załącznik nr 1 do uchwały nr 30/2019
Zarządu Poddębickiego Centrum Zdrowia Sp. z o.o.
z dnia 22 lutego 2019 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

w Poddębickim Centrum Zdrowia Sp. z o.o.

Poddębice, 22 lutego 2019 r.

Wiceprezes Zarządu
lek. med. Urszula Marjańska

opracował Inspektor Ochrony Danych

DOKUMENT DO UŻYTKU WEWNĘTRZNEGO

Spis treści

Rozdział I.

Definicje

pojęcie	znaczenie
1.	*2.*
adekwatność lub minimalizacja danych	zasada dotycząca przetwarzania danych osobowych polegająca na tym, że administrator powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne do realizacji celu dla którego dane są zbierane
Administrator	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych - w niniejszej dokumentacji ochrony danych osobowych przez administratora rozumie się Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach
analiza ryzyka	proces identyfikacji ryzyka, określania jego wartości i identyfikowanie niezbędnych zabezpieczeń
anonimizacja	przekształcenie danych osobowych, po którym nie można już przyporządkować poszczególnych informacji osobistych lub rzeczowych do określonej lub możliwej do zidentyfikowania osoby fizycznej albo można tego dokonać jedynie niewspółmiernie dużym nakładem czasu, kosztów lub działań
audyt zgodności	czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami RODO oraz innymi przepisami o ochronie danych osobowych, a także czynności mające na celu monitorowanie przestrzegania polityki ochrony danych osobowych
dane biometryczne	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
dane dotyczące zdrowia	dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia
dane genetyczne	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

pojęcie	znaczenie
1.	*2.*
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
docelowy poziom ryzyka	docelowy poziom pojedynczego ryzyka, jaki administrator zamierza osiągnąć w odniesieniu do konkretnego ryzyka
dostępność	właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu
działania zaradcze	środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia
hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym
identyfikator	ciąg znaków literowych, cyfrowych lub innych znaków identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym
incydent	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
integralność	zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób
IOD	osoba pełniąca funkcję inspektora ochrony danych w rozumieniu art. 37 RODO
istotność ryzyka	iloczyn prawdopodobieństwa i wpływu ryzyka określający potencjalny skumulowany poziom wpływu ryzyka na osiąganie przez administratora zamierzonych celów

pojęcie	znaczenie
1.	*2.*
legalność	zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane zgodnie z prawem, po spełnieniu przynajmniej jednego z warunków określonych w art. 6. ust. 1. lub art. 9. ust. 2. RODO
mapa ryzyka	graficzne zestawienie ryzyka z punktu widzenia jego istotności, lub innych kryteriów
ocena ryzyka	proces porównywania ryzyka z założonymi kryteriami ryzyka w celu wyznaczenia wagi ryzyka
odbiorca	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, jednak odbiorcą nie jest organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państw członkowskiego
ograniczenie celu	zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami
okresowość	zasada dotycząca przetwarzania danych osobowych zapewniająca, że dane osobowe są przetwarzane przez okres nie dłuższy, niż jest to niezbędne do celów, dla realizacji których dane są przetwarzane
organ nadzorczy	niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych w Unii Europejskiej, zgodnie z art. 51 RODO
osoba upoważniona	osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę
PCZ lub Spółka PCZ	Poddębickie Centrum Zdrowia Sp. z o. o. z siedzibą w Poddębicach, adres: ul. Mickiewicza 16. (99-200) Poddębice
podmiot przetwarzający/procesor	osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarzana dane osobowe w imieniu administratora
Polityka	niniejszy dokument, tj. Polityka Ochrony Danych Osobowych

pojęcie	znaczenie
1.	*2.*
poufność	właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
pracownik	osoba zatrudniona przez PCZ na podstawie umowy o pracę oraz osoba świadcząca na rzecz PCZ usługi na podstawie umów cywilno -prawnych, a także praktykanci, wolontariusze, stażyści i studenci
prawdopodobieństwo	oczekiwana częstość materializacji danego ryzyka
przetwarzanie	operacja 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
pseudonimizacja	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
raport zgodności	dokument opracowywany przez IOD po dokonaniu audytu zgodności zawierający opis niezgodności przetwarzania danych osobowych z przepisami RODO, innymi przepisami o ochronie danych osobowych oraz Polityką, a także zawierający ogólną ocenę poziomu ochrony danych osobowych
rejestr czynności przetwarzania danych osobowych	dokument, o którym mowa w art. 30. ust. 1. RODO, prowadzony w formie pisemnej przez Administratora, udostępniany organowi nadzorczemu na jego żądanie
rejestr wszystkich kategorii czynności przetwarzania	dokument, o którym mowa w art. 30. ust. 2. RODO, prowadzony w formie pisemnej przez podmiot przetwarzając, udostępniany organowi nadzorczemu na jego żądanie
RODO	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)

pojęcie	znaczenie
1.	*2.*
rola	grupa uprawnień przypisanych do stanowiska pracy np.: administracja, lekarz, pielęgniarka, ratownik medyczny, rehabilitant, technik obrazowy, rozliczenia, kadry, płace, księgowość
rozliczalność przetwarzania	właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi
ryzyko	kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji - ryzyko związane z bezpieczeństwem danych osobowych to prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów
rzetelność	zasada dotycząca przetwarzania danych osobowych zapewniająca merytoryczną poprawność danych osobowych poprzez ich zgodność ze stanem faktycznym, kompletność i aktualność
skutek	efekt materializacji ryzyka
strona trzecia lub osoba trzecia	osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe
system informatyczny	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych
szacowanie ryzyka	całościowy proces analizy i oceny ryzyka
właściciel ryzyka	osoba, która ze względu na zajmowane stanowisko i przydział odpowiedzialności zarządza głównymi czynnikami ryzyka, przypisanego do niej - właścicielami ryzyka mogą być prezesi, dyrektorzy, kierownicy, samodzielne stanowiska lub pełnomocnicy odpowiadający za zarządzane przez nich procesy przetwarzania danych osobowych
wpływ	potencjalne skutki materializacji ryzyka
upoważnienie	uprawnienie nadane przez administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w upoważnieniu, nad którym administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę
uwierzytelnianie	działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby upoważnionej

pojęcie	znaczenie
1.	*2.*
zabezpieczenie	środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną
zagrożenie	niepożądane zdarzenie, które powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie danych osobowych na utratę, ujawnienie, zniszczenie lub zmianę
zarządzanie ryzykiem	skoordynowane działania w celu identyfikacji, minimalizacji lub eliminacji prawdopodobieństwa oraz skutków realizacji zagrożeń
zbiór danych	uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie

Rozdział II.

Wstęp

Niniejsza Polityka służy realizacji obowiązków wynikających z powszechnie obowiązującego prawa, w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Administrator wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO. Aby móc to wykazać Administrator wdraża niniejszą Politykę.

Proces przetwarzania odbywa się w sposób zapewniający należytą ochronę danych osobowych, będących w zasobach Administratora i jemu powierzonych, gdy przetwarzanie obywa się z zachowaniem następujących zasad:

- zgodności z prawem,
- rzetelności, przejrzystości i ograniczoności celu,
- adekwatności, prawidłowości i okresowości przetwarzanych danych,
- poufności, integralności i rozliczalności danych.

Polityka jest aktualizowana gdy zachodzą zmiany przepisów prawa w zakresie ochrony danych osobowych lub w związku ze zmianą stanu faktycznego, co ma wpływ na treść dokumentu.

Zakres podmiotowy stosowania niniejszej Polityki obejmuje wszystkich pracowników lub współpracowników przetwarzających dane osobowe.

Żadna procedura ani regulacja wewnętrzna obowiązująca u Administratora nie może naruszać zasad określonych w niniejszej Polityce.

Administrator, zgodnie z treścią art. 37. ust. 1. lit. b) RODO, wyznaczył IOD, który wykonując zadania zgodnie z art. 39. RODO, podlega bezpośrednio Prezesowi PCZ.

Dane osobowe chronione niniejszą Polityką przetwarzane są w siedzibie Administratora mieszczącej się przy ul. Mickiewicza nr 16. (99-200) w Poddębicach i/lub w siedzibie procesora.

Rozdział III.

Określenie obowiązków Administratora, IOD, Działu ds. Informatyzacji i Baz Danych, osoby upoważnionej

Administrator powinien:

- zapewnić niezbędne środki do stworzenia i funkcjonowania systemu ochrony danych osobowych,
- wdrożyć niezbędne środki organizacyjne i techniczne zapewniające rozliczalność, integralność oraz poufność przetwarzanych danych osobowych,
- zapewnić, by systemy informatyczne wykorzystywane do przetwarzania danych spełniały odpowiednie środki techniczne zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których dane osobowe są przetwarzane,
- wdrożyć odpowiednie środki organizacyjne zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych,
- zapewnić, by osoby dopuszczone do przetwarzania danych osobowych przestrzegały przepisów o ochronie danych osobowych,
- zapewnić, by dostęp do danych osobowych miały wyłącznie osoby upoważnione do ich przetwarzania,
- podejmować odpowiednie środki, by w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13. i 14. RODO, oraz prowadzić z nią wszelką komunikację na mocy art. 15. - 22. i 34. RODO w sprawie przetwarzania,

- zapewnić, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
- zapewnić, by IOD nie otrzymywał instrukcji dotyczących wykonywania przez niego zadań,
- zatwierdzić Politykę oraz dokumenty opracowane na jej podstawie oraz na podstawie przepisów obowiązujących w zakresie ochrony danych osobowych.

Inspektor Ochrony Danych powinien:

- informować Administratora oraz pracowników (w drodze odpowiednich poleceń Administratora), którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych osobowych a także doradzać im w tym zakresie,
- monitorować przestrzeganie przepisów o ochronie danych osobowych oraz niniejszej Polityki poprzez, między innymi, przeprowadzane audyty zgodności,
- opracowywać, po każdorazowym przeprowadzeniu audytu zgodności, raport dla Administratora,
- nadzorować wdrażanie zaleceń będących wynikiem audytu zgodności oraz analizy ryzyka,
- podejmować działania pogłębiające wiedzę Administratora i pracowników z zakresu ochrony danych osobowych, w tym informować o zagrożeniach związanych z dostępem do danych osobowych,
- okresowo szkolić personel uczestniczący w operacjach przetwarzania,
- na żądanie Administratora udzielać zaleceń co do oceny skutków dla ochrony danych oraz monitorować ich wykonania, zgodnie z art. 35. RODO,
- współpracować z organem nadzorczym,
- pełnić rolę punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem,
- pełnić rolę punktu kontaktowego dla osób, których dane osobowe dotyczą,
- reagować na zgłaszane incydenty związane z naruszeniem ochrony danych osobowych, analizować ich przyczyny oraz kierować do Administratora wnioski dotyczące usprawnienia ochrony danych osobowych i wyciągania konsekwencji wobec osób winnych naruszeń,
- aktualizować zapisy Polityki,
- prowadzić wykaz podmiotów przetwarzających dane/procesorów,
- prowadzić rejestr czynności przetwarzania danych osobowych,
- prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu podmiotu powierzającego.

Dział ds. Informatyzacji i Baz Danych powinien:

- nadzorować stosowane środki techniczne i organizacyjne zapewniające ochronę danych osobowych przetwarzanych w systemach informatycznych,
- utrzymać bieżące funkcjonowanie systemów informatycznych służących do przetwarzania danych osobowych, zapewniając poufność, integralność i dostępność, m.in. poprzez właściwą aktualizację tych systemów,
- zarządzać systemem komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji w sposób zapewniający bezpieczeństwo wymiany danych,
- nadzorować funkcjonowanie mechanizmów uwierzytelniania użytkowników w systemie informatycznym oraz kontrolę dostępu do danych osobowych,
- wykonywać kopie bezpieczeństwa elektronicznych zbiorów danych osobowych,
- okresowo sprawdzać kopie bezpieczeństwa pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
- prowadzić depozyt kopii bezpieczeństwa i logów danych,
- przydzielać użytkownikom indywidualnych identyfikatorów i haseł do systemu informatycznego oraz dokonywać ewentualnych modyfikacji uprawnień, a także usuwać konta użytkowników, gdy zajdzie taka konieczność,
- okresowo zmieniać hasła dostępu użytkowników do systemów informatycznych w przypadkach, gdy systemy te nie wymuszają okresowej zmiany haseł użytkowników,
- bieżąco prowadzić ewidencję wszystkich użytkowników systemów informatycznych służących do przetwarzania danych osobowych,
- osobiście wykonywać lub sprawować nadzor na wykonaniem napraw, konserwacji oraz likwidacji urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane osobowe,
- uczestniczyć w procesie zakupu aplikacji oraz oprogramowania zatwierdzonego do włączenia do sytemu informatycznego służącego do przetwarzania danych osobowych,
- zapewnić legalności oprogramowania wykorzystywanego w systemie informatycznym służącym do przetwarzania danych osobowych oraz zarządzać licencjami do odpowiednich elementów systemu informatycznego,
- zapewnić właściwą konfigurację systemów zarządzania hasłami,
- przeprowadzać okresową inwentaryzację sprzętu komputerowego oraz systemów informatycznych,

- bieżąco inwentaryzować przepływy danych osobowych pomiędzy systemami służącymi do przetwarzania danych osobowych,
- prowadzić, przy współpracy z IOD, postępowania wyjaśniające w sytuacji wystąpienia naruszenia ochrony danych osobowych.

Osoba upoważniona powinna:

- przestrzegać obowiązujących u Administratora zasad ochrony danych osobowych ze szczególnym uwzględnieniem zasad bezpieczeństwa,
- informować bezpośredniego przełożonego lub Głównego Specjalistę ds. Informatyzacji i Baz Danych lub IOD o incydentach godzących w bezpieczeństwo danych osobowych,
- dochowywać szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane są przetwarzane,
- zachować w poufności przetwarzane dane osobowe oraz sposobów ich zabezpieczania,
- zmieniać hasła dostępowe do systemu informatycznego, w którym przetwarzane są dane osobowe, nie rzadziej niż co 90 dni,
- usuwać dane osobowe, które Administrator pozyskuje lub są na rzecz Administratora przekazywane, zawsze wtedy, gdy Administrator nie posiada ani interesu prawnego, ani faktycznego w ich przetwarzaniu (w tym archiwizowaniu) - w razie wątpliwości, co do obowiązku usunięcia danych osobowych osoba upoważniona powinna zwrócić się o opinię do Administratora lub IOD,
- dla ochrony danych, wykonywać adekwatne czynności zabezpieczające do zastosowanych u Administratora rozwiązań technicznych i organizacyjnych, w szczególności, zabezpieczać komputery i wszelkie nośniki danych.

Rozdział IV.

Odpowiedzialność Administratora, podmiotu przetwarzającego, osoby upoważnionej

Administrator za naruszenie ochrony danych osobowych może ponieść odpowiedzialność cywilną zgodnie z art. 82. RODO lub odpowiedzialność administracyjną na podstawie wskazanej w art. 83. lub 84. RODO.

Podmiot przetwarzający za naruszenie ochrony danych osobowych może ponieść odpowiedzialność cywilną zgodnie z art. 82. RODO lub odpowiedzialność administracyjną na podstawie wskazanej w art. 83. i 84. RODO.

Osoba upoważniona za naruszenie ochrony danych osobowych może ponieść odpowiednio odpowiedzialność wskazaną w Kodeksie Pracy albo odpowiedzialność kontraktową przewidzianą

w Kodeksie Cywilnym. Osoba upoważniona może także ponieść odpowiedzialność karną przewidzianą w Kodeksie Karnym.

