraz przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów przetwarzania, lub okres określony przepisami prawa.

3. Przetwarzanie danych wyłącznie do celów archiwalnych w interesie publicznym, badań naukowych, historycznych, statystycznych po upływie okresu o którym mowa w ustępie 1 jest dopuszczalne.

4. Przetwarzanie danych może odbywać się również na podstawie zgody podmiotu danych. Zgoda ta powinna mieć formę pisemną, wskazywać datę jej udzielenia oraz określać cele jakich dotyczy.

1) Przed wyrażeniem zgody podmiot danych otrzymuje informację o przetwarzaniu jego danych.
2) Zgoda w formie pisemnej nie jest wymagana gdy działanie podmiotu danych potwierdzające zgodę jest wyraźne i jednoznaczne. Poprzez wyraźne działanie rozumie się, w szczególności, wybór przez podmiot danych określonych ustawień technicznych w systemie informatycznym, własnoręczne wypełnienie pól formularzy, przekazanie danych osobowych przez pacjenta w celu rejestracji do świadczeń medycznych oraz wysłanie lub zatwierdzenie wprowadzonych zmian. § 6 ust.4 punkt 1) stosuje się odpowiednio.
3) Zgoda może być wycofana w każdym czasie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Podmiot danych, jest o tym informowany przed wyrażeniem zgody. Jeżeli wycofanie zgody odbywa się poprzez ustne oświadczenie podmiotu danych osoba przetwarzająca odnotowuje w odnośnej dokumentacji ten fakt z oznaczeniem daty oraz podejmuje właściwe czynności w celu zaniechania dalszego przetwarzania.
4) Podmiot danych powinien uzyskać informacje, jakie są konsekwencje niewyrażenia zgody na przetwarzanie danych, w odniesieniu do pacjentów nie może to mieć wpływu na możliwość uzyskania świadczeń zdrowotnych i ich jakość.

§ 7. Dane osobowe mogą być przetwarzane po spełnieniu co najmniej jednego z warunków:

1) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO,
2) 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,
3) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
5) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią.

§ 8. Szczególne kategorie danych mogą być przetwarzane jeżeli:

1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych,
2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez ADO lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
3) 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,

4) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
5) jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń,
6) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa,
7) 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
8) 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,
9) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

§ 9. 1. Dane dotyczące zdrowia pacjentów mogą być przetwarzane jeżeli jest to niezbędne do celów udzielania świadczeń zdrowotnych, profilaktyki zdrowotnej lub medycyny pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego przez osobę wykonująca zawód medyczny.

2. Dane te mogą być przetwarzane również w celu rejestracji do świadczeń zdrowotnych, weryfikacji uprawnień do tych świadczeń, zarządzania systemami i usługami opieki zdrowotnej, w tym rozliczeń z płatnikami, wykonywania innych czynności pomocniczych przy udzielaniu świadczeń zdrowotnych, utrzymania systemu informatycznego oraz przekazywania danych pacjentów do rejestrów publicznych prowadzonych na podstawie ustawy przez inne osoby.

3. Dane te mogą być również przetwarzane w niezbędnym zakresie w celu przygotowania osób do wykonywania zawodu medycznego i kształcenia osób wykonujących zawód medyczny.

4. Dane dotyczące przekonań religijnych pacjentów mogą być przetwarzane wyłącznie w trybie art. 37 Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Wymogu zgody w formie pisemnej w tym przypadku nie stosuje się.

5. Dane dotyczące naruszeń prawa i środków powiązanych mogą być przetwarzane wyłącznie w zakresie niezbędnym do realizacji decyzji sądu.

§ 10. Dane dotyczące pracowników w zakresie określonym przez Kodeks pracy mogą być przetwarzane wyłącznie w celu prowadzenia akt pracowniczych, w tym ewidencji czasu pracy, rozliczeń z pracownikami, naliczania obciążeń, składek i świadczeń, zapewnienia warunków i narzędzi pracy, doskonalenia zawodowego, zgłoszeń do organów wobec których obowiązek taki wynika z ustawy.

