POLITYKA BEZPIECZEŃSTWA

w zakresie ochrony danych osobowych

Centrum Zdrowia Panaceum Sp. z o.o.
ul. Sienna 86 lok 129
00-815 Warszawa

Wydanie I z dnia 01.02.2023 r
Ostatnia aktualizacja 01.08.2023

(podpis Administratora)

Spis treści

Podstawowe pojęcia i skróty

1. **Ustawa o ochronie danych osobowych (**zwana dalej UODO**)** – ustawa z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000.)
2. **Rozporządzenie RODO** (zwane dalej RODO) rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, s. 1)
3. **Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta** (zwana dalej URPP) - ustawa z dnia 6 listopada 2008 r. (Dz.U. z 2016 r. poz. 186 z późn. zm.))
4. **Ustawa o systemie informacji w ochronie zdrowia** (zwana dalej UIOZ) - ustawa z dnia 28 kwietnia 2011 (Dz.U. z 2011r. poz. 657 z późn. zm.)
5. **Przepisy o ochronie danych osobowych-** przepisy ustawy o ochronie danych osobowych oraz wszelkie właściwe powiązane lub pochodne regulacje i wytyczne dotyczące przetwarzania danych osobowych
6. **UODO**- Urząd Ochrony Danych Osobowych
7. **Administrator (A)–** (art.4 pkt.7 RODO) oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
8. **Inspektor Ochrony Danych (IOD)** oznacza osobę pełniącą obowiązki na podstawie z art. 37 ust. 1 RODO i w zakresie zgodnym z RODO
9. **Administrator Systemu Informatycznego (ASI)** - podmiot, osoba odpowiedzialna za techniczno- organizacyjną obsługę systemu teleinformatycznego
10. **Dane osobowe** - 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.
11. **Przetwarzanie danych**– operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki 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.
12. **Zbiór danych osobowych**– (art. 4 pkt. 6 RODO) oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
13. **Dokument elektroniczny**- stanowiący odrębną całość znaczeniowa zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisanych na informatycznym nośniku danych.
14. **System teleinformatyczny** – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z 16 lipca 2004 r.– Prawo telekomunikacyjne (Dz. U z 2014 poz. 243).
15. **Środki komunikacji elektronicznej** rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną.

16. **System tradycyjny**– zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji, wyposażenia i środków trwałych w celu przetwarzania danych osobowych w formie papierowej.
17. **Zabezpieczenie danych w systemie teleinformatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mające na celu w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą uszkodzeniem lub zniszczeniem.
18. **Osoba upoważniona do przetwarzania danych osobowych –** osoba, która została upoważniona do przetwarzania danych osobowych przez Administratora na piśmie; dotyczy to zarówno zatrudnionych, świadczących usługi na podstawie umów cywilno-prawnych jak i innych, np. stażystów, wolontariuszy, praktykantów, itp.
19. **Użytkownik systemu teleinformatycznego**– osoba, upoważniona przez Administratora, do przetwarzania danych osobowych w systemie informatycznym, która odbyła stosowne szkolenie z zakresu ochrony tych danych.
20. **Identyfikator użytkownika (login)**– ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
21. **Hasło**– ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
22. **Uwierzytelnian**ie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
23. **Usuwanie danych –** oznacza to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
24. **Integralność danych**– funkcjonalność zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
25. **Integralność systemu** – nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
26. **Poufność danych**– funkcjonalność zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
27. **Rozliczalność**- funkcja zapewniająca, że określone działanie dowolnego podmiotu jest jednoznacznie przypisane temu podmiotowi. **Od 25 maja 2018** oznacza to również zgodność z regulacją RODO
28. **Dostępność informacji** - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, kiedy jest to potrzebne.
29. **Zarządzanie ryzykiem**- proces identyfikowania, kontrolowania, minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.
30. **Podmiot przetwarzający/Procesor**- (art.4 pkt.8 RODO) oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora
31. **Naruszenie ochrony danych osobowych** (art.4 pkt.12 RODO) 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
32. **Zgoda osoby, której dane dotyczą** (art.4 pkt.11 RODO) 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.