Nieuzasadnione zaniechanie obowiązków wynikających z niniejszej Polityki potraktowane będzie jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku wykrycia incydentu lub uzasadnionego podejrzenia powstania incydentu nie podjęła działań określonych w niniejszej Polityce, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie udokumentowała takiego przypadku, może zostać wszczęte postępowanie dyscyplinarne.

Kara dyscyplinarna nałożona na osobę uchylającą się od powiadomienia, o którym mowa powyżej, nie wyklucza jej odpowiedzialności karnej oraz nie stanowi przeszkody prawnej dla kierowania wobec niej roszczeń cywilnych przez Administratora o zrekompensowanie poniesionych strat.

Rozdział V.

Zapewnienie poufności, integralności oraz rozliczalności danych osobowych

Administrator zapewnia poufność, integralność oraz rozliczalność przetwarzanych danych osobowych, poprzez zastosowanie niezbędnych środków organizacyjnych oraz technicznych.

Dobór powyższych środków ma na celu obniżenie poziom ryzyka wystąpienia incydentów, związanych z naruszeniem bezpieczeństwa przetwarzania danych osobowych, do poziomu akceptowalnego przez Administratora.

Wprowadzenie omawianych środków, zostało poprzedzone przeprowadzeniem analizy kosztów ich wdrożenia w odniesieniu do stopnia bezpieczeństwa przetwarzania danych osobowych, jaki Administrator zamierza osiągnąć po ich wdrożeniu.

W ramach grupy środków organizacyjnych wprowadzono, w szczególności:

- monitorowanie przestrzegania niniejszej Polityki przez IOD,
- nadzór środowiska informatycznego sprawowany przez Głównego Specjalistę ds. Informatyzacji i Baz Danych,
- pisemne upoważnienia do przetwarzania danych osobowych, które są wydawane każdemu pracownikowi zgodnie z jego zakresem obowiązków,
- prowadzenie ewidencji wydanych upoważnień do przetwarzania danych osobowych,
- składanie przez osoby upoważnione do przetwarzania danych osobowych pisemnych oświadczeń o zachowaniu tych danych w poufności,
- szkolenie osób upoważnionych z zasad bezpiecznego przetwarzania danych osobowych,

- zawierane z procesorami umów powierzenia, w rozumieniu art. 28. ust. 3. RODO,
- ewidencjonowanie umów powierzenia,
- prowadzenie rejestru czynności przetwarzania danych osobowych, zgodnie z art. 30. RODO,
- przypisanie odpowiedzialność pracownikom i procesorom za działania związane z naruszeniem bezpieczeństwa przetwarzania danych osobowych.
- wprowadzenie zasady, zgodnie z którą osoby trzecie przebywają w obszarze przetwarzania danych wyłącznie w obecności osoby upoważnionej,
- wprowadzenie zasady zgodnie. z którą w wyjątkowych okolicznościach, w obszarze przetwarzania danych osoby trzecie mogą przebywać bez obecności osoby upoważnionej tylko po uprzednim wydaniu na to zgody przez Administratora.

Grupa środków zabezpieczenia technicznego i informatycznego zapewniająca poufność przetwarzanych danych osobowych:

- obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych, poprzez zastosowanie zamków patentowych,
- dane osobowe przechowywane w formie papierowej są przechowywane w zamykanych na klucz szafkach, szafach lub szufladach,
- dostęp do danych w systemie informatycznym jest możliwy wyłącznie po udanym uwierzytelnieniu użytkownika,
- hasła składają się z minimum ośmiu znaków (małe, wielkie litery, przynajmniej jedna cyfra lub znak specjalny),
- hasła są zmieniane nie rzadziej niż co 90 dni,
- na stacjach roboczych, za pomocą których są przetwarzane dane osobowe, zainstalowano oprogramowanie antywirusowe automatycznie ściągające najnowsze sygnatury wirusów,
- zapewniono monitorowanie działania systemu informatycznego,
- zapewniono logiczną i fizyczną separację sieci,
- zapewniono ochronę systemów informatycznych przed nieuprawnionym dostępem także z zewnątrz - logiczny dostęp do danych osobowych z sieci publicznej ograniczony jest poprzez zastosowanie zapory ogniowej (firewall).

Grupa środków zabezpieczenia technicznego zapewniająca integralność przetwarzanych danych osobowych:

- organizacyjna i informatyczna ochrona przed nieautoryzowanym dostępem,
- zainstalowane oprogramowania antywirusowe automatycznie ściągającego najnowsze sygnatury wirusów na stacjach roboczych, za pomocą których są przetwarzane dane osobowe,

- zapewnienie awaryjnego podtrzymywanie zasilania serwerów oraz stacji roboczych za pomocą UPS,
- właściwe okablowanie sieci,
- cykliczna weryfikacja integralności baz danych poprzez odtwarzanie danych zawartych na kopiach zapasowych.

Grupa środków zabezpieczenia technicznego zapewniająca rozliczalność przetwarzanych danych osobowych:

- dostępu do danych w systemie informatycznym możliwy jest wyłącznie po udanym uwierzytelnieniu użytkownika,
- zapis zdarzeń w systemach informatycznych.

Przetwarzanie danych osobowych poza obszarem przetwarzania dopuszczalne jest wyłącznie po spełnieniu poniższych przesłanek:

- uzyskanie pisemnej zgody Administratora na przetwarzanie danych osobowych poza obszarem przetwarzania ustalonym niniejszą Polityką,
- zachowanie szczególnej ostrożności podczas transportu, przechowywania i użytkowania nośników zawierających dane osobowe,
- stosowanie środków ochrony kryptograficznej wobec przetwarzanych danych,
- przestrzegania zakazu pozostawiania nośników zawierających dane osobowe w miejscach powszechnie dostępnych,
- wykorzystywanie nośników wyłącznie w celach służbowych.

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- likwidacji - przed likwidacją pozbawia się je z zapisu danych osobowych, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający odczytanie danych osobowych,
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych - przed przekazaniem pozbawia się je z zapisu danych osobowych, w sposób uniemożliwiający ich odzyskanie,
- naprawy - przed przekazaniem do naprawy pozbawia się je z zapisu danych osobowych, w sposób umożliwiający ich odzyskanie.

Rozdział VI.

Zapewnienie realizacji praw i wolności osób, których dane osobowe dotyczą

Administrator ma świadomość, że zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator zapewniając realizację praw i wolności osób, których dane dotyczą, podjął odpowiednie, środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13. i 14. RODO oraz by w sprawie przetwarzania jej danych osobowych prowadzić z nią wszelką komunikację na mocy art. 15.-22. i 34. RODO.

Realizacji praw i wolności osób, których dane dotyczą zapewniają obowiązujące u Administratora następujące zasady:

- informacji udziela się na piśmie lub w sposób żądany przez wnoszącego o jej udzielenie, w tym telefonicznie i drogą poczty elektronicznej,
- gdy osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, ustalając uprzednio tożsamość osoby żądającej,
- informacji udziela się niezwłocznie, nie później niż w ciągu miesiąca od otrzymania żądania jej udzielenia,
- osobie, której dane dotyczą, udziela się informacji o działaniach podjętych w związku z jej żądaniem wniesionym na podstawie art. 15.-22. RODO,
- gdy pracownik upoważniony do udzielenia informacji ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15. - 21., powinien zażądać od tej osoby dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą lub upoważnionej przez nią,
- gdy Administrator nie jest w stanie zidentyfikować podmiotu danych, można odmówić podjęcia żądanego działania,
- gdy dane osobowe osoby, której one dotyczą, uzyskiwane są od tej osoby, przedstawia się jej klauzulę informacyjną, w treści zgodnej z załącznikiem nr 2. do niniejszej Polityki,
- gdy dane osobowe pozyskiwane są w sposób inny niż od osoby, której dotyczą, przedstawia się jej klauzulę informacyjną w treści zgodnej z załącznikiem nr 2. do niniejszej Polityki,
- klauzule informacyjne publikuje się w sposób i miejscach ustalonych w tychże klauzulach,
- Administrator planując dalsze przetwarzanie danych osobowych w celu innym niż cel, w którym dane zostały pozyskane, przed dalszym przetwarzaniem informuje osobę której dane

dotyczą o tym innym celu i udziela jej odpowiednio wszelkich stosowanych informacji, o których mowa powyżej,

- Administrator niezwłocznie informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu udostępniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernego nakładu pracy i kosztów. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Administrator zapewnia realizację praw i wolności osób, których dane dotyczą

I. Prawo dostępu przysługujące osobie, której dane dotyczą

Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarza on dane osobowe ją dotyczące. Gdy ma to miejsce, jest ona uprawniona do uzyskania dostępu do nich oraz uzyskania informacji o:

- celu przetwarzania,
- kategorii przetwarzanych danych osobowych,
- odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
- planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu, w miarę możliwości,
- prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
- prawie wniesienia skargi do organu nadzorczego,
- źródle pozyskania przetwarzanych jej danych osobowych, jeżeli dane te nie zostały uzyskane od niej,
- zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22. ust. 1. i 4. RODO, oraz o istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Na żądanie osoby, której dane dotyczą, Administrator dostarcza jej bezpłatnie pierwszą kopię danych osobowych podlegających przetwarzaniu, z danego okresu i zakresu.

Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.

Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną równocześnie nie wskazując formy ich przekazania, informacji udziela się drogą elektroniczną.

II. Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

III. Prawo do bycia zapomnianym

Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek niezwłocznie usunąć dane, jeżeli zachodzi jedna z następujących okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
- osoba, której dane dotyczą, cofnęła zgodę będącą podstawą przetwarzania, i nie ma innej podstawy prawnej przetwarzania tych danych,
- osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21. ust. 1. RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21. ust. 2. RODO wobec przetwarzania,
- dane osobowe były przetwarzane niezgodnie z prawem,
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega Administrator,
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Jeżeli Administrator upublicznił dane osobowe, a ma obowiązek je usunąć, to - biorąc pod uwagę dostępną technologię i koszt realizacji - podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe o tym, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

Prawo do usunięcia danych nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne do:

- korzystania z prawa do wolności wypowiedzi i informacji,

- wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,
- celów: archiwalnych w interesie publicznym, badań naukowych lub historycznych lub statystycznych, o ile prawdopodobne jest, że realizacja prawa do bycia zapomnianym uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania,
- ustalenia, dochodzenia lub obrony roszczeń.

IV. Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania w następujących przypadkach:

- gdy kwestionuje ona prawidłowość danych osobowych - na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych,
- przetwarzanie jest niezgodne z prawem, a osoba ta sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
- Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
- gdy osoba ta wniosła sprzeciw na mocy art. 21. ust. 1. RODO wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu.

Jeżeli zgodnie z żądaniem przetwarzanie zostało ograniczone, dane osobowe można nadal przetwarzać, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń a także w celu ochrony praw innej osoby fizycznej lub prawnej lub z uwagi na ważne względy interesu publicznego.

Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, której dane dotyczą i żądała ograniczenia przetwarzania.

V. Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi. Ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe, jeżeli:

- przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy,

- przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane te zostały przesłane przez Administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku prawa do bycia zapomnianym. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Administrator odmawia realizacji prawa do przenoszenia danych w sytuacji, gdy realizacja tego prawa może niekorzystnie wpływać na prawa i wolności innych osób.

VI. Prawo do sprzeciwu

Osoba, której dane osobowe dotyczą, ma prawo wnieść w dowolnym momencie sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych, gdy:

- przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,
- przetwarzanie danych osobowych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora, 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.

Administratorowi nie wolno przetwarzać danych osobowych w sytuacji skorzystania z prawa do sprzeciwu, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych osoba, której dane dotyczą, ma prawo wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Rozdział VII.

Procedura dotyczące monitorowania przetwarzania danych osobowych

W Spółce PCZ wdrożono do stosowania odrębny dokument wewnętrzny Procedura ZI1„Instrukcja zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych w Poddębickim Centrum Zdrowia Spółce z o.o. siedzibą w Poddębicach". Jej przestrzeganie przez

pracowników powinno skutecznie zapewnić bezpieczeństwo przetwarzania danych w systemie informatycznym. W Instrukcji ustalono procedury i zasady:

- procedurę nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym,
- metody i środki uwierzytelniania użytkownika oraz procedury związane z ich zarządzaniem i użytkowaniem,
- procedurę rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym,
- procedurę tworzenia kopii zapasowych danych osobowych,
- procedurę przechowywania elektrycznych nośników informacji oraz kopii zapasowych,
- zasady zabezpieczenia systemu informatycznego przed oprogramowaniem, które może doprowadzić do uzyskania nieuprawnionego dostępu do systemu informatycznego oraz zabezpieczenia przed wirusami komputerowymi,
- zasady wykonywania przeglądów i konserwacji systemów informatycznych oraz elektronicznych nośników informacji służących do przetwarzania danych osobowych.

Rozdział VIII.

Procedura monitorowania użytkowania sprzętu i oprogramowania przez pracownika

1. Administrator wyposaży pracownika, o ile wymaga tego zajmowane stanowisko pracy, w służbowy sprzęt, w tym sprzęt komputerowy (dalej sprzęt) i służbowe oprogramowanie komputerowe (dalej oprogramowanie) niezbędne do prawidłowego wykonywania powierzonych zadań. Pracownik w trakcie wykonywania tych zadań może mieć, w ramach wydanego mu upoważnienia, dostęp do informacji stanowiących: tajemnicę służbową, o danych osobowych, danych poufnych lub danych, co do których Administrator zobowiązał się do ich zabezpieczenia przed nieuprawnionym ujawnieniem.
2. Pracownik może korzystać ze sprzętu i oprogramowania wyłącznie w celu wykonywania powierzonych mu obowiązków, zgodnie z obowiązującymi przepisami prawa. Powyższy obowiązek należy do podstawowych obowiązków pracowniczych z uwagi na konieczność dbałości o mienie i obowiązki Administratora.
3. Pracownik jest obowiązany do:
   - niekorzystania z jakiegokolwiek oprogramowania komputerowego innego niż oprogramowanie, w szczególności niedokonywania instalacji takiego oprogramowania na użyczonym sprzęcie,

- niekorzystania ze sprzętu i oprogramowania w celach prywatnych, w szczególności poprzez prowadzenie korespondencji e-mail nie związanej ze świadczeniem pracy, poprzez korzystanie z komunikatorów, portali społecznościowych, witryn www, innych niż konieczne do wykonywania obowiązków pracowniczych,
- niekorzystania z oprogramowania w sposób mogący naruszyć prawa osób trzecich, w tym niekopiowania i nierozpowszechniania oprogramowania,
- niezwłocznego udostępniania Administratorowi, na każde jego żądanie, sprzętu i oprogramowania celem umożliwienia wykonania kontroli, o której mowa w pkt 4. niniejszej Procedury.

4. Dochowywanie przez pracowników powyższych zasad, na polecenie Administratora, może sprawdzać pracownik Działu ds. Informatyzacji i Baz Danych lub IOD, poprzez:
   - monitoring operacji wykonywanych na sprzęcie,
   - sprawdzanie wykazu połączeń telefonicznych dokonywanych z telefonów służbowych,
   - kontrolę zainstalowanego oprogramowania i sposobu korzystania z niego,
   - kontrolę czasu pracy przy wykorzystaniu sprzętu i oprogramowania,
   - kontrolę aktywności w internecie,
   - kontrolę wysyłanej poczty służbowej.
5. Bezwzględnie zabronione jest wykorzystywanie sprzętu lub oprogramowania w celach niezgodnych z prawem lub zasadami obowiązującymi u Administratora, a w szczególności dla dostępu do internetu w celach:
   - korzystania z treści pornograficznych,
   - naruszania praw autorskich (nielegalnego pobierania bądź udostępniania plików),
   - infekowania sieci komputerowej wirusami pobieranymi z plikami z internetu;
   - korzystania ze służbowej poczty elektronicznej w sprawach prywatnych.
6. W związku z naruszeniem zasad niniejszej Polityki pracownik może podlegać odpowiedzialności karnej, o której stanowi Kodeks Karny oraz odpowiedzialności karnej i cywilnej przewidzianej w ustawie o prawie autorskim i prawach pokrewnych za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie oprogramowania oraz odpowiedzialności karnej określonej w tej ustawie.
7. Naruszenie przez pracownika jego obowiązków pracowniczych w zakresie wskazanym w niniejszej Polityce może stanowić podstawę do podjęcia przez Spółkę PCZ przysługujących jej środków prawnych, a w szczególności może stanowić przyczynę uzasadniającą

wypowiedzenie przez Spółkę PCZ umowy o pracę łączącej Spółkę PCZ z pracownikiem lub wymierzenie kary porządkowej przewidzianej przepisami ustawy Kodeks Pracy.