1) Dane dotyczące kandydatów do pracy w zakresie określonym przez Kodeks pracy mogą być przetwarzane wyłącznie w celu przeprowadzenia rekrutacji, chyba że kandydat wyraża zgodę na udział w przyszłych rekrutacjach.
2) Dane dotyczące stażystów i praktykantów mogą być przetwarzane wyłącznie w celu zapewnienia odbycia praktyki lub stażu, oraz dochodzenia roszczeń lub obrony przed roszczeniami.
3) Dane dotyczące zdrowia pracowników mogą być przetwarzane wyłącznie do celów profilaktyki zdrowotnej lub medycyny pracy oraz do oceny zdolności pracownika do pracy.
4) Dane dotyczące zdrowia osób wykonujących w imieniu ZOZ świadczenia zdrowotne mogą być przetwarzane wyłącznie w zakresie zdolności zdrowotnej do wykonywania świadczeń.
5) Dane dotyczące przynależności do związków zawodowych mogą być przetwarzane wyłącznie na podstawie zgody podmiotu danych w zakresie określonym ustawą z dnia 23 maja 1991 r. o związkach zawodowych oraz kodeks pracy.

6) Dane dotyczące sytuacji rodzinnej i materialnej oraz życiowej pracowników i innych osób mogą być przetwarzane w celu realizacji zadań zakładowego funduszu świadczeń socjalnych określonych w ustawie, za zgodą podmiotu danych.
7) Dane dotyczące sytuacji rodzinnej pracownika mogą być przetwarzane w przypadku korzystania przez pracownika ze szczególnych uprawnień określonych w prawie pracy za zgodą pracownika wyrażoną poprzez złożenie wniosku o te świadczenia.

§ 11. W ZOZ nie są przetwarzane dane: dotyczące przynależności do organizacji innych niż określone w § 10, punkt 5) oraz do których przynależność wynika z obowiązku ustawowego, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, lub światopoglądowe, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące seksualności lub orientacji seksualnej osoby.

§ 12. 1. Dane osobowe przetwarzane w ZOZ są upubliczniane tylko w przypadkach gdy obowiązek taki wynika z ustawy i w zakresie określonym ustawą.

2. Dane osobowe dotyczące pacjentów nie są upubliczniane w żadnym trybie ani zakresie.

3. Dane osobowe pracowników mogą być upubliczniane w zakresie niezbędnym do realizacji zadań i obowiązków pracodawcy związanych z prowadzeniem zakładu.

§ 13. 1. Dane osobowe mogą być udostępniane innym podmiotom tylko na podstawie ustawy i w zakresie określonym ustawą.

2. Dane te mogą być również udostępnione osobom przetwarzającym w zakresie niezbędnym do realizacji zadań powierzonych przez ZOZ, oraz podmiotowi danych.

3. Dane zawarte w dokumentacji medycznej mogą być udostępniane podmiotom wykonującym działalność leczniczą, w celu zapewnienia kontynuacji świadczeń opieki zdrowotnej.

4. Dane zawarte w dokumentacji medycznej mogą być udostępniane innym podmiotom i osobom tylko w trybie zarządzenia Dyrektora ZOZ wydanego na postawie art 9 i 26 Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

§ 14. Dane osobowe, w tym dane zawarte w dokumentacji medycznej, na podstawie pisemnej umowy, mogą być powierzone do przetwarzania, podmiotom przetwarzającym. które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych chroniących prawa osób, których dane dotyczą oraz spełniają wymogi RODO, w szczególności art. 28 ust. 1 RODO.

1) Stosowane środki powinny zapewniać, że proces przetwarzania nie będzie powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej.
2) Przed powierzeniem przetwarzania, ADO ocenia, czy podmiot przetwarzający zapewnia wystarczające gwarancje. Ocena ta może się opierać o przebieg uprzedniej współpracy z danym podmiotem.
3) ADO zastrzega sobie prawo osobistej kontroli bezpieczeństwa przetwarzania danych w siedzibie podmiotu przetwarzającego.

§ 15. 1 Osoba przetwarzająca przetwarza dane osobowe na podstawie pisemnego upoważnienia wydanego przez ADO, wyłącznie w zakresie wykonywania obowiązków zawodowych lub wykonania umowy z ADO. Osoba przetwarzająca nie może przetwarzać danych wykraczających poza minimalny zakres, niezbędny do wykonania powierzonych jej zadań.

§ 16. 1. Źródłem danych osobowych przetwarzanych przez ZOZ jest podmiot danych albo osoba reprezentująca jego prawa lub działająca z jego upoważnienia.

2. Źródłem danych osobowych członków rodziny jest pracownik korzystający ze szczególnych świadczeń przewidzianych przez Kodeks pracy.

3. Źródłem danych osobowych może być oferent lub kontrahent w odniesienie do danych, których jest administratorem.