Wprowadzenie

1. Niniejsze, wydanie Polityki Bezpieczeństwa jest efektem wdrożenia zasad 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. Urz. UE L 119 z 04.05.2016, s. 1)
2. Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Administratora Centrum Zdrowia Panaceum Sp. z o.o. ul. Sienna 86 lok 129, 00-815 Warszawa zwanym dalej Centrum Zdrowia Panaceum przed zagrożeniami wewnętrznymi i zewnętrznymi.
3. Zapewnienie ochrony danych osobowych w Centrum Zdrowia Panaceum rozumiane jest jako zapewnienie ich poufności, integralności, adekwatności, rozliczalności oraz dostępności na odpowiednim poziomie.
4. W celu zapewnienia bezpieczeństwa przetwarzanych danych osobowych w Centrum Zdrowia Panaceum stosuje się następujące zasady:
   1) Każda osoba uprawniona do przetwarzania danych osobowych posiada dostęp wyłącznie do tych danych, które są jej niezbędne do wykonywania obowiązków służbowych
   2) Każdy osoba uprawniona do przetwarzania danych osobowych i mająca do nich dostęp ma obowiązek zachowania ich w tajemnicy, także po cofnięciu jej uprawnienia
   3) Każda osoba uprawniona do przetwarzania danych osobowych posiada jednoznacznie przypisany zakres indywidualnej odpowiedzialności za przetwarzane dane osobowe
5. Miarą bezpieczeństwa przetwarzanych danych osobowych jest określone postępowanie z ryzykiem zgodnie z podejściem *risk based approach*.
6. Opracowanie Polityki Bezpieczeństwa wynika z przepisów:
   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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, s. 1)
   2) Ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2018 r. poz. 1000.)
   3) Ustawy z dnia 28 kwietnia 2011 o systemie informacji w ochronie zdrowia (Dz.U. z 2011r., poz. 657 z późn. zm.)
7. Dokument Polityka Bezpieczeństwa opisuje procedury zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz postępowanie dla zapobiegania skutkom zagrożeń.
8. Centrum Zdrowia Panaceum ma świadomość znaczenia przetwarzanych danych osobowych, przykłada najwyższą wagę do zapewnienia im odpowiedniego poziomu bezpieczeństwa, ponieważ mają one fundamentalne znaczenia dla realizacji misji i celów statutowych, a ich zgodne z prawem wykorzystanie pozwala na wzmocnienie reputacji.
9. Dane osobowe stanowią kluczowe zasoby informacyjne Centrum Zdrowia Panaceum i zapewnia się im odpowiednią ochronę.
10. Opisane reguły obowiązują wszystkie osoby uprawnione do przetwarzania danych osobowych oraz podmioty współpracujące na podstawie umowy cywilnoprawnej, które mają jakikolwiek kontakt z danymi osobowymi objętymi ochroną.
11. Administrator podejmuje decyzję o powoływaniu lub odwoływaniu Inspektora Ochrony Danych na podstawie:
    1) Wyniku przeprowadzonej analizy zgodności zasad powołania IOD z RODO oraz wytycznych Grupy Roboczej Art. 29 (w załączniku do Polityki Bezpieczeństwa)
    2) Oszacowania ryzyka naruszenia praw i wolności osób fizycznych, których dane są przetwarzane i zgodnie z procedurą zarządzania ryzykiem
12. Administrator, w przypadku niepowołania IOD, w trybie ciągłym monitoruje poziom ryzyka naruszenie praw i wolności osób fizycznych, których dane są przetwarzane oraz utraty zgodności w tym zakresie z RODO i w zależności od wyników podejmuje określone działania korekcyjne korygujące oraz zachowawcze

13. W przypadku niepowołania Inspektora Ochrony Danych Administrator odpowiada w pełnym zakresie za realizację wykonywanych na tym stanowisku czynności.

Zadania Administratora

1. Administrator stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. Zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem
2. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
3. W zakresie zadań realizowanych w pkt 1 Administrator:
   1) Prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki organizacyjne i techniczne zabezpieczające dane osobowe;
   2) Nadaje upoważnienia do przetwarzania danych i dopuszcza do pracy wyłącznie osoby posiadające takie upoważnienie;
   3) Zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane;
   4) Prowadzi ewidencję osób upoważnionych do ich przetwarzania, która zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych, a także identyfikator, jeżeli dane są przetwarzane w systemie informatycznym;
   5) Nadaje i odwołuje upoważnienia do przetwarzania danych osobowych oraz prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych;
   6) Podejmuje decyzję o powołaniu lub odwołaniu IOD na podstawie:
      a) analizy ryzyka braku zgodności z RODO
      b) analizy ryzyka naruszenia praw i wolności osób fizycznych, których dane przetwarza;
   7) Czuwa nad stosowaniem i przestrzeganiem przepisów ustawy oraz nadzoruje pracę dodatkowych osób odpowiedzialnych za bezpieczeństwo przetwarzanych danych osobowych;
   8) Jeżeli dany rodzaj przetwarzania– w szczególności z użyciem nowych technologii– ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw wolności osób fizycznych, Administrator, przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych *data protection impact assessment;*
   9) Zgłasza naruszenia ochrony danych osobowych organowi nadzorczemu oraz informuje o tym osobę, którą to naruszenie dotyczy, w formie i trybie zgodnym z regulacją RODO;
   10) Zarządza ryzykiem ochrony danych osobowych, zgodnie z podejściem *risk based approach* i dokumentuje proces;
   11) Prowadzi rejestr czynności przetwarzania.