Rozdział IX.

Procedura zarządzania systemem monitoringu wizyjnego

Na potrzeby niniejszej Polityki, w Spółce PCZ wprowadzono Procedurę ZI1.1 „Procedurę Zarządzania Monitoringiem Wizyjnym". Jej przestrzeganie przez pracowników powinno skutecznie zapewnić bezpieczeństwo przetwarzania danych pozyskanych z monitoringu.

Procedura określa:

- cel i zasady funkcjonowania systemu monitoringu wizyjnego, miejsca instalacji kamer systemu, reguły rejestracji i przechowywania zapisu z kamer, sposób ich zabezpieczania oraz tryb udostępniania danych z zapisu z kamer,
- osoby uprawnione do przeglądania zarejestrowanego obrazu,
- sposób podania do publicznej wiadomości informacji o monitoringu,
- czasokresie przechowywania zapisu z monitoringu,
- środki organizacyjne wdrożone dla ochrony danych osobowych zarejestrowanych monitoringiem,
- zasady udostępniania zapisu z monitoringu.

Rozdział X.

Procedura fizycznego dostępu do pomieszczeń służbowych

Celem niniejszej procedury obowiązującej pracowników komórek organizacyjnych pracujących w trybie jednodniowym jest określenie zasad pobierania kluczy do pomieszczeń, w których przetwarzane są dane osobowe, jak również do innych pomieszczeń zamykanych na noc.

1. Obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych poprzez zastosowanie zamków patentowych.
2. Klucze do pomieszczeń, w których przetwarzane są dane osobowe, dla jak również do innych pomieszczeń zamykanych na noc, pracownicy komórek organizacyjnych pracujących w trybie jednodniowym pobierają w portierni przed rozpoczęciem pracy i tam je zdają po jej zakończeniu.
3. Pracownicy portierni są odpowiedzialni za całodobowe sprawowanie nadzoru nad powierzonymi im kluczami i ich wydawanie, w tym, kluczy do pomieszczeń służbowych,

kluczy zapasowych do pomieszczeń służbowych, kodów do pomieszczeń wyposażonych w instalację alarmową, gdy zostaną one zainstalowane.

4. Klucze do pomieszczeń przechowywane są w sposób uporządkowany w zamykanej gablocie.
5. Klucze zapasowe i kody do pomieszczeń wyposażonych w instalację alarmową przechowywane są w sposób uporządkowany w zamkniętej metalowej kasetce.
6. Kluczy mogą być wydane tylko pracownikowi, którego nazwisko znajduje się w wykazie pracowników upoważnionych do pobierania kluczy.
7. Kierownik Działu Technicznego jest odpowiedzialny za sporządzenie i bieżącą aktualizację wykazu pracowników upoważnionych do pobierania kluczy do pomieszczeń służbowych. Wykaz ten opracowywany jest po przekazaniu kierownikowi Działu Technicznego stosownych informacji przez osoby kierujące pracą poszczególnych komórek organizacyjnych.
8. Upoważnieni pracownicy pobierają i zdają klucze codziennie, za potwierdzeniem tej czynności czytelnym podpisem w ewidencji.
9. Za prowadzenie ewidencji pobranych i zdanych kluczy do pomieszczeń służbowych odpowiedzialne są osoby świadczące usługi na stanowisku portiera.
10. Ewidencja prowadzona jest zgodnie ze wzorem, który przygotowuje kierownik Działu Technicznego. Niezbędne dane w ewidencji to: nr pomieszczenia służbowego, data oraz godzina pobrania i zdania kluczy, imię i nazwisko osoby pobierającej i zdającej klucze a także jej czytelny podpis.
11. Wydanie kluczy zapasowych oraz kodów dostępów do pomieszczeń wyposażonych w instalację alarmową może nastąpić tylko w sytuacjach awaryjnych, na polecenie:
    - członka Zarządu Spółki PCZ,
    - osoby kierującej pracą danej komórki organizacyjnej,
    - starszego lekarza dyżuru.
12. Gdy w siedzibie Administratora dojdzie do sytuacji powstania zagrożenia życia i zdrowia ludzi lub zagrożenia powstania strat materialnych, wydanie kluczy zapasowych oraz kodów dostępów może nastąpić również na polecenie Pełnomocnika ds. Ochrony Informacji Niejawnych.
13. Zmiana kodów do pomieszczeń wyposażonych w instalację alarmową następuję co pół roku.
14. Odpowiedzialnym za bieżącą aktualizację wykazu kodów do pomieszczeń wyposażonych w instalację alarmową odpowiedzialny jest Pełnomocnika ds. Ochrony Informacji Niejawnych.

15. Pracownicy portierni zobowiązani są do sporządzenia notatki służbowej w sytuacji wydania kluczy zapasowych a także kodów dostępu do pomieszczeń wyposażonych w instalację alarmową.
16. W notatce służbowej należy odnotować: imię i nazwisko osoby pobierającej klucz zapasowy lub kod dostępu, informację o osobie wydającej polecenie wydania kluczy lub kodu, datę i godzinę pobrania kluczy lub kodu, datę i godzinę zwrotu klucza.
17. Pracownik dysponujący pobranym kluczem zapasowym ponosi pełną odpowiedzialność za ich ochronę, do momentu zdania klucza pracownikowi portierni.
18. Każdą utratę, uszkodzenie lub zniszczenie klucza należy niezwłocznie zgłosić bezpośredniemu zwierzchnikowi służbowemu. O dalszym postępowaniu decyduje członek Zarządu Spółki PCZ.
19. Zakazane jest:
    - dorabianie kluczy do pomieszczeń służbowych, gdy są do dyspozycji klucze, nad którymi pieczę sprawują pracownicy portierni,
    - udostępnianie kluczy oraz kodów dostępów do pomieszczeń służbowych wyposażonych w instalację alarmową osobom nieupoważnionym,
    - pozostawianie pomieszczeń służbowych a także kluczy bez dozoru.

Rozdział XI.

Procedura udostępniania danych osobowych

W Spółce PCZ wdrożono do stosowania odrębny dokument wewnętrzny „Zasady udostępniania dokumentacji medycznej pacjentów Poddębickiego Centrum Zdrowia Spółki z o.o. z siedzibą w Poddębicach". Przestrzeganie zasady przez pracowników powinno skutecznie zapewnić bezpieczeństwo przetwarzania danych osobowych, w związku z udostępnianiem dokumentacji medycznej. W Instrukcji określono, między innymi:

- formy udostępniania dokumentacji medycznej,
- zasady ogólne udostępniania dokumentacji medycznej: osobom fizycznym, uprawnionym organom i instytucjom, między jednostkami organizacyjnymi Spółki PCZ,
- zasady odpłatności za sporządzenie wyciągów, odpisów oraz kopii danych z dokumentacji medycznej.

Rozdział XII.

Procedura powierzania przetwarzania danych osobowych

Administrator może korzystać z usług podmiotów przetwarzających dane osobowe (procesorów), którzy dają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.

Przetwarzanie danych osobowych przez procesora odbywa się na podstawie pisemnej umowy zawartej z nim przez Administratorem, zgodnie z załącznikiem nr 3. do niniejszej Polityki.

Rozdział XIII.

Procedura przeprowadzania szkoleń pracowników

Celem niniejszej procedury jest zapewnienia realizacji zadania Administratora jakim jest informowanie pracowników, którzy będą przetwarzać dane osobowe lub je przetwarzają, o ich obowiązkach wynikających z przepisów RODO oraz innych przepisów z zakresu ochrony danych osobowych, w tym niniejszej Polityki.

1. Pracownik Działu Kadrowo-Płacowego lub Działu Prawno-Organizacyjnego przekazuje, odpowiednio, IOD informację o każdym pracowniku, którego zakres obowiązków wymaga lub może spowodować przetwarzanie danych osobowych. Informacja powinna być przekazana IOD najpóźniej z dniem podpisania stosownej umowy ale zawsze przed dopuszczeniem pracownika do realizacji umowy.
2. IOD, na podstawie informacji przekazanej mu, zgodnie z treścią pkt. 1., przygotowuje pracownikowi pisemne upoważnienie do przetwarzania danych osobowych, wraz z pisemną informacją o zasadach przetwarzania danych osobowych oraz pisemną informacją o zasadach ochrony danych osobowych, stanowiącymi załączniki nr 4.
3. Obie informacje, o których mowa powyżej, są traktowane jako indywidualne szkolenie pracownika z zakresu podstawowych zasad ochrony danych osobowych zgodnie z RODO, i jako takie pracownik potwierdza własnoręcznym podpisem w dokumentacji IOD.
4. Każdy pracownik upoważniony do przetwarzania danych osobowych, przed dopuszczeniem do wykonywania czynności służbowych czy realizacji umowy cywilno-prawnej, jest szkolony z zakresu praw i obowiązków zajmowanego stanowiska. Szkolenie przeprowadza bezpośredni przełożony lub osoba wyznaczona przez niego. Szkolenie powinno zaznajomić pracownika z regulacjami wewnętrznymi obowiązującymi u Administratora, w tym z niniejszą Polityką, dla zgodnego z prawem sposobu przetwarzania danych osobowych.

5. Przynajmniej raz w roku IOD przeprowadza szkolenia grupowe dla wszystkich pracowników, którzy przetwarzają dane osobowe. Szkolenie jest obowiązkowe dla wszystkich pracowników, którym Administrator wydał upoważnienie do przetwarzania danych osobowych. Szkolenie obejmuje swym zakresem omówienie obowiązków spoczywających na pracownikach przetwarzających dane osobowe na mocy RODO oraz innych przepisów z zakresu ochrony danych osobowych, a także na mocy niniejszej Polityki. Uczestnicy szkolenia własnoręcznym podpisem na liście obecności potwierdzają udział w szkoleniu. Lista ta pozostaje w dokumentacji IOD.
6. Administrator zapewnia odpowiednie warunki do przeprowadzenia szkoleń grupowych oraz udział w nich pracowników upoważnionych do przetwarzania danych osobowych.
7. Zakres obowiązków służbowych (w przypadku osób wykonujących zadania na podstawie umów cywilno-prawnych, zakres świadczonych usług ustalony tymi umowami) wraz z przyznanymi przez Głównego Inspektora ds. Informatyzacji i Baz Danych dostępami do systemów informatycznych stanowi każdorazowo polecenie, o którym mowa w art. 29. RODO.

Rozdział XIV.

Procedura zgłaszania incydentów

Procedura definiuje katalog zagrożeń i incydentów mogących prowadzić do naruszenia bezpieczeństwa danych osobowych przetwarzanych przez Administratora (w tym powierzonych Administratorowi przez inny podmiot) oraz sposób reagowania na ww. zagrożenia i incydenty.

Celem procedury jest ograniczenie skutków wystąpienia incydentów godzących w bezpieczeństwo przetwarzania danych osobowych oraz zmniejszenie ryzyka ich powstania w przyszłości.

Postępowanie wewnętrzne

1. Najczęściej występujące zagrożenia bezpieczeństwa danych osobowych:
   - niewłaściwe zabezpieczenie stacji roboczych, komputerów przenośnych, tabletów, smartphonów, telefonów, przenośnych elektronicznych nośników danych oraz oprogramowań informatycznych przed kradzieżą, zniszczeniem lub utratą danych osobowych,
   - niewłaściwe fizyczne zabezpieczenie pomieszczeń, urządzeń oraz dokumentów,
   - nieprzestrzeganie przez upoważnione osoby przyjętych zasad przetwarzania danych oraz zasad ochrony danych osobowych, obowiązujących u Administratora.
2. Przykładowe incydenty naruszenia zasad bezpieczeństwa danych osobowych:

- incydenty losowe zewnętrzne np.: pożar obiektu lub pomieszczenia, zalanie wodą, utrata zasilania czy łączności,
- incydenty losowe wewnętrzne niezależne od pracownika np. awaria stacji roboczych, serwera czy oprogramowania, utrata lub zgubienie danych zawartych na nośnikach przenośnych,
- incydenty umyślne np.: ataki hakerskie, włamania do pomieszczeń, celowe i świadome niszczenie lub zniszczenie dokumentów, korzystanie ze szkodliwego oprogramowanie.

3. Każdy pracownik gdy stwierdzi zagrożenie lub podejmie podejrzenie naruszenia zasad ochrony danych osobowych, obowiązany jest do niezwłocznego poinformowania o tych okolicznościach bezpośredniego przełożonego lub Głównego Specjalistę ds. Informatyzacji i Baz Danych.
4. Osoby powiadomione o stwierdzonym naruszeniu lub podejrzeniu naruszenia zasad ochrony danych osobowych są obowiązane do niezwłocznego przekazania tego powiadomienia IOD.
5. W przypadku podejrzenia wystąpienia zagrożenia lub incydentu IOD w porozumieniu z Głównym Inspektorem ds. Informatyzacji i Baz Danych prowadzą postępowanie w toku którego:
   - ustalają zakres i przyczyny zagrożenia lub incydentu oraz jego ewentualne skutki,
   - inicjują ewentualne postępowanie dyscyplinarne,
   - rekomendują działania prewencyjne zmierzające do eliminacji podobnych zagrożeń lub incydentów w przyszłości,
   - dokumentują prowadzone postępowanie,
   - przedstawiają Administratorowi raport z przeprowadzonego postępowania.
6. Po stwierdzeniu poważnego incydentu lub powzięcia uzasadnionej informacji o podejrzeniu poważnego naruszenia zasad ochrony danych osobowych, IOD informuje Administratora o konieczności zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu chyba, że jest mało prawdopodobne by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
7. Oceny, czy występuje ryzyko naruszenia praw lub wolności człowieka, Administrator dokonuje we współpracy z IOD. Ocena powinna wynikać z obiektywnych kryteriów, takich jak dotychczasowe doświadczenie związane z podobnymi naruszeniami lub wiedza z zakresu bezpieczeństwa informacji, oraz z uwzględnienia okoliczności samego ryzyka naruszenia ochrony danych osobowych.

8. W toku dokonywania oceny, o której mowa powyżej, Administrator bierze pod uwagę wszelkie możliwe szkody, jak i krzywdy, które mogą wyniknąć dla osób fizycznych z danego naruszenia. Mogą one w szczególności polegać na:
   - utracie kontroli nad własnymi danymi osobowymi,
   - negatywnych konsekwencjach wizerunkowych,
   - możliwości zawierania przez inną osobę umów z wykorzystaniem danych osobowych innej osoby fizycznej,
   - stratach finansowych,
   - negatywnym odbiorze społecznym, który może być konsekwencją upublicznienia niektórych danych osobowych.
9. W przypadku stwierdzenia poważnego incydentu lub powzięcia uzasadnionej informacji o podejrzeniu poważnego naruszenia zasad ochrony danych osobowych IOD zawiadamia Administratora o rozpoczęciu audytu doraźnego, przed podjęciem pierwszej czynności w toku audytu.
10. Po zawiadomieniu, o którym mowa powyżej, IOD, niezależenie od działań omówionych w pkt. 5., niezwłocznie rozpoczyna audyt doraźny. W ramach czynności audytowych IOD, przy czynnym współudziale Głównego Specjalisty ds. Informatyzacji i Baz Danych, określa sposób dokumentowania audytu, a w jego ramach:
   - sporządza notatki z czynności audytowych, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych,
   - odbiera pisemne wyjaśnienia od osoby, której czynności objęto audytem,
   - sporządza niezbędne kopie okazanych dokumentów,
   - sporządza niezbędne kopie obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
   - sporządza niezbędne kopie zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu,
   - zabezpiecza ewentualne dowody związane z incydentem,
   - ustala osoby odpowiedzialne za powstanie incydentu,
   - wskazuje możliwe sposoby przywrócenia stanu zgodnego z prawem,
   - wnioskuje o wszczęcie postępowań dyscyplinarnych,

- przygotowuje raport dla Administratora.

11. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta powinna pozwolić organowi nadzorczemu na zweryfikowanie przestrzegania niniejszej Procedury.
12. IOD prowadzi rejestr incydentów, w którym należy odnotować: l.p. incydentu; datę i ewentualnie godzinę, w której do niego doszło: imię i nazwisko osoby zgłaszającej, datę i godzin ę zgłoszenia, szczegółowy opis incydentu i wywołanych przez niego skutków, zalecone przez Administratora i IOD działania naprawcze; datę i godzinę stwierdzonego usunięcia sytuacji powodującej incydent.

Zgłaszanie naruszenia ochrony danych osobowych

1. Gdy dojdzie do naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza to naruszenie organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Gdy naruszenie dotyczy danych osobowych osób fizycznych, których Spółka PCZ nie jest Administratorem, a podmiotem przetwarzającym, któremu na podstawie art. 28. RODO zostały dane powierzone, wtedy po stwierdzeniu naruszenia ochrony danych osobowych PCZ, bez zbędnej zwłoki, zgłasza naruszenie podmiotowi, który dane PCZ powierzył.
3. Zgłoszenie, o którym mowa w pkt. 1., zawiera co najmniej:
   - opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorii i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   - imię i nazwisko oraz dane kontaktowe IOD lub wskazanie dane innej osoby, od której można uzyskać niezbędne informacje,
   - opis możliwych konsekwencji naruszenia ochrony danych osobowych,
   - opisy środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach opis środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Gdy naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, tak aby umożliwić jej podjęcie niezbędnych działań zapobiegawczych.
2. W zawiadomieniu jasnym i prostym językiem należy opisać charakter naruszenia ochrony danych osobowych oraz zawrzeć przynajmniej następujące informacje i środki:
   - imię i nazwisko oraz dane kontaktowe IOD lub wskazanie dane innej osoby, od której można uzyskać niezbędne informacje,
   - opis możliwych konsekwencji naruszenia ochrony danych osobowych,
   - opisy środków zastosowanych lub proponowanych w celu zaradzenia naruszeniu ochrony danych osobowych, a w stosownych przypadkach, opis środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.
3. Zawiadomienie nie jest wymagane gdy:
   - Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   - Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   - wymagałoby ono niewspółmiernie dużego wysiłku - wtedy Administrator wyda publiczny komunikat lub zastosuje podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

Rozdział XV.

Procedura zarządzania ryzykiem

Procedura zarządzania ryzkiem to szereg skoordynowanych działań podejmowanych przez członków Zarządu Spółki PCZ, kierowników i koordynatorów poszczególnych komórek organizacyjnych i jednostek organizacyjnych PCZ, jak i pracowników, którzy poprzez identyfikację i analizę ryzyka oraz określanie adekwatnych reakcji na ryzyko zwiększają poziom bezpieczeństwa przetwarzania danych osobowych w ramach poszczególnych procesów ich przetwarzania.

1. W ramach działań dla zidentyfikowanych procesów przetwarzania danych osobowych w tabela stanowiących integralną część niniejszej Procedury wskazano, przeanalizowano i oszacowano:
   1.1. **zasoby**, które należy chronić:
      1.1.1. sprzęt komputerowy przechowujący dane,
      1.1.2. dane osobowe przetwarzane w formie papierowej i elektronicznej,
      1.1.3. prawa i wolności osób fizycznych, których dane dotyczą,
      1.1.4. aplikacje, w których przetwarzane są dane osobowe,
      1.1.5. pomieszczenia, w których pracują osoby upoważnione do przetwarzania danych osobowych;
   1.2. **zastosowane środki bezpieczeństwa techniczne i organizacyjne,** opisane w niniejszej Polityce;
   1.3. **zagrożenia** - zdarzenia, które można wyróżnić ze względu na zagrożenie lub utratę poufności, dostępności, integralności i rozliczalności przetwarzanych danych osobowych a mogące powodować wystąpienie incydentu,
   1.4. **podatności** - słabości zasobów, które mogą być wykorzystane przez potencjalne zagrożenia,
   1.5. **skutki** - wpływ jaki będzie miał zaistniały incydent na utratę danych osobowych.
2. Biorąc powyższe pod uwagę Administrator zapewnia warunki pracy systemach informatycznych gwarantujące poufność, dostępność, integralność i rozliczalność przetwarzanych danych osobowych.
3. Administrator dostosowuje środki bezpieczeństwa zarówno techniczne, fizyczne, jak i organizacyjne do wyników przeprowadzonej analizy ryzyka.
4. Zidentyfikowane przez Administratora zagrożenia, podatności oraz skutki związane z utratą poufności, dostępności, integralności i rozliczalność przetwarzanych danych osobowych wyszczególnione są w tabeli stanowiącej integralną część niniejszej Procedury. W niniejszej Polityce omówiono zagrożenia wewnętrzne (np. działanie pracownika, awaria systemu spowodowana brakiem zasilania) i zewnętrzne (np. atak hakerski) mogące być następstwem działań (umyślnych lub nieumyślnych) człowieka lub wynikające z przyczyn naturalnych (środowiskowych).
5. Zidentyfikowane zagrożenia, podatności oraz skutki naruszeń podlegają obiektywnej analizie mającej na celu oszacowanie tzw. istotności ryzyka. Na potrzeby niniejszej Procedury poziomem istotności ryzyka obrazuje tabela nr 5., która obrazuje macierz ryzyka i jest

iloczynem oceny prawdopodobieństwa wystąpienia danego ryzyka - przedstawionym w tabeli nr 3. oraz oceny jego skutku przedstawionej w tabela nr 4. do niniejszej Procedury.

6. Istotność konkretnego ryzyka określa czy jego poziom jest akceptowalny (patrz tabela nr 6. do niniejszej Procedury). Ryzykiem:
   6.1. akceptowalnym jest ryzyko na poziomie N (niskim, iloczyn = 3). Przy tym poziomie ryzyka podjęcie dodatkowych działań ograniczających wystąpienie zagrożenia może nastąpić w okresie dłuższym niż w ciągu roku, w zależności od możliwości i koniecznych nakładów finansowych,
   6.2. nieakceptowalnym jest ryzyko na poziomie Ś i W (średni i wysoki, iloczyn od 4 - 16). Przy tym poziomie ryzyka konieczne jest zastosowanie dodatkowych mechanizmów kontrolnych (wdrażane są adekwatne, skuteczne i efektywne działania zaradcze), z uwzględnieniem sposób postępowania określonych w pkt. 7. niniejszej Procedury.
7. Administrator podejmuje poniższe sposoby postępowania z ryzykiem:
   7.1. przeniesienie ryzyka - polega na wykupieniu ubezpieczenia od konkretnego zdarzenia lub scedowaniu skutków ryzyka na kontrahenta, przy czym przeniesienie ryzyka nie eliminuje go,
   7.2. akceptacja ryzyka - świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu Administratora, w szczególności gdy koszty podjętych ewentualnych działań mogą przekroczyć przewidywane korzyści,
   7.3. redukcja ryzyka - polega na obniżeniu poziomu ryzyka do poziomu akceptowalnego poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenia skutków jego wystąpienia np. poprzez zwiększenie mechanizmów kontroli (procedury, wytyczne, zasadny, nadzór),
   7.4. unikanie ryzyka - polega na unikaniu przez Administratora działań, które powodują powstanie określonych zagrożeń np. w przypadku gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatnych do przewidywanych korzyści.
8. Identyfikację i analizę ryzyka przeprowadza się:
   - na bieżąco jako element systematycznego działania,
   - okresowo, co najmniej raz w roku, w sposób udokumentowany, odnosząc się do obecnych oraz nowo zidentyfikowanych procesów przetwarzania danych osobowych.
9. Za każde zidentyfikowane ryzyko, w tym za sposób postępowania odnośnie tego ryzyka odpowiedzialna jest osoba mająca uprawnienia wystarczające do zapewnienia efektywnego zarządzania ryzkiem w ramach zidentyfikowanego procesu przetwarzania, tj. właściciel ryzyka.

10. Właściciel ryzyka w zakresie wykonywanych zadań ponosi odpowiedzialność za:
    - przeprowadzanie i dokumentowanie identyfikacji i analizy ryzyka,
    - podejmowane decyzje o zakresie i sposobie zarządzania ryzykiem,
    - bezzwłoczne zgłoszenie bezpośredniemu przełożonemu ryzyka, które nie jest akceptowalne i które wymaga zastosowania dodatkowych mechanizmów kontrolnych oraz wskazania konkretnych działań zaradczych ograniczających wystąpienie ryzyka i jego skutków.
11. IOD w ramach niniejszej Procedury odpowiada za:
    - nadzór nad przestrzeganiem Procedury nad dokumentowaniem identyfikacji i analizy ryzyka,
    - rozstrzyganie wraz z Administratorem kwestii spornych w zakresie stosowanej metodyki zarządzania ryzykiem.
12. Podstawową dokumentację identyfikacji i analizy ryzyka stanowi arkusz ryzyk zagrażających bezpieczeństwu przetwarzania danych osobowych u Administratora zwany dalej „arkuszem ryzyk" (patrz tabela nr 7. do niniejszej Procedury).
13. Formularz arkusza ryzyk przekazywany jest przez IOD do właścicieli ryzyk w drodze elektronicznej, w terminach uzgodnionych z Prezesem Zarządu Spółki PCZ.
14. Wypełniony przez właściciela ryzyk arkusz ryzyk przekazywany jest IOD w postaci papierowej zawierającej datę sporządzenia i podpis właściciela ryzyka.
15. IOD konsoliduje wyniki analizy ryzyk i przedstawia Prezesowi Zarządu Spółki PCZ wraz z propozycją postępowania z ryzykiem.
16. Jeżeli na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka (patrz tabela nr 6. do niniejszej Procedury), zgodnie z art. 35. RODO przeprowadza się dla danego procesu przetwarzania ocenę jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane. Przy czym podczas przeprowadzania oceny skutków dla ochrony danych bierze się pod uwagę nie interesy Administratora, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.
17. Niniejsza Procedura podlega raz na rok przeglądowi, a w przypadku konieczności - aktualizacji. Przeglądu i aktualizacji procedury dokonuje IOD we współpracy z Głównym Specjalistą ds. Informatyzacji i Baz Danych.

Typowe czynności procesów przetwarzania danych osobowych przedstawia poniższe zestawienie:

tabela nr 1. do Procedury zarządzania ryzykiem

l.p.	proces	czynność związana z
1.	*2.*	*3.*
1.	rekrutacji pracowników i współpracowników	przeprowadzeniem rekrutacji i wyłonieniem kandydata
		dopuszczeniem kandydata do pracy lub nawiązaniem współpracy
		archiwizacją dokumentacji
2.	obsługi pracowników i współpracowników, w tym byłych pracowników i współpracowników	nawiązaniem zatrudnienia lub podpisaniem umowy cywilno-prawnej
		bieżąca obsługa pracowników
		bieżąca obsługa współpracowników
		bieżąca obsługa byłych pracowników
		bieżąca obsługa byłych współpracowników
		realizacją świadczeń socjalnych
		archiwizacją dokumentacji
3.	realizacji dostawy usług świadczonych na rzecz administratora	szacowanie wartości zamówienia
		zawarciem umowy
		realizacją umowy
		dochodzeniem roszczeń
		archiwizacją dokumentacji
4.	obsługi skarg i wniosków	przyjęciem skargi lub wniosku
		rozpatrzeniem skargi lub wniosku
		wydaniem rozstrzygnięcia w przedmiocie skargi lub wniosku
		z archiwizacją dokumentacji
5.	obsługi wniosków o udostępnienie informacji publicznej	przyjęciem wniosku o udostępnienie informacji publicznej
		rozpatrzeniem wniosku o udostępnienie informacji publicznej
		wydaniem rozstrzygnięcia w przedmiocie udostępnienia informacji publicznej
		archiwizacją dokumentacji
6.	obsługi korespondencji i osób kontaktujących się z Administratorem	rejestracją korespondencji przychodzącej i wychodzącej
		obiegiem dokumentów
		telefoniczną obsługą osób kontaktujących się
		archiwizacją dokumentacji
7.	obsługi finansowej i księgowej	realizacją zobowiązań finansowych
		windykacją należności
		archiwizacją dokumentacji

tabela nr 1. do Procedury zarządzania ryzykiem

l.p.	proces	czynność związana z
1.	*2.*	*3.*
8.	udzielania świadczeń zdrowotnych	rejestracją pacjenta
		przyjęciem pacjenta do oddziału lub poradni
		pobraniem materiału do badań lub wykonanie badania
		odbiorem wyników badania
		prowadzeniem dokumentacji medycznej pacjentów i byłych pacjentów
		wypisanie lub przeniesienie pacjenta z oddziału
		rozliczenie pacjentów z NFZ
		rejestracją wniosków o udostępnienie dokumentacji medycznej
		przygotowaniem wnioskowanej dokumentacji medycznej do udostępnienia
		wydaniem dokumentacji medycznej lub wyników badań
9.	zabezpieczania osób i mienia	obsługą monitoringu wizyjnego
		archiwizacją zapisu

Możliwie zagrożenia w procesie przetwarzania danych osobowych, wspólne dla wszystkich zasad i właściwości tj. poufności, dostępności integralności oraz rozliczalności przedstawia poniższe zestawienie:

tabela nr 2. do Procedury zarządzania ryzykiem

l. p.	wyszczególnienie	opis
1.	*2.*	*3.*
1.	**właściwość lub zasada postępowania**	**poufność, dostępność, integralność, rozliczalność**
2.	**zagrożenie**	awaria sprzętu, odcięcie zasilania, pożar, zalanie wodą, atak wirusa, kradzież nośników danych, nieuprawniony dostęp, nieprzestrzeganie wewnętrznych regulacji prawnych, przekroczenie uprawnień brak umowy powierzenia, brak okresowych szkoleń z zakresy ochrony danych, udostępnienie informacji podmiotom nieuprawnionych, przetwarzanie danych osobowych po upływie okresu niezbędnego do realizacji celu, przetwarzanie danych w zakresie nieadekwatnym do celu
3.	**przyczyna zagrożenia**	brak zabezpieczeń fizycznych, instalowanie nielegalnego oprogramowania, niefrasobliwość pracowników, niewyciąganie konsekwencji za przekroczenie uprawnień, niestosowanie się do obowiązujących regulacji prawnych i obowiązujących z Spółce PCZ, niewystarczający poziom świadomości pracowników a także ich zwierzchników z powagi zagrożeń i ich skutków, nieprzestrzeganie zasad przetwarzania danych osobowych i ich ochrony, wynoszenie poza siedzibę Spółki PCZ elektronicznych nośników zawierających dane osobowe, pozostawianie osób trzecich bez nadzoru w obszarze przetwarzania danych osobowych, brak legalnego oprogramowania, brak nadzoru nad oprogramowaniami służącymi przetwarzaniu danych, niewystarczające nakłady finansowe na fizyczne oraz

		informatyczne zabezpieczenie danych osobowych, nienależyte niszczenie danych osobowych przetwarzanych w formie papierowej, wykorzystywanie do celów prywatnych sprzętu i oprogramowania służbowego, niewystarczający nadzór nad dokumentacją archiwalną, brak reakcji na żądanie sprostowania danych osobowych, uniemożliwianie dostępu do danych osobowych osobom, których dane dotyczą
4.	**skutek**	wyciek, utrata, fizyczne zniszczenie lub uszkodzenie danych osobowych, straty wizerunkowe Spółki PCZ, straty finansowe, odpowiedzialność dyscyplinarna, karna lub kontraktowa, naruszenie praw i wolności osób, których dane dotyczą, przetwarzanie danych osobowych niezgodnie z prawem, przetwarzanie nieaktualnych danych osobowych, naruszenie zasady adekwatności/minimalizacji