4. W szczególnych, uzasadnionych przypadkach, źródłem danych może być inna osoba niż podmiot danych.

5. Źródłem danych osobowych pacjentów może być również pracownik służby zdrowia, urządzenie medyczne lub badanie laboratoryjne lub diagnostyczne. albo inny podmiot wykonujący działalność leczniczą udostępniający dane pacjentów w trybie art. 26 ust. 3 pkt. 1 Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta lub podmiot powierzający je na podstawie umowy.

1) Źródłem danych osobowych osób upoważnionych przez pacjenta w trybie art 14 ust. 1 pkt.1 oraz art 26 ust.3 pkt.1 jest pacjent.
2) Źródłem danych pacjentów w zakresie weryfikacji uprawnień do świadczeń zdrowotnych jest EWUŚ.

6. W ZOZ nie są zbierane ani przetwarzane dane osobowe pochodzące z innych źródeł.

7. W ZOZ dane nie są przetwarzane w sposób zautomatyzowany.

1) Zautomatyzowanym przetwarzaniem danych pacjentów nie jest: automatyczne ustalanie wyników skal stosowanych w medycynie, automatyczne klasyfikowanie wyniku na podstawie zdefiniowanych przedziałów wyników (zależnych od czynników wynikających z danych Pacjenta takich jak m.in. płeć czy wiek), wspieranie, za pomocą algorytmów procesu terapeutycznego np. poprzez przedstawienie sugestii badania diagnostycznego, sugestii terapii farmakologicznej i podobnych przez system komputerowy, pod warunkiem, że ostateczną decyzję o sposobie leczenia podejmuje personel medyczny, działanie aplikacji i algorytmów będących wyrobami medycznymi lub częściami wyrobów medycznych, pod warunkiem że wyroby takie zostały dopuszczone do obrotu na terytorium Unii Europejskiej w zgodzie z obowiązującymi przepisami prawa, w zakresie dokonanej certyfikacji.
2) Zautomatyzowanym przetwarzaniem danych nie są procesy dotyczące badań profilaktycznych i medycyny pracy, gdzie decyzja o skierowaniu Pacjenta na określone badania opiera się o czynniki charakterystyczne dla danego stanowiska pracy (zdefiniowane przez pracodawcę), a nie czynniki charakterystyczne dla osoby Pacjenta.
3) Zautomatyzowanym przetwarzaniem danych nie jest przekazywanie danych bezpośrednio z systemu informatycznego do rejestrów państwowych, w ramach realizacji obowiązku prawnego.

8. Dane osobowe nie są wykorzystywane do zautomatyzowanej 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.

9. Dane osobowe zawarte w korespondencji telefonicznej i elektronicznej są przetwarzane wyłącznie w celu wynikającym z treści tej korespondencji.

10. Na stronie internetowej ZOZ, dla wygody użytkowników, mogą być umieszczane linki prowadzące do stron zewnętrznych, nie prowadzonych przez ZOZ. ZOZ nie ponosi odpowiedzialności za zbieranie i przetwarzanie danych przez te strony.

ROZDZIAŁ III
ZASADY DOTYCZĄCE REALIZACJI PRAW PODMIOTU DANYCH

§ 17. 1. ADO zapewnia spełnienie obowiązku informacyjnego wobec podmiotu danych poprzez klauzule informacyjne publikowane na stronie internetowej, jako załącznik do formularzy dokumentów aplikacyjnych, w menu telefonicznych połączeń przychodzących, uwidocznienie ogłoszeń w miejscach dostępnych dla podmiotu danych, przedstawianie indywidualnych klauzul podmiotowi danych.

2. Spełnienie obowiązku informacyjnego wobec podmiotu danych następuje przed przyjęciem od podmiotu danych jego danych.

3. Informację określoną w ust.1 ADO zapewnia również na żądanie podmiotu danych.

4. Wymogu określonego w ust. 1 nie stosuje się wobec osób upoważnionych przez pacjenta w trybie art. 9 ust. 3 oraz 26 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta

5. Wymogu określonego w ust. 1 można nie stosować również w przypadku, gdy osoba, której dane dotyczą, dysponuje już tymi informacjami; udzielenie informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku lub pozyskiwanie danych jest wyraźnie uregulowane prawem, któremu podlega ADO, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą.

§ 18. Komunikację z podmiotem danych w zakresie realizacji jego praw prowadzi się w języku polskim; w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem; w formie w jakiej został złożony wniosek lub żądanie, chyba że inna forma wynika z istoty czynności lub treści wniosku podmiotu.