Zadania Inspektora Ochrony Danych (IOD)

1. Inspektor ochrony danych ma następujące zadania
   1) informowanie Administratora, podmiotu przetwarzającego oraz osób, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   2) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie

ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia osób uczestniczących w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4) współpracę z organem nadzorczym;
5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania danych, mając na uwadze charakter, zakres, kontekst i cele przetwarzania danych.

Rejestrowanie czynności przetwarzania danych osobowych

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych, za który odpowiada.
2. Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora.
3. Zakres informacji zawartych w powyższych rejestrach określony jest w art. 30 rozporządzenia RODO.
4. Rejestr czynności przetwarzania zawarty jest w załączniku do Polityki Ochrony Danych.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Centrum Zdrowia Panaceum stosuje odpowiednie środki informatyczne, techniczne, organizacyjne zapewniające ochronę przetwarzanych danych osobowych, które są odpowiednie do stopnia zagrożeń oraz kategorii danych objętych ochroną.
   Centrum Zdrowia Panaceum zabezpiecza dane osobowe przed:
   1) Udostępnieniem ich osobom nieupoważnionym,
   2) Zabraniem przez osobę nieuprawnioną,
   3) Utratą dostępu do danych,
   4) Przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem.
2. Do zastosowanych środków technicznych należy:
   1) Przetwarzanie danych osobowych w wydzielonych, odpowiednio zabezpieczonych i przystosowanych do tego pomieszczeniach lub częściach pomieszczeń;
   2) Zabezpieczenie wejść do pomieszczeń, o których mowa w pkt 1;
   3) Wyposażenie pomieszczeń w szafki, zamykane na klucz, dające gwarancję bezpieczeństwa dokumentacji i nośników danych;
   4) Przechowywanie dokumentacji bieżącej i archiwalnej w obszarach przetwarzania danych osobowych w szafach zamykanych na zamki.
3. Dodatkowe zabezpieczenia techniczne obszarów przetwarzania danych osobowych zawarte są w załączniku do Polityki Bezpieczeństwa
4. Do zastosowanych przez Administratora środków organizacyjnych służących zapewnieniu poufności, dostępności, integralności i rozliczalności przy przetwarzaniu danych osobowych należą:
   1) Opracowanie i wdrożenie Polityki Bezpieczeństwa,
   2) Opracowanie i wdrożenie Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych,
   3) Zapoznanie każdej osoby, przed jej przystąpieniem do pracy przy przetwarzaniu danych osobowych, z przepisami dotyczącymi ochrony danych osobowych;
   4) Prowadzenie rejestru czynności przetwarzania danych osobowych
   5) Prowadzenie dokumentacji zarządzania ryzykiem (szacowanie, postępowanie i monitorowanie ryzyka).
   6) Prowadzenie rejestru incydentów oraz zgłoszeń incydentów bezpieczeństwa.

7) Regularne szkolenia osób przetwarzających dane osobowe w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych. IOD lub inna powołana osoba organizuje szkolenia z ochrony danych osobowych oraz aktualnych aktów wykonawczych.
8) Okresowe szkolenia każdej osoby, uprawnionej do przetwarzania danych osobowych, z zakresu obowiązujących standardów ochrony danych osobowych i aktualnych przepisów wykonawczych. Administrator prowadzi w tym celu rejestr zawarty w załączniku do Polityki Bezpieczeństwa.
9) Podpisanie przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i zrozumieniu treści szkolenia oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
10) Okresowe sprawdzanie, zgodnie z podejściem opartym na analizie ryzyka, w razie konieczności, lecz nie rzadziej niż raz w roku i przynajmniej raz na 5 lat wszystkich zabezpieczeń zbiorów danych w tym systemów informatycznych służących do ich przetwarzania.
11) Kontrolowanie otwierania i zamykania pomieszczeń, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę i niepozostawianiu pomieszczenia w czasie pracy bez nadzoru. Osobami upoważnionymi do przetwarzania danych osobowych są osoby wyszczególnione w załączniku stanowiącym integralną część Polityki Bezpieczeństwa.
12) Odbieranie pisemnego oświadczenia każdej osoby upoważnionej do przetwarzania danych osobowych, przed przystąpieniem do pracy, że została zaznajomiona z przepisami ustawy UODO i regulacją RODO, aktami wykonawczymi oraz że rozumie zasady dotyczące ochrony danych osobowych opisane w Polityce Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym i zobowiązuje się do ich przestrzegania.
13) Zapewnienie przestrzegania wszelkich wewnętrznych regulaminów i instrukcji dotyczących bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualnych zakresów zadań osób zatrudnionych przy przetwarzaniu danych osobowych, w tym dokumentów zawartych w niniejszej Polityce Bezpieczeństwa.