Skale ocen prawdopodobieństwa wystąpienia zagrożenia w procesie przetwarzania danych osobowych, wspólne dla wszystkich procesów, przedstawia poniższe zestawienie:

tabela nr 3. do Procedury zarządzania ryzykiem

l. p.	**prawdopodobieństwo wystąpienia zagrożenia**	**istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne**
1.	*2.*	*3.*
1.	**niskie (N)**	ale w ostatnim okresie nie wystąpiło
2.	**średnie (Ś)**	ponieważ w ostatnim okresie już raz wystąpiło
3.	**wysokie (W)**	ponieważ w ostatnim okresie wystąpiło 2 lub 3 razy
4.	**bardzo wysokie (K)**	ponieważ w ostatnim okresie wystąpiło częściej niż 3 razy

Skale oceny prawdopodobieństwa wpływu wystąpienia zagrożenia w procesie przetwarzania danych osobowych, wspólne dla wszystkich procesów, przedstawia poniższe zestawienie:

tabela nr 4. do Procedury zarządzania ryzykiem

wystąpienie zagrożenia danych osobowych		
l. p.	**skala oceny**	**opis wpływu na dane osobowe objęte ryzykiem**
1.	*2.*	*3.*
1.	**niski**	**ma niewielki wpływ** na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka: • w dłuższym okresie czasu może spowodować niewielkie straty materialne, • nie powoduje strat lub powoduje minimalne straty lub koszty finansowe, • nie wpływa na prawa i wolności osób fizycznych
2.	**średni**	**ma umiarkowany wpływ** na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka: • może spowodować w okresie roku niewielkie straty materialne lub koszty finansowe, • stanowi naruszenie wewnętrznych regulacji, • ma znikomy wpływ na prawa i wolności osób fizycznych, których dane dotyczą, • ma niewielki wpływa na wizerunek Administratora.

3.	**wysoki**	**ma duży wpływ** na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka: • może spowodować w krótkim okresie czasu znaczące straty materialne lub koszty finansowe, • stanowi naruszenie wewnętrznych regulacji, • może stanowić naruszenie przepisów prawa, a brak reakcji może rodzić odpowiedzialność administracyjną lub cywilną, • ma wysoki wpływ na prawa i wolności osób fizycznych, których dane dotyczą, • może powodować zakłócenia w funkcjonowaniu Administratora, • ma duży wpływa na wizerunek Administratora.
4.	**bardzo wysoki**	**ma bardzo duży wpływ** na bezpieczeństwo przetwarzania danych osobowych. Przykładowy skutek ryzyka: • powoduje znaczące straty materialne lub koszty finansowe, • stanowi naruszenie przepisów prawa, a brak reakcji rodzi odpowiedzialność administracyjną, karną lub cywilną, • ma bardzo wysoki wpływ na prawa i wolności osób fizycznych, których dane dotyczą, • destabilizuje pracę Administratora, • wywołuje zdecydowanie negatywną reakcje publiczną, w mediach w całym kraju.

Korelację poziomu prawdopodobieństwa wystąpienia ryzyka zagrożenia i jego możliwego skutku przedstawia poniższe zestawienie nr 5. i 6.:

tabela nr 5. do Procedury zarządzania ryzykiem

l. p.	prawdopodobieństwo	skutek			
		niski	średni	wysoki	bardzo wysoki
1.	*2.*	*3.*	*4.*	*5.*	*6.*
1.	niskie (N)	niski	niski	niski	średni
2.	średnie (Ś)	niski	średni	średni	wysoki
3.	wysokie (W)	niski	średni	wysoki	krytyczny
4.	bardzo wysokie (K)	średni	wysoki	krytyczny	krytyczny

tabela nr 6. do Procedury zarządzania ryzykiem

l. p.	poziom ryzyka	poziom
1.	*2.*	*3.*
1.	niski (N)	**akceptowalny** - działanie naprawcze można przesunąć w czasie i wymaga monitorowania
2.	średni (Ś)	**akceptowalny** - działanie naprawcze można przesunąć w czasie i nie wymaga monitorowania
3.	wysoki (W)	**nieakceptowalny** - działanie naprawcze można przesunąć w czasie, ale wymaga stałego monitorowania
4.	krytyczny (K)	**nietolerowany** - wymaga natychmiastowego działania

Arkusz ryzyk zagrażających bezpieczeństwu danych przedstawia poniższe zestawienie:

tabela nr 7. do Procedury zarządzania ryzykiem

l. p.	komórka organizacyjna:	
1.	*2.*	*3.*
1.	proces przetwarzania	
2.	czynność przetwarzania	
3.	zagrożenia	
4.	ocena prawdopodobieństwa wystąpienia zagrożenia	
5.	ocena skutku	
6.	poziom istotności	
7.	sposób postępowania z ryzykiem	

Rozdział XV.

Procedura oceny skutków

Celem niniejszej Procedury jest zapewnienie realizacji obowiązków wynikających z art. 35. RODO, tj. ustalenie zasad wykonywania oceny skutków dla ochrony danych osobowych.

1. Jeżeli na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka (patrz tabela nr 6. do Procedury zarządzani ryzykiem), zgodnie z art. 35. RODO przeprowadza się dla danego procesu przetwarzania ocenę jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane.
2. Przeprowadzając ocenę skutków dla ochrony danych bierze się pod uwagę nie interesy Administratora, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane.
3. 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, przed rozpoczęciem tego przetwarzania dokonuje się oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
4. Dokonując oceny skutków dla ochrony danych, Administrator konsultuje się z IOD, m.in. kwestie dotyczące:
   - konieczności przeprowadzenia oceny skutków dla ochrony danych,
   - metodologii przeprowadzenia oceny skutków dla ochrony danych,
   - decyzji, czy przeprowadzić wewnętrzną ocenę, czy też zlecić ją podmiotowi zewnętrznemu,
   - zabezpieczeń, w tym środków technicznych i organizacyjnych, stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą,

- prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO, w szczególności czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy zastosować.

5. W sytuacji, gdy Administrator nie zgadza się z zaleceniami IOD, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia tych zaleceń.
6. Ocenę skutków, której formularz stanowi załącznik nr 6. do niniejszej Polityki, z wyłączeniem oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą, dokonuje się także w razie:
   - systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną,
   - przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa,
   - systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
7. Ocena skutków zawiera co najmniej:
   - systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez Administratora,
   - ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
   - ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
   - środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
8. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, IOD dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.
9. Administrator ustala następujący sposób oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą:
   - Administrator zidentyfikował możliwe skutki związane z naruszenia praw lub wolności osób, których dane dotyczą (patrz tabeli nr 1. do niniejszej Procedury),

- zidentyfikowane skutki podlegają obiektywnej analizie mającej na celu oszacowanie tzw. istotności ryzyka naruszenia praw w wolności osób, których dane dotyczą. Na potrzeby niniejszej Procedury poziomem istotności ryzyka jest iloczyn (patrz tabela nr 4. do niniejszej Procedury, która obrazuje macierz ryzyka) oceny prawdopodobieństwa wystąpienia danego ryzyka (patrz tabela nr 2. do niniejszej Procedury) oraz oceny jego skutku (patrz tabela nr 3. do niniejszej Procedury),
- istotność konkretnego ryzyka określa czy jego poziom jest akceptowalny (patrz tabela nr 5. do niniejszej Procedury). Ustala się, że ryzykiem:
  - ✓ akceptowalnym jest ryzyko na poziomie 3 i poniżej. Przy tym poziomie ryzyka podjęcie dodatkowych działań ograniczających wystąpienie zagrożenia może nastąpić w okresie dłuższym niż w ciągu roku, w zależności od możliwości i koniecznych nakładów finansowych;
  - ✓ nieakceptowalnym jest ryzyko na poziomie od 4 - 16. Przy tym poziomie ryzyka konieczne jest zastosowanie dodatkowych mechanizmów kontrolnych.
- Administrator przyjmuje następujące sposoby postępowania z ryzykiem związanym z naruszeniem praw i wolności osób, których dane dotyczą:
  - ✓ przeniesienie ryzyka - polegające na wykupieniu ubezpieczenia od konkretnego zdarzenia lub scedowaniu skutków ryzyka na kontrahenta, przy czym należy pamiętać, że przeniesienie ryzyka nie eliminuje go;
  - ✓ akceptacja ryzyka - świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu Administratora, w szczególności gdy koszty podjętych ewentualnych działań mogą przekroczyć przewidywane korzyści;
  - ✓ redukcja ryzyka - polegająca na obniżeniu poziomu ryzyka do poziomu akceptowalnego poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszeniu skutków jego wystąpienia np. poprzez zwiększenie mechanizmów kontroli (procedury, wytyczne, zasadny, nadzór);
  - ✓ unikanie ryzyka - polega na unikaniu przez Administratora działań, które powodują powstanie określonych zagrożeń np. w przypadku gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatnych do przewidywanych korzyści.
- Podstawową dokumentację identyfikacji i analizy ryzyka stanowi arkusz ryzyk zagrażających prawom i wolnościom osób, których dane dotyczą, zwany dalej „arkuszem ryzyk praw i wolności" (patrz tabela nr 6. do niniejszej Procedury).

10. Jeżeli wykonana ocena skutków dla ochrony danych wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym.
11. Konsultując się z organem nadzorczym Administrator przedstawia mu:
    - gdy ma to zastosowanie - odpowiednie obowiązki Administratora,
    - cele i sposoby zamierzonego przetwarzania,
    - środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z RODO,
    - dane kontaktowe inspektora ochrony danych,
    - ocenę skutków dla ochrony danych,
    - wszelkie inne informacje, których żąda organ nadzorczy.
12. Niniejsza Procedura podlega raz na rok przeglądowi oraz w przypadku konieczności aktualizacji.
13. Przeglądu i aktualizacji procedury dokonuje IOD.

tabela nr 1. do Procedury oceny skutków

możliwe nieprawidłowości w przetwarzaniu danych i skutki naruszenia praw lub wolności osób, których dane osobowe dotyczą		
l. p.	**nieprawidłowości w przetwarzaniu danych**	**skutek**
1.	*2.*	*3.*
1.	**naruszenie poufności danych osobowych chronionych tajemnicą zawodową**	dyskryminacja
		oszustwa dotyczące tożsamości
		kradzież tożsamości
		strata finansowa
2.	**nieuprawnione odwrócenie pseudonimizacji**	pozbawienie praw i wolności
		szkoda gospodarcza
		szkoda społeczna
3.	**pozbawienie możliwości sprawowania kontroli nad swoimi danymi osobowymi**	naruszenie dobrego imienia
		uszczerbek fizyczny

Skale ocen prawdopodobieństwa wystąpienia skutków w wyniku nieprawidłowości w procesie przetwarzania danych osobowych, przedstawia poniższe zestawienie:

tabela nr 2. do Procedury oceny skutków

l. p.	**prawdopodobieństwo wystąpienia zagrożenia**	**istnieją powody by sądzić, że zagrożenie objęte ryzykiem jest prawdopodobne**
1.	*2.*	*3.*
1.	**niskie (N)**	ale w ostatnim okresie nie wystąpiło
2.	**średnie (Ś)**	ponieważ w ostatnim okresie już raz wystąpiło
3.	**wysokie (W)**	ponieważ w ostatnim okresie wystąpiło 2 lub 3 razy
4.	**bardzo wysokie (K)**	ponieważ w ostatnim okresie wystąpiło częściej niż 3 razy

Korelację poziomu prawdopodobieństwa wystąpienia ryzyka zagrożenia i jego możliwego skutku przedstawiają poniższe zestawienia nr 3., 4. i 5.

tabela nr 3. do Procedury oceny skutków

l. p.	skala ocen	wpływ zagrożenia na prawa i wolności osób, których dane osobowe dotyczą
1.	*2.*	*3.*
1.	**niski (N)**	zagrożenie objęte ryzykiem ma **niewielki wpływ**
2.	**średni (Ś)**	zagrożenie objęte ryzykiem ma **umiarkowany wpływ**
3.	**wysoki (W)**	zagrożenie objęte ryzykiem ma **duży wpływ**
4.	**bardzo wysoki (K)**	zagrożenie objęte ryzykiem ma **bardzo duży wpływ**

tabela nr 4. do Procedury oceny skutków

l. p.	prawdopodobieństwo	skutek			
		niski	średni	wysoki	bardzo wysoki
1.	*2.*	*3.*	*4.*	*5.*	*6.*
1.	**niskie (N)**	niski	niski	średni	średni
2.	**średnie (Ś)**	niski	średni	wysoki	wysoki
3.	**wysokie (W)**	niski	średni	wysoki	krytyczny
4.	**bardzo wysokie (K)**	średni	wysoki	krytyczny	krytyczny

tabela nr 5. do Procedury oceny skutków

l. p.	poziom ryzyka	poziom
1.	*2.*	*3.*
1.	niski (N)	**akceptowalny** - działanie naprawcze można przesunąć w czasie i nie wymaga monitorowania
2.	średni (Ś)	**akceptowalny** - działanie naprawcze można przesunąć w czasie i wymaga monitorowania
3.	**wysoki (W)**	**nieakceptowalny** - działanie naprawcze można przesunąć w czasie, ale wymaga stałego monitorowania
4.	krytyczny (K)	**nietolerowany** - wymaga natychmiastowego działania

Arkusz ryzyk - skutków zagrażających prawom i wolnościom osób, których dane dotyczą przedstawia poniższe zestawienie:

tabela nr 6. do Procedury oceny skutków

l. p.	komórka organizacyjna:	
1.	*2.*	*3.*
1.	**proces przetwarzania**	
2.	**czynność przetwarzania**	
3.	**możliwy skutek**	
4.	**ocena prawdopodobieństwa wystąpienia skutku**	
5.	**ocena skutku**	
6.	**poziom istotności**	
7.	**sposób postępowania z ryzykiem**	

Rozdział XVI.

Procedura prowadzenia wykazów i rejestrów

Celem niniejszej Procedury jest ustalenie zasad prowadzenia przez IOD „Rejestru Podmiotów przetwarzających dane w imieniu administratora", „Rejestru czynności przetwarzania danych osobowych" oraz ewentualnego „Rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora", prowadzonych w celu realizacji przez Administratora zasady rozliczalności.