1) Komunikację z podmiotem danych w zakresie realizacji jego praw jako podmiotu danych podejmuje się po ustaleniu jego tożsamości. Komunikacja ta jest wolna od opłat.
2) Realizacja praw podmiotu danych określonych w art 15-22 RODO jest wolna opłat przy czym pierwsza kopia danych jest wydawana nieodpłatnie, za kolejne kopie jest pobierana opłata zgodnie z cennikiem lub w wysokości rzeczywistych kosztów administracyjnych jeżeli cennik nie został określony. Wydanie podmiotowi danych, kopii jego danych nie może naruszać praw i wolności innych osób, przy czym naruszenia tego nie stanowi ujawnienie danych osób dokonujących wpisu w dokumentacji oryginalnej.
3) Prawo podmiotu danych do bycia zapomnianym nie znajduje zastosowania wobec danych w zakresie w jakim przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku, któremu podlega ADO, lub do ustalenia, dochodzenia lub obrony roszczeń.
4) Można odmówić realizacji żądania, jeśli jest ono ewidentnie nieuzasadnione lub nadmierne jednakże do wiadomości żądającego należy podać przyczynę przyczyny odmowy podjęcia działań.

§ 19. 1. Przyjmowanie danych od podmiotu danych odbywa się w wydzielonych pomieszczeniach, w obecności upoważnionych osób przetwarzających, bez obecności osób postronnych.

2. W przypadkach, w których przetwarzanie danych odbywa się na podstawie ustawy, odmowa podania wymaganych danych osobowych skutkuje odmową udzielenia świadczenia lub zawarcia umowy.

3. Przyjmowanie danych pacjentów odbywa się również w wyznaczonych punktach rejestracji, które są wyraźnie oznaczone oraz wydzielone poprzez naklejenie na podłodze przed stanowiskiem rejestracji taśmy w jaskrawych barwach wyznaczającej obszar, w którym przebywa tylko osoba obsługiwana przez rejestrację, zamieszczenie komunikatu o konieczności przebywania przy stanowisku rejestracyjnym tylko jednej osoby, oddzielenie strefy rejestracji, wprowadzenie możliwości rejestracji elektronicznej lub telefonicznej.

§ 20. 1. Weryfikowanie tożsamości podmiotu danych następuje przed utrwaleniem jego danych w oparciu o dokument tożsamości wydany na podstawie ustawy, zawierający co najmniej imię i nazwisko, zdjęcie osoby, numer PESEL. Dokumentem potwierdzającym tożsamość jest w szczególności: dowód osobisty, prawo jazdy, paszport, legitymacja studencka, legitymacja szkolna.

2. Nie sporządza się kopii dokumentu na podstawie którego ustalono tożsamość podmiotu danych, jednakże można odnotować cechy tegoż dokumentu.

3. Weryfikacja danych pacjenta pozostającego pod władzą przedstawiciela ustawowego lub opiekuna faktycznego następuje poprzez weryfikacje tożsamości tegoż przedstawiciela lub opiekuna i przyjęcie od niego oświadczenia o tożsamości pacjenta.

4. W przypadku, gdy weryfikacja tożsamości realizowana jest w sposób inny niż osobiście lub przy użyciu środków komunikacji elektronicznej lub w sytuacji powzięcia wątpliwości co do tożsamości osoby, można zażądać dodatkowych informacji lub podjęcia przez podmiot danych

dodatkowych działań niezbędnych do potwierdzenia tożsamości tej osoby, takich jak: porównanie podanych danych z już posiadanymi, żądanie podania dodatkowych danych osobowych lub przy wykorzystaniu kwalifikowanego podpisu elektronicznego lub podpisu potwierdzonego profilem zaufanym ePUAP, przelewu bankowego potwierdzającego zgodność danych, uwierzytelnianie za pośrednictwem systemów informatycznych udostępnianych w ramach systemu informacji w ochronie zdrowia, kontrolę na odległość dokumentu potwierdzającego tożsamość.

5. Żądanie dodatkowego potwierdzenia tożsamości nie może być dla podmiotu danych uciążliwe ponad miarę.

6. Wymogu określonego w ust. 1 nie stosuje się wobec pacjentów jeżeli ustalenie tożsamości przed uzyskaniem świadczenia nie jest możliwe i mogłoby istotnie utrudnić lub uniemożliwić uzyskanie świadczenia. W przypadku tym ustalenie tożsamości następuje gdy tylko jest możliwe.

§ 21. 1. Wywoływanie pacjenta do udzielenia świadczenia nie może odbywać się przy użyciu nazwiska i odbywa się poprzez wyznaczenie godzin udzielenia świadczenia, kolejność ustanowioną w procesie rejestracji, przy użyciu numerów porządkowych nadawanych w procesie rejestracji, kolejność ustanowioną przez samych pacjentów.