Powierzenie, udostępnienie przetwarzania danych osobowych

Zasady powierzania danych

1. Centrum Zdrowia Panaceum na podstawie umów zawartych w formie pisemnej, powierza podmiotom zewnętrznym przetwarzanie danych osobowych w zakresie objętym umową.
2. Zgodnie z umowami podmioty zewnętrzne zobowiązują się przetwarzać powierzone im dane osobowe zgodnie z ustawą UODO, rozporządzeniem RODO, ustawą URPP, rozporządzeniami wykonawczymi oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Wykaz podmiotów zewnętrznych przetwarzających dane osobowe znajduje się załączniku do Polityki Bezpieczeństwa.

Zasady udostępniania danych

1. Dane osobowe przetwarzane zgodnie z regulacją RODO, a także na podstawie art. 25 ustawy URPP, mogą być wydane na pisemny wniosek osoby, której dotyczą lub pisemny wniosek osoby upoważnionej na piśmie przez zainteresowanego; o ile inne przepisy prawa nie stanowią inaczej
2. Dopuszcza się przekazywanie danych osobowych, mających odniesienie do regulacji RODO, podmiotom i organom upoważnionym na podstawie odrębnych przepisów.
3. Elektroniczna dokumentacja medyczna, o której mowa w art. 2 pkt 6 ustawy UIOZ i URPP jest udostępniana na zasadach określonych w przepisach tych ustaw
4. Wzór wniosku o udostępnienie danych osobowych zawarty jest w załączniku do Polityki Bezpieczeństwa
5. Ewidencja wniosków zawarta jest w załączniku do Polityki Bezpieczeństwa;
6. Z czynności przekazania danych sporządza się protokół przekazania, którego wzór stanowi załącznik do Polityki Bezpieczeństwa
7. Administrator prowadzi zestawienie przekazywanych danych osobowych zgodnie z załącznikiem do Polityki Bezpieczeństwa.

8. Dokumentacja medyczna jest udostępniana zgodnie z art. 26 oraz 27.1 Ustawy z dnia 6 listopada 2008 o Prawach Pacjenta i Rzeczniku Praw Pacjenta (tekst jedn.: Dz.U. z 2017 r. poz. 1318 ze zm.)

Opis zdarzeń naruszających ochronę danych osobowych

1. Podział zagrożeń:
   1) Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona, lecz nie dochodzi do naruszenia poufności danych;
   2) Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, Administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych;
   3) Zagrożenia zamierzone, świadome i celowe- najpoważniejsze zagrożenia, gdzie występują naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.
2. Naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to głównie:
   1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
   2) Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
   3) Awaria sprzętu lub oprogramowania, w wyniku umyślnego działania;
   4) Pojawienie się komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
   5) Pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
   6) Naruszenie lub próba naruszenia integralności systemu lub bazy danych w systemie;
   7) Próba modyfikacji lub modyfikacja danych bez odpowiedniego upoważnienia (autoryzacji);
   8) Ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
   9) Nieautoryzowane konta dostępu do danych;
   10) Podmiana, niszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia
   11) Kasowanie lub kopiowanie w sposób niedozwolony danych osobowych
   12) Nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych;
   13) Kradzież nośników, na których zapisane są dane osobowe;
   14) Rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp.);
   15) Nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej

Instrukcja postępowania w przypadku zdarzeń naruszających ochronę danych osobowych