1. IOD prowadzi:
   - Rejestr Podmiotów Przetwarzających Dane Osobowe w imieniu Spółki PCZ, w którym należy ewidencjonować: nazwę i siedzibę procesora; kategorie przetwarzanych danych oraz osób, których dane dotyczą; numer umowy łączącej Administratora z procesorem oraz okres jej obowiązywania.
   - Rejestr Czynności Przetwarzania Danych Osobowych, zgodnie z art. 30. ust. 1. RODO, w którym należy ewidencjonować: nazwę i siedzibę administratora oraz jego dane kontaktowe, dane kontaktowe IOD, nazwę procesu, czynności przetwarzania, kategorie podmiotów danych, kategorie danych, szczególne kategorie danych, cel przetwarzania, planowany termin usunięcia danych, kategorie odbiorców danych, techniczne i organizacyjne środki bezpieczeństwa, aktualizację pozycji rejestru.
   - Rejestr Wszystkich Kategorii Czynności Przetwarzania Dokonywanych w Imieniu Administratora, zgodnie z art. 30. ust. 2. RODO, w którym należy ewidencjonować: nazwę i siedzibę podmiotu przetwarzającego i dane kontaktowe jego IOD, kategorie przetwarzań, techniczne i organizacyjne środki bezpieczeństwa, ostatnią aktualizację pozycji rejestru.
2. Wykazy i rejestry mają formę pisemną - mogą być prowadzone w formie elektronicznej.
3. IOD prowadzi wykazy i rejestry na podstawie danych otrzymanych od osób koordynujących pracę komórek organizacyjnych oraz od osób zajmujących samodzielne stanowiska pracy.
4. Osoby koordynujące pracę komórek organizacyjnych lub osoby zajmujące samodzielne stanowiska pracy są obowiązane do bieżącego przekazywania danych potrzebnych do prowadzenia wykazów i rejestrów, w szczególności są obowiązane do niezwłocznego informowania IOD o każdej zmianie mającej wpływ na treść wykazów i rejestrów.
5. Administrator, w ramach współpracy z organem nadzorczym, udostępnia rejestry i wykazy na żądanie tego organu w celu monitorowania przez organ operacji przetwarzania.

Rozdział XVII.

Procedura przeprowadzania audytów zgodności

Celem niniejszej Procedury jest określenie trybu i zasad monitorowania przez IOD przestrzegania RODO i przepisów powszechnie obowiązujących o ochronie danych osobowych, a także przepisów wewnętrznych obowiązujących u Administratora w dziedzinie ochrony danych osobowych, w tym niniejszej Polityki, poprzez przeprowadzanie audytów zgodności przetwarzania danych osobowych.

Audytor realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, regulaminów, zasad, zabezpieczeń, celów stosowanych dla spełniania wymagań RODO.

1. Audyt zgodności jest przeprowadzany w trybie:
   - audytu planowanego - przeprowadzanego przynajmniej raz w roku;
   - audytu doraźnego - w sytuacji powzięcia przez IOD wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takie naruszenia. Audyt doraźny przeprowadza się na zasadach opisanych w rozdziale „Procedura zgłaszania incydentów".
2. Przynajmniej na 14 dni przed rozpoczęciem audytu planowanego IOD informuje Administratora o przedmiocie, zakresie oraz terminie przeprowadzenia audytu i wnosi, w razie potrzeby, o współudział w audycie Głównego Specjalisty ds. Informatyzacji i Baz Danych.
3. Planując przeprowadzenie audytu IOD uwzględnia w szczególności: procesy przetwarzania danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych z:
   3.1. zasadami, o których mowa w art. 5., art. 12.-22. i art. 28. RODO i w niniejszej Polityce,
   3.2. zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 32. RODO i w niniejszej Polityce;
   3.3. zasadami przekazywania danych osobowych, o których mowa w art. 44.-49. RODO,
   3.4. obowiązkami wynikającymi z art. 33.-36. RODO,
   3.5. zweryfikowanym stanem faktycznym w zakresie przetwarzania danych osobowych,
   3.6.zasadami i obowiązkami określonymi w niniejszej Polityce.
4. IOD dokumentuje czynności przeprowadzone w toku audytu, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych oraz do opracowania raportu.
5. Dokumentowanie czynności w toku audytu może polegać, w szczególności, na utrwaleniu danych z systemu informatycznego służącego do przetwarzania danych osobowych lub

zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonania wydruku tych danych oraz na:

5.1. sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych,

5.2. odebraniu wyjaśnień od osoby, której czynności objęto audytem,

5.3. sporządzeniu kopii otrzymanego dokumentu,

5.4.sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania danych osobowych,

5.5. sporządzaniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych.

6. Czynności IOD dotyczące systemów informatycznych służących do przetwarzania lub zabezpieczania danych osobowych są wykonywane przy udziale osób zarządzającym tym systemem oraz przy współudziale Głównego Specjalisty ds. Informatyzacji i Baz Danych.

7. Osoba, której dotyczy audyt, bierze udział w audycie i umożliwia IOD przeprowadzenia czynności audytu.

8. Po zakończeniu audytu IOD przygotowuje raport zgodności sporządzony w postaci elektronicznej lub postaci papierowej.

9. IOD przekazuje Administratorowi raport zgodności:

- z audytu planowanego - nie później niż w terminie 30 dni od dnia zakończenia audytu,
- z audytu doraźnego - niezwłocznie, nie później niż w terminie 7 dni od dnia zakończenia audytu.

10. IOD jest uprawniony, w każdym czasie, do przeprowadzania weryfikacji przestrzegania niniejszej Polityki, bez konieczności przeprowadzania audytu zgodności.

11. IOD jest uprawniony do ustnego pouczenia osoby nieprzestrzegającej zasad określonych w niniejszej Polityce lub pisemnego zawiadomienia Administratora o nieprzestrzeganiu zasad przez wskazaną osobę.

12. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia.

13. Administrator dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia uchybień.

Rozdział XVIII.

Postanowienia końcowe

1. Niniejsza Polityka jest dokumentem wewnętrznym i osoby, które uzyskały wgląd w jej treść, zobowiązane są do zachowania jej w poufności.
2. Przypadki nieuzasadnionego zaniechania obowiązków określonych w niniejszym Polityce traktowane będą jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
3. W sprawach nieuregulowanych w niniejszej „Polityce ochrony danych osobowych" mają zastosowanie przepisy 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 przepisy prawa powszechnie obowiązujące z zakresu ochrony danych osobowych.

załącznik nr 1.

Wykaz kategorii osób, których dane dotyczą oraz kategorii danych osobowych					
l. p.	**kategoria osób, których dane dotyczą**	**kategorie danych osobowych**		**zastosowany program**	**wersja papierowa lub elektroniczna**
		zwykłe	**szczególne**		
1.	*2.*	*3.*	*4.*	*5.*	*6.*
1.	potencjalni pracownicy i współpracownicy	imię i nazwisko, wizerunek, data urodzenia, miejsce urodzenia, adres zamieszkania, adres do korespondencji, nr telefonu, adres poczty elektronicznej, przebieg kariery, informacje o zatrudnieniu u innego pracodawcy, informacje o statusie bezrobotnego, poziom wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia, umiejętności, stopień znajomości języków obcych, obsługa komputera, prawo jazdy, zainteresowania, nr prawa do wykonywania zawodu, data uzyskania prawa wykonywania zawodu, data wygaśnięcia prawa wykonywania zawodu	dane dotyczące zdrowia, wyroków skazujących lub naruszeń prawa	poczta elektroniczna	do wyboru
2.	pracownicy, współpracownicy oraz byli pracownicy i byli współpracownicy a także członkowie ich rodzin	imię i nazwisko, wizerunek, nazwa miejsca pracy, funkcja lub stanowisko, seria i nr dowodu tożsamości, data i miejsce urodzenia, miejsce zameldowania, adres zamieszkania, NIP, PESEL, nazwisko rodowe, obywatelstwo, prywatny nr telefonu, prywatny adres poczty elektronicznej, służbowy nr telefonu, służbowy adres poczty elektronicznej, imiona rodziców, stan rodzinny, imię i nazwisko oraz data urodzenia współmałżonka, data urodzenia dziecka lun dzieci pracownika, imię i nazwisko, oraz adres i nr telefonu osoby, którą należy poinformować w razie wypadku pracownika, stosunek do powszechnego obowiązku obrony, przebieg kariery, czas pracy, wysokość wynagrodzenia, nagrody, premie, kwoty udzielonych pożyczek, informacje o zatrudnieniu u innego pracodawcy, informacje o statusie bezrobotnego, informacje o oddziale NFZ, informacje o US, poziom wykształcenia, rok ukończenia szkoły, nazwa ukończonej szkoły, typ ukończonej szkoły, profil, tytuł naukowy, stopień naukowy, tytuł zawodowy, specjalizacja, ukończone studia podyplomowe, ukończone kursy i szkolenia, posiadane dodatkowe uprawnienia, umiejętności, stopień znajomości języków obcych, obsługa	dane dotyczące zdrowia, dane dotyczące wyroków skazujących i naruszeń prawa, dane dotyczące przynależności do związków zawodowych	poczta elektroniczna AXON Kadry AXON Płace, Płatnik	do wyboru

		komputera, prawo jazdy, zainteresowania, nr rachunku bankowego, firma, adres siedziby firmy, godzina i data użycia karty dostępu, imię i nazwisko osoby zgłoszonej do ubezpieczenia zdrowotnego, nr prawa do wykonywania zawodu, data uzyskania prawa wykonywania zawodu, data wygaśnięcia tego prawa			
3.	potencjalni dostawcy, ich pracownicy oraz współpracownicy	imię, nazwisko, nazwa firmy, adres e-mail, strona www, nr telefonu, dane z CEIDG, forma rozliczania, REGON, NIP, PESEL, seria i numer dowodu tożsamości		poczta elektroniczna	do wyboru
4.	dostawcy ich pracownicy i współ-pracownicy	imię, nazwisko, nazwa firmy, adres siedziby, adres dostawy, termin odstawy, adres e-mail, strona www, nr telefonu, dane z CEIDG, forma rozliczania, nr: REGON, NIP, PESEL, seria i nr dowodu tożsamości, historia dostaw		poczta elektroniczna AXON Magazyn	do wyboru
5.	skargi, wnioski i petycje	imię, nazwisko, numer telefonu, adres poczty elektronicznej, adres do korespondencji, adres zamieszkania, treść podania, nr PESEL		poczta elektroniczna	do wyboru
6.	informacja publiczna	imię, nazwisko, nr telefonu, adres poczty elektronicznej, adres do korespondencji, adres zamieszkania, treść podania, nr PESEL		poczta elektroniczna	do wyboru
7.	rejestr korespondencji	imię, nazwisko, nazwa firmy lub instytucji, adres zamieszkania, adres siedziby, informacja czego dotyczy pismo		poczta elektroniczna	do wyboru
8.	osoby do kontaktowania się	imię, nazwisko, adres poczty elektronicznej, nr telefonu, miejsce pracy		poczta elektroniczna	do wyboru
9.	finanse i księgowość	imię, nazwisko, nr: NIP, PESEL, rachunku bankowego, nazwa banku w którym prowadzony jest rachunek, REGON, telefonu, kwota, tytuł płatności, wysokość zadłużenia, informacje o egzekucji		poczta elektroniczna AXON Finanse system bankowy	do wyboru
10.	pacjenci byli pacjenci	imię, nazwisko, identyfikator pacjenta, nr: PESEL, NIP, płeć, data urodzenia, miejsce urodzenia, nazwisko rodowe, stan cywilny, imię ojca, imię matki, nr: ubezpieczenia, RUM, kod wykształcenia, adres poczty elektronicznej, adres zamieszkania, nr telefonu, adres korespondencyjny, kod wykonywanego zawodu, imię i nazwisko opiekuna, miejsce zamieszkania opiekuna, grupa krwi, seria i numer dowodu tożsamości, nr PESEL opiekuna, data ważności dokumentu ubezpieczenia, miejsce zameldowania, nr identyfikacyjny w kraju UE, numer europejskiej kartu ubezpieczeniowej, miejsce pracy, liczba dzieci, nr telefonu opiekuna, miejsce pracy opiekuna, zawód opiekuna, informacja o placówce w której dziecko mieszka, instytucja do której dziecko	dane dotyczące: zdrowia, biometryczne, genetyczne	poczta elektroniczna Clininet MMedica PharmaNet Chazon eWUŚ	do wyboru

		uczęszcza, obywatelstwo, narodowość, nr karty Polaka, dane wojskowe, numer noworodka, stopień pokrewieństwa opiekuna			
11.	darczyńcy	imię, nazwisko, nazwa przedsiębiorcy, adres, adres poczty elektronicznej, nr: PESEL, NIP, REGON, KRS.		poczta elektroniczna	do wyboru
12.	osoby objęte monitoringiem wizyjnym	wizerunek		system monitoringu wizyjnego	do wyboru

załącznik nr 2.

KLAUZULE:

Klauzula informacyjna dla kandydatów do pracy i ich zgoda

treść klauzuli	podanie do wiadomości
Część informacyjna klauzuli Zgodnie z art. 13. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, Zarząd Spółki PCZ informuje: **1.** Administratorem Danych Osobowych pozyskanych od kandydatów do pracy jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach (99-200) ul. Mickiewicza nr 16. (dalej Administratorem). **2.** Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. **3.** Dane osobowe kandydata do pracy przetwarzane będą dla potrzeb aktualnej i przyszłej rekrutacji - na podstawie art. 6. ust. 1. lit. a) RODO oraz Kodeksu Pracy i przez ten okres przechowywane. **4.** Dane osobowe kandydata do pracy będą mogły być udostępnione wyłącznie podmiotom uprawnionym na podstawie odrębnych przepisów prawa, a także podmiotom, z którymi Administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcom świadczącym usługę z zakresu ochrony danych osobowych, serwisantom). **5.** Kandydatowi do pracy przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2. RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego. **6.** Podanie danych osobowych jest obligatoryjne w oparciu o przepisy prawa, a w pozostałym zakresie jest dobrowolne. Konsekwencją niepodania danych osobowych lub cofnięcia zgody na ich przetwarzanie będzie brak możliwości przeprowadzenia rekrutacji. **7.** Dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania i nie będą przekazywane do państw trzecich. **Oświadczenie kandydata do pracy w Poddębickim Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach** - zgodnie z art. 6. ust.1. lit. a) RODO wyrażam zgodę na przetwarzanie moich danych osobowych na potrzeby aktualnej i przyszłych rekrutacji.	• *strona www.nzozpcz.pl,* • *kwestionariusz osobowy kandydata do pracy,* *z potwierdzeniem przyjęcia do wiadomości*

Klauzula informacyjna dla pracowników

treść klauzuli	podanie do wiadomości
Zgodnie z art. 13. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, Zarząd Spółki PCZ informuje: **1.** Administratorem Danych Osobowych pozyskanych od pracownika jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach (99-200) ul. Mickiewicza nr 16. (dalej Administratorem). **2.** Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. **3.** Przetwarzanie danych osobowych jest niezbędne dla wypełniania szczególnych obowiązków wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora, działającego na podstawie przepisu art. 9. ust. 2. lit. b) RODO w związku z przepisami w szczególności: prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, w zakresie, między innymi: **1)** zatrudnienia, zapewnienia bezpieczeństwa pracy i mienia, monitoringu systemów informatycznych; **2)** zapewnienia świadczeń socjalnych; **3)** wewnętrznej identyfikacji wizualnej, kontroli dostępu do danych osobowych, kształcenia, organizacji wyjazdów służbowych. **4.** Dane osobowe pracownika będą mogły być udostępniane wyłącznie podmiotom uprawnionym na podstawie odrębnych przepisów prawa, a także podmiotom, z którymi Administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcom świadczącym usługę z zakresu ochrony danych osobowych, serwisantom). **5.** Dane osobowe będą przechowywane na podstawie Kodeksu Pracy przez okres 10 lat licząc od końca roku kalendarzowego, w którym ustał stosunek pracy, a w pozostałych przypadkach do ustania przyczyn analitycznych, statystycznych oraz do momentu skutecznego odwołania zgody. **6.** Pracownikowi przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2. RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego. **7.** Podanie danych osobowych jest obligatoryjne w oparciu o przepisy prawa, a w pozostałym zakresie jest dobrowolne. Konsekwencją niepodania danych osobowych lub cofnięcia zgody na ich przetwarzanie może być brak możliwości kontynuowania umowy o pracę. **8.** Dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania i nie będą przekazywane do państw trzecich.	• *strona www.nzozpcz.pl,* • *kwestionariusz osobowy pracownika, z potwierdzeniem przyjęcia do wiadomości*