2. O ile zidentyfikowanie pacjenta przy użyciu wyżej wymienionych środków nie jest możliwe, wywołanie może nastąpić po imieniu, a następnie należy potwierdzić jego tożsamości bez obecności osób postronnych.

ROZDZIAŁ IV
OCHRONA FIZYCZNA

§ 22. 1.Budynki i pomieszczenia, w których przetwarzane są dane osobowe, powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osobom postronnym, na czas nieobecności osób przetwarzających poprzez adekwatne rozwiązania techniczne.

2. Przebywanie osób postronnych w pomieszczeniach, w których dane są przetwarzane jest dopuszczalne wyłącznie za pozwoleniem i w obecności osoby przetwarzającej.

§ 23. 1. ADO podejmuje niezbędne działania techniczne i organizacyjne w celu minimalizacji ryzyka naruszenia ochrony danych osobowych na każdym etapie przetwarzania, a zwłaszcza podczas przyjmowania od podmiotu danych jego danych oraz weryfikowania tożsamości podmiotu danych.

2. Osoba przetwarzające dane, z uwzględnieniem możliwości technicznych i lokalowych podczas przetwarzania danych, podejmuje niezbędne środki w celu minimalizacji ryzyka ujawnienia danych, w szczególności danych o stanie zdrowia, osobom postronnym.

§ 24. Zabrania się, bez względu na czasokres nieobecności osoby przetwarzającej w pomieszczeniu:

1) pozostawiania drzwi do pomieszczenia niezamkniętych na klucz przez ostatnią wychodząca osobę,
2) pozostawiania klucza w zamku od zewnątrz, zarówno podczas pobytu w pomieszczeniu jak również po opuszczeniu go i zamknięciu zamka,
3) pozostawiania otwartych okien w pomieszczeniach, zwłaszcza na porterze; w razie konieczności, za wyjątkiem pierwszej kondygnacji, okna mogą na czas chwilowej nieobecności pozostać uchylone,
4) pozostawiania w pomieszczeniu osoby postronnej, bez nadzoru,
5) pozostawianie otwartych okien obsługowych w pomieszczeniach rejestracji.

§ 25. 1. Sposób postępowania z danymi na etapie ich bieżącego przetwarzania oraz po jego zakończeniu, określa Instrukcja kancelaryjna Zespołu Opieki Zdrowotnej w Łowiczu.

2. Dane osobowe przetwarzane zarówno w formie papierowej, jak też na elektronicznych nośnikach danych, należy przechowywać w szafach zamykanych na klucz.

3. Dokumenty i elektroniczne nośniki danych, na których są wykonywane bieżące operacje przetwarzania, mogą znajdować się poza szafą, jedynie na czas tego przetwarzania

4. Zbędne kopie, wydruki, zapiski, nie będące dokumentem źródłowym, powinny być niszczone niezwłocznie, poprzez fizyczne rozkawałkowanie nośnika w sposób uniemożliwiający odtworzenie danych.

5. Przechowywanie dokumentów po okresie ich bieżącego przetwarzania oraz niszczenie dokumentów źródłowych, po upływie okresu przechowywania, odbywa się na podstawie Instrukcji w sprawie organizacji i działania składnicy akt w Zespole Opieki Zdrowotnej w Łowiczu.

ROZDZIAŁ V
DODATKOWE ŚRODKI OCHRONY DANYCH OSOBOWYCH PRZETWARZANYCH W FORMIE ELEKTRONICZNEJ

§ 26. 1. Szczegółowe zasady funkcjonowania i użytkowania systemu informatycznego określa „instrukcja zarządzania systemem informatycznym ZOZ w Łowiczu.

2. Osoba przetwarzająca wykonująca czynności zawodowe przy użyciu systemu informatycznego zobowiązana jest do zapoznania się i przestrzegania „instrukcji zarządzania systemem informatycznym ZOZ w Łowiczu".

§ 27. 1. Korespondencja elektroniczna wewnętrzna może być prowadzona tylko przy użyciu poczty zakładowej. Korespondencja elektroniczna zewnętrzna w miarę możliwości powinna być prowadzona przy użyciu poczty zakładowej.

2. Wydruki zawierające dane z systemu informatycznego podlegają ochronie jak dokumentacja w formie papierowej.

3. Dane osobowe przetwarzane wyłącznie w stacji roboczej lub urządzeniu mobilnym, w tym pliki i dokumenty oraz wiadomości tekstowe należy usuwać niezwłocznie po ich wykorzystaniu, chyba że ich dalsze przetwarzanie jest nakazane przepisami prawa.