1. Każda osoba uprawniona do przetwarzania danych osobowych, w przypadku podejrzenia naruszenia lub faktu naruszenia zasad ochrony danych osobowych, ma obowiązek do natychmiastowego powiadomienia bezpośredniego przełożonego o zaistniałej sytuacji.
2. Zgłoszenie jest przekazywane bezpośrednio przez osobę upoważnioną, która stwierdziła podatność na zagrożenie lub powstały incydent.
3. Informacja jest przekazywana przez osobę upoważnioną w zależności od pory i sytuacji zgodnie ze szczegółową wewnętrzną procedurą. Droga przekazania informacji zależy przede wszystkim od subiektywnej oceny rangi sytuacji przez osobę uprawnioną i decyzji jaką podejmie.
4. Po otrzymaniu powiadomienia należy niezwłocznie:
   1) Sprawdzić stan urządzeń wykorzystywanych do przetwarzania danych osobowych;
   2) Sprawdzić sposób działania programów (w tym obecność wirusów komputerowych);
   3) Sprawdzić jakość komunikacji w sieci telekomunikacyjnej;
   4) Sprawdzić zawartość zbioru danych osobowych;
   5) Przeanalizować metody pracy osób uprawnionych do przetwarzania danych osobowych.
5. W przypadku zaistnienia incydentu Administrator wdraża postępowanie zgodnie z procedurą oceny skutków ochrony danych DPIA *Data Protection Impact Assesment*
6. Działania, w przypadku stwierdzenia incydentu, polegają w szczególności na:
   1) Uniemożliwieniu dalszego naruszenia bezpieczeństwa przetwarzanych danych osobowych (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.);
   2) Powstrzymaniu lub ograniczeniu dostępu do danych osoby niepowołanej poprzez: fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej, wylogowanie użytkownika podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła na konto Administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania;
   3) Zabezpieczeniu i utrwala wszelkich informacji i dokumentów mogących stanowić pomoc przy ustaleniu przyczyn naruszenia;
   4) Niezwłocznym przywróceniu prawidłowego stanu działania systemu;
   5) Dokonaniu analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia;
   6) Wydrukowaniu na bieżąco wszystkich możliwych dokumentów i raportów, które mogą pomóc w ustaleniu okoliczności zdarzenia;
   7) Sporządzenia szczegółowego raportu zawierającego w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzeń (w załączniku do Polityki Bezpieczeństwa).
7. Postępowanie w przypadku zaistnienia incydentu obejmuje następujące działania:
   1. Działanie korekcyjne– działanie w celu wyeliminowania skutków powstałego incydentu/ zdarzenia,
   2. Działanie korygujące– działanie w celu wyeliminowania przyczyny zdarzenia incydentu,
   3. Działanie zapobiegawcze– działanie, które należy przedsięwziąć, aby w przyszłości ograniczyć lub wyeliminować przyczyny zaistniałego zdarzenia/ incydentu.
8. Postępowanie z zaistniałym lub potencjalnie istniejącym incydentem wywołanym przez określone zagrożenia, odbywa się zgodnie z podejściem *risk based approach* opisane w procedurze zarządzania ryzykiem (w załączniku do Polityki Bezpieczeństwa).
9. Rejestr incydentów znajduje się w załączniku do Polityki Bezpieczeństwa.
10. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii– ze względu na swój charakter, zakres, kontekst i cele- z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator **przed rozpoczęciem przetwarzania** dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

11. W przypadku, kiedy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
12. Przez naruszenie praw lub wolności osoby fizycznej rozumie się:
    1. Powstanie uszczerbku fizycznego, szkód majątkowych lub niemajątkowych takich jak utrata kontroli nad własnymi danymi osobowymi,
    2. Ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości,
    3. Stratę finansową, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia,
    4. Naruszenie poufności danych osobowych chronionych tajemnicą zawodową,
    5. Wszelkie inne znaczne szkody gospodarcze lub społeczne.
13. Administrator systemów informatycznych prowadzi dziennik zdarzeń/ incydentów (załącznik do Polityki Bezpieczeństwa.

Postanowienia końcowe

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków służbowych, w szczególności przez osobę, która po stwierdzeniu naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie bezpośredniego przełożonego i zgodnie z wewnętrzną procedurą.
2. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także kiedy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie.
3. Orzeczona kara wobec osoby uchylającej się od powiadomienia j.w. nie wyklucza odpowiedzialności karnej oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego o zrekompensowanie poniesionych strat.
4. Wdrożenie Polityki Bezpieczeństwa oraz działania korygujące i zachowawcze odbywają się poprzez:
   1) Zapoznanie osób uprawnionych do przetwarzania danych osobowych z treścią Polityki Bezpieczeństwa;
   2) Okresowe szkolenia z zakresu ochrony danych osobowych.

5. Polityka Bezpieczeństwa wchodzi w życie z dniem podpisania jej przez Administratora.