Zgoda na publikację w mediach (na stronie www i w facebooku) wizerunku pracownika i osoby wykonującej zadania na rzecz Spółki PCZ na podstawie umowy cywilno-prawnej

treść zgody	podanie do wiadomości
Zgodnie z art. 6. ust. 1. lit. a) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, wyrażam zgodę na przetwarzanie moich danych osobowych wizerunkowych do celów kontaktowych* i/lub budowania w przestrzeni publicznej i/lub w mediach pozytywnego wizerunku Administratora*. Administrator (Poddębickie Centrum Zdrowia Spółka z o.o. z siedzibą w Poddębicach ul. Mickiewicza nr 16., kod pocztowy 99-200) wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. Osobie wyrażającej powyższą zgodę przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2. RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego. Podanie danych osobowych jest dobrowolne. Cofnięcie zgody na przetwarzanie danych osobowych będzie równoznaczne z cofnięciem zgody na publikację wizerunku pracownika w mediach (na www i na facebooku). Poddębice, dnia .... *czytelny podpis* * *niepotrzebne skreślić*	• *akta osobowe pracownika* • *dokumentacja osoby wykonującej zadania na rzecz Spółki PCZ na podstawie umowy cywilno-prawnej*

Klauzula informacyjna dla osób wykonujących zadania na podstawie umowy cywilno-prawnej

treść klauzuli	podanie do wiadomości
Zgodnie z art. 13. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, Zarząd Spółki PCZ informuje: **1.** Administratorem Danych Osobowych pozyskanych od osoby realizującej umowę jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach (99-200) ul. Mickiewicza nr 16. (dalej Administratorem). **2.** Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej:*sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. **3.** Na podstawie art. 6. ust. 1. lit. b) RODO dane osobowe przetwarzane będą w celu realizacji umowy. **4.** Dane osobowe będą mogły być udostępnione wyłącznie podmiotom uprawniony na podstawie odrębnych przepisów prawa, a także podmiotom, z którymi Administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcom świadczącym usługę z zakresu ochrony danych osobowych, serwisantom). **5.** Dane osobowe przechowywane będą przez okres przewidziany w przepisach powszechnie obowiązujących. **6.** Osobie realizującej umowę przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2. RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego. **7.** Podanie danych osobowych jest obligatoryjne w oparciu o przepisy prawa, a w pozostałym zakresie jest dobrowolne. Konsekwencją niepodania danych osobowych lub cofnięcia zgody na ich przetwarzanie będzie brak możliwości zawarcia umowy lub jej rozwiązanie. **8.** Dane osobowe nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania i nie będą przekazywane do państw trzecich.	•*ogłoszenie o konkursie* • *umowa* •*oświadczenie zleceniobiorcy*

Klauzula informacyjna dla pacjentów

treść klauzuli	podanie do wiadomości
Zgodnie z art. 13. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, Zarząd Spółki PCZ informuje: 1. Administratorem Danych Osobowych pacjentów i ich przedstawicieli ustawowych oraz osób przez nich upoważnionych jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach (99-200) ul. Mickiewicza nr 16. (dalej Administratorem). 2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można się kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*. 3. Na podstawie art. 6. ust. 1. lit. c) oraz na podstawie art. 9. ust.1. lit. h) RODO dane osobowe przetwarzane będą w celu udzielania świadczeń zdrowotnych. 4. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich pozyskiwania na podstawie odrębnych przepisów prawa. 5. Dane osobowe przechowywane będą przez okres zakreślony przepisami prawa. 6. Pacjentom i ich przedstawicielom ustawowym oraz osobom przez nich upoważnionych przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2 RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; wniesienia skargi do organu nadzorczego. 7. Dane osobowe nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania i nie będą przekazywane do państw trzecich. 8. Podanie danych osobowych jest obligatoryjne na mocy przepisów prawa.	• *strona www.nzozpcz.pl,* • *wypis ze szpitala,* • *w siedzibie Administratora na tablicy ogłoszeń w: recepcji, rejestracjach, oddziałach*

Klauzula informacyjna dla monitoringu

treść klauzuli	podanie do wiadomości
Ikonka z informacją „Obiekt monitorowany" Zgodnie z art. 13. 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, dalej RODO, Zarząd Spółki PCZ informuje: 1. Administratorem Danych Osobowych pozyskanych z systemu monitoringu wizyjnego jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach ul. Mickiewicza nr 16. 2. Kontakt z Inspektorem Ochrony Danych - e-mail: sekretariat@nzozpcz.pl; lub na adres pocztowy Administratora Danych Osobowych. 3. Podstawą prawną przetwarzania danych osobowych jest art. 6. ust. 1. lit c), a prawnie uzasadnionym interesem jest bezpieczeństwo osób, mienia oraz dobre imię Administratora Danych Osobowych. 4. Monitoring wizyjny obejmuje wszystkie obiekty zarządzane przez Poddębickie Centrum Zdrowia Spółkę z o.o. 5. Zapisy z monitoringu będą przechowywane przez Administratora Danych Osobowych przez okres 14 dni. 6. Osoba zarejestrowana przez system monitoringu ma prawo do dostępu do swoich danych osobowych oraz do żądania ograniczenia ich przetwarzania. 7. W uzasadnionych przypadkach osobie zarejestrowanej przez system monitoringu przysługuje prawo wniesienia skargi do organu nadzorczego.	*wywieszki przy wejściach na teren obiektu monitorowanego*

Klauzula informacyjna dla darczyńców

treść klauzuli	podanie do wiadomości
Zgodnie z art. 13. oraz 14. Rozporządzenie Parlamentu Europejskiego 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, dalej RODO, Zarząd Spółki PCZ informuje: 1. Administratorem Danych Osobowych pozyskanych od darczyńcy jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach ul. Mickiewicza nr 16. (dalej Administratorem). 2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. 3. Na podstawie art. 6. ust. 1. lit. e) RODO dane osobowe będą przetwarzane w celu wykonania zadania realizowanego przez Administratora w interesie publicznym oraz w korespondencji adresowanej do darczyńcy. 4. Dane osobowe będą mogły być udostępnione wyłącznie podmiotom uprawnionym do uzyskania danych osobowych na podstawie odrębnych przepisów prawa, a także podmiotom, z którymi Administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcom świadczącym usługę z zakresu ochrony danych osobowych, serwisantom). 5. Dane osobowe przechowywane będą przez okres niezbędny do realizacji umowy darowizny, zakreślony przepisami prawa obowiązującymi w tym zakresie. 6. Darczyńcy przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2 RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego. 7. Dane osobowe nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania i nie będą przekazywane do państw trzecich.	*w korespondencji do darczyńcy*

Klauzula informacyjna dla oferentów w postepowaniach o udzielenie zamówienia publicznego

treść klauzuli	podanie do wiadomości
Zgodnie z art. 13. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, Zarząd Spółki PCZ informuje: **1.** Administratorem Danych Osobowych pozyskanych od uczestnika postępowania o udzielenie zamówienia publicznego jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach (99-200) ul. Mickiewicza nr 16. (dalej Administrator). **2.** Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej:*sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. **3.** Dane osobowe przetwarzane będą na podstawie art. 6. ust. 1. lit. c) RODO w celu prowadzenia postępowaniem o udzielenie zamówienia publicznego *(tu dane identyfikujące np.: nazwa, numer/ prowadzonym w trybie*). **4.** Dane osobowe będą mogły być udostępnione wyłącznie podmiotom uprawnionym do uzyskania danych osobowych na podstawie odrębnych przepisów prawa; w tym na podstawie ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (dalej ustawa Pzp), a także podmioty, z którymi Administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcom świadczącym usługę z zakresu ochrony danych osobowych, serwisantom). **5.** Dane osobowe będą przechowywane, zgodnie z przepisami ustawy Pzp, przez okres 4 lat licząc od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania liczy się od dnia zakończenia czas trwania umowy. **6.** Obowiązek podania przez uczestnika postępowania danych osobowych bezpośrednio go dotyczących jest wymogiem ustawowym określonym przepisami ustawy Pzp. Konsekwencje niepodania określonych danych wynikają wprost z ustawy Pzp. **7.** Uczestnikowi postępowania przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2. RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego. **8.** Dane osobowe nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania i nie będą przekazywane do państw trzecich.	*informacja w:* •*ogłoszeniu o postepowaniu;* •*SIWZ;* •*umowie*

Klauzula informacyjna dla oferentów w postepowaniach konkursowych przeprowadzanych na podstawie ustawy o działalności leczniczej

treść klauzuli	podanie do wiadomości
Zgodnie z art. 13. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, Zarząd Spółki PCZ informuje: **1.** Administratorem Danych Osobowych pozyskanych od uczestnika postępowania konkursowego jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach (99-200) ul. Mickiewicza nr 16. (dalej Administratorem). **2.** Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. **3.** Dane osobowe będą przetwarzane na podstawie art. 6. ust. 1. lit. c. i e.) RODO w celu przeprowadzenia postępowania konkursowego oraz przepisów ustawy o działalności leczniczej. **4.** Dane osobowe będą mogły być udostępnione podmiotom uprawnionym do ich uzyskania danych na podstawie odrębnych przepisów prawa, a także podmiotom, z którymi Administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcom świadczącym usługę z zakresu ochrony danych osobowych, serwisantom). **5.** Dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania i nie będą przekazywane do państw trzecich. **6.** Dane osobowe będą przechowywane przez okres 5 lat licząc od dnia zakończenia postępowania konkursowego. **7.** Obowiązek podania danych jest wymogiem związanym z udziałem w postępowaniu konkursowym. Konsekwencją niepodania danych określonych w formularzu ofertowym i w załącznikach do niego, będzie odrzucenie oferty. **8.** Uczestnikowi postępowania konkursowego przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2. RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego.	*informacja w* • *ogłoszeniu o postepowaniu,* • *SWKO,* • *umowie*

Klauzula informacyjna dla pracowników składających wnioski do Komisji Socjalnej

treść klauzuli	podanie do wiadomości
Zgodnie z art. 13. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, Zarząd Spółki PCZ informuje: **1.** Administratorem Danych Osobowych pozyskanych od pracownika wnoszącego wniosek do Komisji Socjalnej jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach (99-200) ul. Mickiewicza nr 16. (dalej Administratorem). **2.** Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. **3.** Na podstawie art. 6. ust. 1. lit. b) RODO dane osobowe przetwarzane będą w celu realizacji złożonego wniosku. **4.** Dane osobowe będą mogły być udostępnione podmiotom uprawnionym do ich uzyskania na podstawie odrębnych przepisów prawa, a także podmiotom, z którymi Administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcom świadczącym usługę z zakresu ochrony danych osobowych, serwisantom). **5.** Dane osobowe przechowywane będą przez okres przewidziany w przepisach odrębnych, w tym dotyczących dokumentacji pracowniczej. **6.** Osobie składającej wniosek przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2. RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego. **7.** Podanie danych osobowych jest dobrowolne, jednakże odmowa podania danych lub cofnięcie zgody na ich przetwarzanie skutkować będzie odmową rozpatrzenia wniosku. **8.** Dane osobowe nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania i nie będą przekazywane do państw trzecich.	*we wniosku wnoszonym do Komisji Socjalnej*

Klauzula informacyjna dla formularza kontaktowego na stronie www

treść klauzuli	podanie do wiadomości
Zgodnie z art. 13. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, Zarząd Poddębickiego Centrum Zdrowia Spółki z o.o. z siedzibą w Poddębicach informuje: **1.** Administratorem Danych Osobowych jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach (99-200) ul. Mickiewicza nr 16. (dalej Administratorem). **2.** Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. **3.** Przysługuje Państwu prawo żądania od Administratora: dostępu, w jego siedzibie, do swoich danych osobowych; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2. RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego. **4.** Więcej informacji można znaleźć na stronie www. nzozpcz.pl w zakładce „o nas”	*strona www.nzozpcz.pl*

Klauzula informacyjna dla osób składających oświadczenie dla celów: płacowych, ubezpieczeniowych i podatkowych

treść klauzuli	podanie do wiadomości
Zgodnie z art. 13. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, Zarząd Spółki PCZ informuje: **1.** Administratorem Danych Osobowych pozyskanych od pracownika wnoszącego wniosek do Komisji Socjalnej jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach (99-200) ul. Mickiewicza nr 16. (dalej Administratorem). **2.** Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. **3.** Na podstawie art. 6. ust. 1. lit. b) RODO dane osobowe przetwarzane będą w celu realizacji złożonego oświadczenia. **4.** Dane osobowe będą mogły być udostępnione podmiotom uprawnionym do ich uzyskania na podstawie odrębnych przepisów prawa, a także podmiotom, z którymi Administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcom świadczącym usługę z zakresu ochrony danych osobowych, serwisantom). **5.** Dane osobowe przechowywane będą przez okres przewidziany w przepisach odrębnych, w tym w szczególności Kodeksu Pracy, Kodeksu Cywilnego oraz dotyczących spraw podatkowych, ubezpieczeń społecznych. **6.** Osobie składającej oświadczenie przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2. RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego. **7.** Podanie danych osobowych jest dobrowolne, jednakże odmowa podania danych lub cofnięcie zgody na ich przetwarzanie skutkować będzie odmową rozpatrzenia składanego oświadczenia. **8.** Dane osobowe nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania i nie będą przekazywane do państw trzecich.	*akta osobowe pracowników, zleceniobiorców*

Klauzula informacyjna dla osób składających skargi lub wnioski

treść klauzuli	podanie do wiadomości
Zgodnie z art. 13. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119. z 4 maja 2016 r.), dalej RODO, Zarząd Spółki PCZ informuje: **1.** Administratorem Danych Osobowych osoby wnoszącej skargę lub wniosek jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach (99-200) ul. Mickiewicza nr 16. (dalej Administratorem). **2.** Administrator wyznaczył Inspektora Ochrony Danych, z którym można kontaktować się za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*, w sprawach przetwarzania Państwa danych osobowych. **3.** Na podstawie art. 6. ust. 1. lit. b) RODO dane osobowe przetwarzane będą w celu rozpatrzenia skargi lub wniosku. **4.** Dane osobowe będą mogły być udostępnione podmiotom uprawnionym do ich uzyskania na podstawie odrębnych przepisów prawa, a także podmiotom, z którymi Administrator zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcom świadczącym usługę z zakresu ochrony danych osobowych, serwisantom). **5.** Dane osobowe przechowywane będą przez okres przewidziany w przepisach odrębnych, w tym w szczególności dotyczących archiwizowania dokumentacji i brakowania dokumentacji niearchiwalnej. **6.** Osobie składającej oświadczenie przysługuje prawo żądania od Administratora: uzyskania w jego siedzibie kopii swoich danych osobowych; dostępu do nich; ich sprostowania, usunięcia lub ograniczenia przetwarzania z zastrzeżeniem przypadków, o których mowa w art. 18. ust. 2. RODO; wniesienia sprzeciwu wobec przetwarzania; przenoszenia danych; cofnięcia w dowolnym momencie zgody na ich przetwarzanie; wniesienia skargi do organu nadzorczego. **7.** Podanie danych osobowych jest dobrowolne, jednakże odmowa podania danych lub cofnięcie zgody na ich przetwarzanie skutkować będzie odmową rozpatrzenia składanej skargi lub wniosku. **8.** Dane osobowe nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania i nie będą przekazywane do państw trzecich.	*w pierwszej korespondencji kierowanej do skarżącego lub wnioskodawcy* *w dokumentacji dotyczącej skargi lub wniosku*

załącznik nr 3.

załącznik nr do umowy nr .....zawartej w dniu .....