§ 28. Prawo dostępu do systemu informatycznego na określonym poziomie nadaje ASI, stosownie do zakresu obowiązków osoby przetwarzającej w trybie określonym w instrukcji zarządzania systemem informatycznym ZOZ w Łowiczu.

§ 29. ASI oraz osoby przetwarzające dane przy użyciu systemu informatycznego są zobowiązane informować IOD o ewentualnych przypadkach naruszenia bezpieczeństwa systemu ochrony danych osobowych.

ROZDZIAŁ VI
ZASADY PRZEKAZYWANIA INFORMACJI DOTYCZĄCYCH PACJENTA W STNANACH NAGŁYCH

§ 30. ZOZ może podjąć kontakt z osobą trzecią, która nie została przez pacjenta upoważniona w rozumieniu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w celu przekazania lub uzyskania danych, w tym danych o stanie zdrowia Pacjenta, niezbędnych dla ochrony żywotnych interesów Pacjenta lub innej osoby, w szczególności ochrony zdrowia lub życia tych osób, w przypadku, w którym Pacjent nie jest fizycznie albo prawnie zdolny do wyrażenia zgody w odpowiednim czasie, a w szczególności w przypadku:

1) nagłej utraty przytomności przez Pacjenta, gdy niezbędne jest uzyskanie dodatkowych informacji o stanie zdrowia Pacjenta w celu udzielania świadczeń zdrowotnych lub przekazanie informacji o pacjencie,

2) gdy Pacjent znajduje się w stanie uniemożliwiającym mu świadome wyrażenie zgody lub udzielenie wiarygodnych informacji a niezbędne jest uzyskanie dodatkowych informacji o stanie zdrowia Pacjenta w celu udzielania świadczeń zdrowotnych,

3) uzyskania wyniku badania diagnostycznego, które wymaga podjęcia pilnych działań medycznych, przy braku możliwości kontaktu z Pacjentem w odpowiednim czasie przy wykorzystaniu standardowych środków komunikacji.

§ 31. Osobą o której mowa w §30 może być osoba bliska lub osoba, której dane odnotowano w dokumentacji medycznej pacjenta w związku z uprzednim leczeniem, osoba odbierająca telefon, którego numer został wskazany przez pacjenta, świadek zdarzenia w trakcie bądź w wyniku którego Pacjent został poszkodowany, osoba kontaktująca się z ZOZ z inicjatywy własnej, która dostatecznie uprawdopodobni fakt bycia osobą bliska dla pacjenta.

§ 32. Działania określone w §30 podejmowane są jedynie w sytuacjach wyjątkowych, gdy nie jest możliwe udostępnienie lub uzyskanie danych od osób upoważnionych zgodnie z przepisami prawa medycznego z zastrzeżeniem, że:

1) w miarę możliwości weryfikuje się, poprzez sprawdzenie wiedzy na temat pacjenta, a także odnotowuje tożsamość osoby trzeciej, której się udostępnia lub od której uzyskuje się dane osobowe,

2) w dokumentacji medycznej pacjenta odnotowuje się okoliczności udostępnienia danych osobowych Pacjenta z uzasadnieniem zaistnienia stanu zagrożenia dla życia lub zdrowia Pacjenta,

3) w miarę możliwości podejmuje działania w celu dostatecznego uprawdopodobnienia zasadności kontaktu z osobą trzecią w celu ochrony żywotnych interesów Pacjenta.

ROZDZIAŁ VII
NADAWANIE UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 33. 1. Podstawą do przetwarzania danych, jest pisemne upoważnienie wydane przez ADO które określa zbiór danych, zakres przetwarzania oraz termin ważności. Wzór upoważnienia stanowi załącznik nr 1.

2. Podstawą wydania upoważnienia jest karta obiegowa przyjęcia do pracy lub podpisana umowa o wykonywaniu świadczeń opieki zdrowotnej w imieniu ZOZ.

3. Dział Spraw Pracowniczych jest zobowiązany informować IOD o zatrudnieniu pracownika lub zawarciu innej umowy skutkującej przetwarzaniem danych osobowych przez osobę niebędąca pracownikiem.

4. IOD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

§ 34. 1. Przed wydaniem upoważnienia ADO lub wyznaczona przez niego osoba zapoznaje pracownika z zasadami przetwarzania danych na stanowisku pracy oraz przyjmuje od niego oświadczenie o zachowaniu w tajemnicy wszelkich danych osobowych uzyskanych w związku zatrudnieniem, również po ustaniu zatrudnienia. Wzór oświadczenia stanowi załącznik nr 2.

2. Wymóg złożenia pisemnego oświadczenia nie dotyczy osób, dla których obowiązek zachowania w tajemnicy danych osobowych uzyskanych w związku z wykonywaniem zawodu został określony w ustawie, chyba że ustawa tak stanowi.

§ 35. Upoważnienie traci moc z chwilą upływu terminu na jaki zostało wydane lub ustania zatrudnienia lub zakończenia wykonywania umowy.

ROZDZIAŁ VIII
POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH

§ 36. 1. Naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,

nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

2. Do zdarzeń o których mowa w ust. 1 w szczególności należą:

1) ślady na drzwiach, oknach i szafach wskazujące na włamanie lub próbę włamania,
2) fizyczna obecność w pomieszczeniach, bez obecności osoby upoważnionej, osób zachowujących się podejrzanie,
3) pozostawianie otwartych drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, bez nadzoru osoby przetwarzającej,
4) pozostawianie dokumentów lub ich kopii w drukarkach i kserokopiarkach dostępnych dla osób postronnych,
5) niszczenie nośników danych w sposób umożliwiający ich odtworzenie,
6) wykonywanie pracy na informacjach służbowych w celach prywatnych,
7) ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
8) wynoszenie danych osobowych w wersji papierowej lub elektronicznej poza teren ZOZ bez upoważnienia,
9) udostępnienie danych osobowych osobom nieupoważnionym,
10) stwierdzenie próby lub modyfikacji lub usunięcia danych bez odpowiedniego upoważnienia,
11) kopiowanie danych, w tym w formie elektronicznej, nie mające uzasadnienia,
12) bezprawny zabór nośników danych,
13) utrata kontroli nad kopią danych osobowych,
14) pojawienie się wirusa komputerowego lub niestandardowe działanie komputerów,
15) inne zachowania lub zdarzenia , które mogą prowadzić do naruszenia ochrony danych.

§ 37.1. Osoba przetwarzająca, która stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązana:

1) niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu, który zgłasza ten fakt IOD.

2) podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

2. Osoba przetwarzająca jest zobowiązana również zgłosić IOD sytuacje mogące prowadzić do naruszenia ochrony danych.

3. ASI jest zobowiązany do informowania IOD o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem naruszenia bezpieczeństwa przetwarzania danych osobowych.

§ 38. W przypadku stwierdzenia naruszenia ochrony danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub innej osoby upoważnionej przez ADO.

§ 39. IOD po uzyskaniu informacji o której mowa w § 36 ust.1. podejmuje następujące kroki:

1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,

2)odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,

3)nawiązuje kontakt ze specjalistami zewnętrznymi, jeśli zachodzi taka potrzeba,

4)dokumentuje zaistniały przypadek naruszenia ochrony danych,

5)zasięga potrzebnych mu opinii i proponuje działania naprawcze oraz minimalizujące skutki.

§ 40. Wszyscy pracownicy ZOZ są zobowiązani udzielić IOD niezbędnej pomocy w realizacji zadań określonych w § 39.

§ 41. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych Osobowych, 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.

§ 42. 1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, jeżeli ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie lub zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

3. Jeżeli zawiadomienie wymagałoby niewspółmiernie dużego wysiłku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

ROZDZIAŁ IX
ZARZĄDZANIE PRZETWARZANIEM DANYCH OSOBOWYCH I ODPOWIEDZIALNOŚCI

§ 43. ADO nie rzadziej niż raz w roku, lub w przypadku istotnej zmiany w zakresie przetwarzania danych, dokonuje oceny skutków dla ochrony danych. Ocena zawiera:

1) opis operacji i celów przetwarzania, w tym, prawnie uzasadnionych interesów realizowanych przez administratora,
2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą.

§ 44. 1. Za czynności w sprawach z zakresu ochrony danych osobowych i ich bezpieczeństwo odpowiada Dyrektor ZOZ w Łowiczu oraz osoby przez niego wskazane:

2. Inspektor Ochrony Danych w zakresie określonym w Regulaminie organizacyjnym ZOZ;

3. Administrator Systemu Informatycznego w zakresie określonym w Regulaminie organizacyjnym ZOZ;

4. Kierownik komórki organizacyjnej w zakresie sprawowania nadzoru nad przetwarzaniem danych w komórce organizacyjnej.

5. Osoba przetwarzająca odpowiada za:

1) zapoznanie się oraz bieżące przestrzeganie przepisów dotyczących ochrony danych osobowych, zasad ustalonych w Polityce ochrony danych oraz Instrukcji zarządzania systemem informatycznym ZOZ w Łowiczu oraz innych aktach wewnętrznych ZOZ,
2) ograniczenie zakresu przetwarzania danych do minimum niezbędnego do realizacji celów przetwarzania na zajmowanym stanowisku pracy,
3) zabezpieczenia w ramach możliwości organizacyjnych i technicznych stanowiska pracy przed naruszeniem bezpieczeństwa przetwarzanych danych,
4) prawidłowość przetwarzanych danych,
5) zachowania w tajemnicy danych osobowych zarówno w okresie zatrudnienia lub współpracy jak również po upływie tego okresu.

§ 45. 1. Dopuszczenie do niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, ujawnienia lub nieuprawnionego dostępu do danych osobowych przetwarzanych w jakiejkolwiek formie, chociażby przypadkowe stanowi ciężkie naruszenie obowiązków pracowniczych.

2. Niepodjęcie działania określonego w niniejszym dokumencie na wypadek niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, ujawnienia lub nieuprawnionego dostępu do danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

Zespół Opieki Zdrowotnej
99-400 Łowicz, ul. Ułańska 28
tel. 46) 837-53-68, fax 46) 837-59-91
e-mail: lowzoz@pro.onet.pl
Regon: 750079660
NIP: 834-14-56-538

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Data nadania upoważnienia**:** ***(data nadania)***

Nr upoważnienia ***(nr)/(rok wydania)***

1. Upoważniam ***(Panią/Pana)***: ***(imię i nazwisko)***

(imię i nazwisko upoważnianego)

(tytuł prawny -zatrudnienie lub inny) na stanowisku ***(określenie stanowiska)***
w Zespole Opieki Zdrowotnej w Łowiczu
(nazwa administratora – pracodawcy)

do przetwarzania danych osobowych:

Zbiór danych osobowych	Komórka organizacyjna	Zakres danych
(określenie zbioru danych osobowych)	***(określenie komórek organizacyjnych)***	***(zakres przetwarzania danych)***

Upoważnienie (*dotyczy również/nie dotyczy)* przetwarzania powyższych danych w systemach informatycznych.
Zakres przetwarzania: ***(czynności przetwarzania)***

Okres trwania upoważnienia: ***(data początkowa obowiązywania)*** **do** ***(data końcowa obowiązywania).***

Jednocześnie zobowiązuję ***(Pana/Panią)*** **do zachowania w tajemnicy informacji uzyskanych podczas przetwarzania danych osobowych oraz sposobów ich zabezpieczania.**
Obowiązek ten istnieje również po ustaniu zatrudnienia.

Podstawa prawna: art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1)

Upoważnienie nadał:

……..

(pieczęć i podpis administratora danych osobowych)

Podpis osoby upoważnionej: …….....

Zespół Opieki Zdrowotnej
99-400 Łowicz, ul. Ułańska 28
tel. 46) 837-53-68, fax 46) 837-59-91
e-mail: lowzoz@pro.onet.pl
Regon: 750079660
NIP: 834-14-56-538

OŚWIADCZENIE

Ja niżej podpisana(-ny) ….....***(imię i nazwisko)***.....
(imię i nazwisko)

(***tytuł prawny- zatrudnienie lub inny)*** jako ***(stanowisko/zawód)*** – w ZOZ w Łowiczu

zobowiązuje się do:

1) zachowania w tajemnicy danych osobowych, w tym danych dotyczących zdrowia, do których będę miał/-a dostęp w związku w wykonywaniem przeze mnie obowiązków na stanowisku pracy w Zespole Opieki Zdrowotnej w Łowiczu, zarówno w czasie zatrudnienia/wykonywania świadczeń jak i po jego/ich zakończeniu.

2) przestrzegać obowiązujących w ZOZ w Łowiczu przepisów związanych z ochroną danych osobowych.

3) zachować na swoim stanowisku szczególną ostrożność podczas przetwarzania danych osobowych oraz powstrzymać od wchodzenia w posiadanie danych wykraczających poza zakres wykonywanych przeze mnie obowiązków.

Oświadczam, że znana mi jest definicja danych osobowych w rozumieniu art. 4 ppkt. 1 oraz definicja szczególnych kategorii danych w rozumieniu art. 9 ust. 1 *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE*
oraz, że zostałem(am) zaznajomiony(a) z przepisami o ochronie tych danych obowiązującymi w Zespole Opieki Zdrowotnej w Łowiczu.

.....
(miejscowość i data)

.....
(czytelny podpis składającego oświadczenie)