UMOWA nr

POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w Poddębicach w dniu .....

stanowiąca uzupełnienie Umowy zawartej w dniu ..... na

.....

..... , zwanej dalej Umową Główną.

Niniejsza Umowa została zawarta pomiędzy:

Poddębickim Centrum Zdrowia Spółką z o. o., z siedzibą w Poddębicach, ul. Mickiewicza nr 16., zarejestrowanym w Sądzie Rejonowym dla Łodzi Śródmieścia XX Wydział Gospodarczy, pod numerem KRS: 0000384815, posiadającym NIP: 828 140 92 38 oraz REGON: 101075971, zwaną dalej **Administratorem**, reprezentowaną przez:

Prezesa/Wiceprezesa Zarządu -

a

, zwanym/ą

dalej **Podmiotem Przetwarzającym, reprezentowanym/ą przez:**

łącznie zwanymi **Stronami**, a każdy z osobna **Stroną**.

Mając na uwadze to, że:

1. od dnia ..... Strony wiąże Umowa Główna, w trakcie której przetwarzane są systematycznie:
2. dane osobowe pacjentów (imię i nazwisko, data urodzenia, numer pesel, płeć, miejsce zamieszkania, nr i rodzaj dokumentu potwierdzającego tożsamość);
3. dane osobowe przedstawiciela ustawowego/faktycznego lub osoby upoważnionej do wglądu do dokumentacji medycznej pacjenta;
4. dane medyczne (rozpoznanie chorobowe, informacje lub dane niezbędne do przeprowadzania badań, konsultacji lub procesu leczenia);
5. dane personelu medycznego (imię i nazwisko, tytuł zawodowy, numer prawa wykonywania zawodu, uzyskane specjalizacje);
6. dane osobowe osób koordynujących wykonywanie Umowy Głównej i umowy niniejszej (imię i nazwisko, stanowisko, numer telefonu);
7. od dnia 25 maja 2018 r. Strony obowiązane są stosować przepisy 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, zwanego dalej RODO;

8. Administrator jest administratorem danych osobowych w rozumieniu art. 4. pkt 7. RODO

Strony zawierają niniejszą umowę, zwaną daje Umową, o następującej treści:

§ 1.

Przedmiot umowy

Administrator, w trybie art. 28. RODO, powierza Podmiotowi Przetwarzającemu przetwarzanie danych osobowych w imieniu Administratora, na zasadach określonych w Umowie oraz we właściwych przepisach regulujących przetwarzanie danych osobowych, w tym w szczególności RODO a Podmiot Przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z Umową, RODO oraz przepisami powszechnie obowiązującymi, które chronią prawa osób, których dane dotyczą.

Strony zobowiązują się wykonywać zobowiązania wynikające z umowy z najwyższą starannością, w celu prawidłowego zabezpieczenia prawnego, organizacyjnego i technicznego interesów Stron oraz osób, których dane osobowe dotyczą, w zakresie przetwarzania danych osobowych.

§ 2.

Zakres i cel przetwarzania danych osobowych

1. Podmiot Przetwarzający będzie przetwarzał dane osobowe, powierzone mu przez Administratora na podstawie niniejszej Umowy.
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot Przetwarzający wyłącznie w celu realizacji Umowy Głównej lub na podstawie odrębnych zleceń Administratora, wyrażonych w formie dokumentowej (papierowej, cyfrowej, w tym za pośrednictwem poczty elektronicznej).
3. Podmiot Przetwarzający ma prawo przetwarzać dane osobowe, jeżeli obowiązek taki nakłada na niego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot Przetwarzający. W takim przypadku Podmiot Przetwarzający jest zobowiązany poinformować Administratora o stosującym się do niego obowiązku prawnym co najmniej na 24 godziny przed rozpoczęciem przetwarzania, chyba że wiążące go przepisy zabraniają mu udzielania takiej informacji, z uwagi na ważny interes publiczny.

§ 3.

Oświadczenie Podmiotu Przetwarzającego

Podmiot Przetwarzający oświadcza, że:

1. wdrożył środki techniczne i organizacyjne gwarantujące przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami, w sposób zapewniający ochronę praw osób, których dotyczą dane osobowe;
2. dysponuje środkami, doświadczeniem, wiedzą oraz odpowiednio wyszkolonym personelem, umożliwiającymi prawidłowe przetwarzanie danych osobowych w zakresie i w celu określonych w Umowie.

§ 4.

Obowiązki Podmiotu Przetwarzającego w związku z przetwarzaniem danych osobowych

1. Podmiot Przetwarzający prowadzi rejestr czynności przetwarzania danych osobowych, zawierający informacje wymagane przez obowiązujące przepisy, chyba że zgodnie z obowiązującymi przepisami nie ma obowiązku prowadzenia takiego rejestru.
2. Podmiot Przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora zgodnie z art. 30. ust. 2 RODO chyba, że zgodnie z obowiązującymi przepisami nie ma obowiązku prowadzenia takiego rejestru.
3. Wszelkie zlecane przez Administratora operacje przetwarzania danych osobowych Podmiot Przetwarzający wykonuje niezwłocznie, w szczególności jeśli chodzi o usunięcie danych osobowych na żądanie osoby, której dotyczą.
4. Biorąc pod uwagę charakter przetwarzania danych osobowych, Podmiot Przetwarzający ma obowiązek współdziałania z Administratorem w celu wywiązania się z obowiązku odpowiadania na żądania osoby, której dane osobowe dotyczą, w zakresie wykonywania jej praw określonych w obowiązujących przepisach, wdrażając odpowiednie środki techniczne i organizacyjne.
5. Podmiot Przetwarzający zapewni, że osoby, które będą zaangażowane w czynności przetwarzania danych osobowych w ramach jego organizacji:
   1) otrzymają pisemne upoważnienia do przetwarzania danych osobowych;
   2) zostaną zaznajomione z obowiązującymi przepisami o ochronie danych osobowych (z uwzględnieniem ich każdorazowych zmian) oraz z odpowiedzialnością za ich nieprzestrzeganie;
   3) będą dokonywały czynności przetwarzania danych osobowych wyłącznie na

polecenie Podmiotu Przetwarzającego;

4) zobowiążą się do bezterminowego zachowania w tajemnicy danych osobowych oraz stosowanych przez Podmiot Przetwarzający sposobów ich zabezpieczenia, o ile taki obowiązek nie wynika dla nich z przepisów odrębnych.

6. Podmiot Przetwarzający prowadzi ewidencję udzielonych upoważnień do przetwarzania danych osobowych.

§ 5.

Dalsze powierzenia przetwarzania

1. Podmiot Przetwarzający ma prawo korzystać z podwykonawców przy przetwarzaniu danych osobowych (dalsze powierzenie przetwarzania), pod warunkiem, że przed powierzeniem podwykonawcy przetwarzania danych osobowych:
   1) uzyska na to zgodę Administratora, wyrażoną w formie dokumentowej (papierowej lub cyfrowej, w tym za pośrednictwem poczty elektronicznej);
   2) zawrze z podwykonawcą umowę powierzenia przetwarzania danych osobowych na warunkach nie gorszych niż warunki niniejszej Umowy;
   3) upewni się, że podwykonawca zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom obowiązujących przepisów.
2. Jeżeli podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, Podmiot Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za wypełnienie obowiązków podwykonawcy.
3. Wykaz podwykonawców, z których usług Podmiot Przetwarzający korzysta w dniu zawarcia niniejszej Umowy, i co do których Administrator wyraża zgodę na dalsze powierzenie przetwarzania danych osobowych, zostanie przedłożony Administratorowi w dniu podpisania niniejszej Umowy.

§ 6.

Bezpieczeństwo danych osobowych

1. Podmiot Przetwarzający stosuje środki techniczne i organizacyjne, odpowiednie do zagrożeń oraz charakteru, zakresu, kontekstu i celu przetwarzania danych osobowych, zapewniające bezpieczeństwo danych osobowych, w szczególności przed ich przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem.
2. Podmiot Przetwarzający zobowiązuje się stale monitorować stan stosowanych zabezpieczeń danych osobowych oraz występujących zagrożeń bezpieczeństwa,

i w razie potrzeby aktualizuje stosowane środki techniczne i organizacyjne, tak, żeby zapewnić najwyższy osiągalny poziom ochrony danych osobowych.

3. Podmiot Przetwarzający, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, ma obowiązek współdziałania z Administratorem w wywiązaniu się z obowiązków określonych w art. 32.-36. RODO.
4. Podmiot Przetwarzający niezwłocznie zawiadamia Administratora, przed podjęciem jakichkolwiek działań, o każdym przypadku:
   1) wystąpienia jakiegokolwiek organu z żądaniem udostępnienia danych osobowych, chyba że zakaz ujawnienia tej informacji wynika z obowiązujących przepisów;
   2) wystąpienia przez osobę, której dane osobowe dotyczą, z żądaniem dotyczącym przetwarzania danych osobowych lub ich treści.
5. Podmiot Przetwarzający niezwłocznie - w każdym wypadku nie później niż w ciągu 24 godzin od wykrycia - informuje Administratora o wszelkich wykrytych naruszeniach bezpieczeństwa danych osobowych, przekazując Administratorowi wszelkie dostępne Podmiotowi Przetwarzającemu informacje na temat naruszenia, w szczególności:
   1) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane osobowe dotyczą, oraz kategorie i przybliżoną liczbę wpisów, których dotyczy naruszenie;
   2) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   3) możliwe konsekwencje naruszenia ochrony danych osobowych; oraz
   4) środki zastosowane lub proponowane przez Podmiot Przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Podmiot Przetwarzający współdziała z Administratorem przy ustalaniu szczegółów związanych ze zgłoszonym Administratorowi naruszeniem, w szczególności przyczyn i skutków jego wystąpienia oraz wdraża zalecane przez Administratora środki mające na celu złagodzenie ewentualnych niekorzystnych skutków naruszenia danych osobowych oraz środki naprawcze.
7. Podmiot Przetwarzający niezwłocznie informuje Administratora, jeśli jego zdaniem wydane mu przez Administratora polecenie dotyczące przetwarzania danych osobowych stanowi naruszenie obowiązujących przepisów.

§ 7.

Prawo do kontroli

1. Administrator ma prawo kontrolowania sposobu wypełniania przez Podmiot Przetwarzający jego obowiązków określonych w umowie lub w obowiązujących przepisach. W szczególności Administrator może żądać udostępnienia określonych informacji lub dokumentów oraz może przeprowadzać - samodzielnie lub przez upoważnionego przez Administratora pracownika lub współpracownika - audyty, w tym inspekcje w miejscu przetwarzania danych osobowych przez Podmiot Przetwarzający.
2. Podmiot Przetwarzający ma obowiązek współpracować z Administratorem lub upoważnionym przez Administratora pracownikiem lub współpracownikiem w czasie przeprowadzanej kontroli, w sposób umożliwiający Administratorowi weryfikację prawidłowej realizacji obowiązków Podmiotu Przetwarzającego.

§ 8.

Czas obowiązywania i rozwiązanie niniejszej Umowy

1. Umowa niniejsza wchodzi w życie z dniem jej podpisania i zostaje zawarta na czas określony do dnia rozwiązania lub wygaśnięcia Umowy Głównej, z realizacji której wynika konieczność przetwarzania danych osobowych przez Podmiot Przetwarzający.
2. W przypadku stwierdzenia naruszenia przez Podmiot Przetwarzający obowiązków wynikających z umowy, Administrator ma prawo rozwiązać Umowę Główną, ze skutkiem natychmiastowym.
3. Najpóźniej w dniu rozwiązania umowy Podmiot Przetwarzający ma obowiązek:
   1) usunąć wszelkie powierzone mu do przetwarzania dane osobowe;
   2) zwrócić Administratorowi wszelkie nośniki zawierające dane osobowe oraz usunąć wszelkie istniejące kopie danych osobowych, chyba że obowiązujące przepisy wymagają od niego dalszego przechowywania części lub całości danych osobowych.
4. W przypadku rozwiązania Umowy w trybie ust. 2. wybór Administratora będzie zakomunikowany Podmiotowi Przetwarzającemu w oświadczeniu o rozwiązaniu umowy ze skutkiem natychmiastowym.
5. Czynności wskazane w ust. 3. zostaną wykazane w pisemnym protokole, podpisanym przez przedstawiciela Podmiotu Przetwarzającego i dostarczonym Administratorowi w terminie 7 dni od dokonania wskazanych w nim czynności.

§ 9.

Postanowienia końcowe

1. Podmiotowi Przetwarzającemu nie przysługuje wynagrodzenie za wykonywanie niniejszej Umowy.
2. Umowa niniejsza stanowi całość porozumienia pomiędzy Stronami i zastępuje w całości uprzednie lub równoczesne uzgodnienia poczynione przez Strony (w formie pisemnej lub ustnej) w przedmiocie regulowanym postanowieniami niniejszej Umowy.
3. Wszelkie spory między Stronami będą rozwiązywane na zasadzie polubownych negocjacji. W przypadku nieosiągnięcia przez Strony porozumienia, spór zostanie przekazany do rozstrzygnięcia sądowi powszechnemu właściwemu dla siedziby Administratora.
4. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
5. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Podmiot Przetwarzający **Administrator**

załącznik nr 4.

Wzory:

upoważnienia do przetwarzania danych osobowych, cofnięcia upoważnienia do przetwarzania danych osobowych, oświadczenia o poufności

Poddębice,

UPOWAŻNIENIE nr

do przetwarzania danych osobowych

W celu zapewnienia realizacji postanowień 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 (RODO), Administrator Danych Osobowych - Poddębickie Centrum Zdrowia Spółka z o.o. z siedzibą w Poddębicach (Spółka PCZ) działając na podstawie Polityki Ochrony Danych Osobowych, upoważnia Panią/a

imię:

nazwisko:

stanowisko:

komórka organizacyjna:

do przetwarzania danych osobowych, których w rozumieniu art. 4. pkt 7. RODO jest Administratorem lub które zostały powierzone Spółce PCZ do przetwarzania.

Upoważnienie dotyczy przetwarzania danych osobowych w postaci papierowej oraz w ramach nadanych dostępów do systemów informatycznych służących do przetwarzania danych osobowych w zakresie zgodnym z zakresem realizowanych świadczeń.

Upoważnienie ważne jest od dnia do

.....

pieczątka i podpis członka Zarządu Spółki PCZ

Potwierdzam otrzymanie Upoważnienia wraz z obowiązującymi w Spółce PCZ „Zasadami Przetwarzania Danych Osobowych".

Poddębice,

załącznik do „Upoważnienia do przetwarzania danych osobowych" nr

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

W celu zapewnienia prawidłowego wykonywania udzielonego „Upoważnienia do przetwarzania danych osobowych" oraz prawidłowego realizowania postanowień 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/W, zwanego dalej RODO, osoba której udzielono upoważnienia obowiązana jest stosować poniższe zasady. Osoba upoważniona:

1. obowiązana jest zapoznać się z „Polityką Ochrony Danych Osobowych" obowiązującą w Poddębickim Centrum Zdrowia Spółce z o.o. (Spółce PCZ) i bezwzględnie przestrzegać jej postanowień oraz przepisów prawa powszechnie obowiązującego w zakresie ochrony danych osobowych;
2. przetwarza dane osobowe pacjentów Spółki PCZ poprzez wgląd do dokumentacji medycznej i/lub edycję danych tylko tych, których przetwarzanie jest niezbędne do realizacji powierzonych jej zadań służbowych;
3. nie ma uprawnień do przetwarzania danych osobowych pacjentów w innym celu niż wskazanym powyżej w pkt. 2.;
4. nie ma uprawnień do przetwarzania danych innych osób, niż wskazanych powyżej w pkt. 2.;
5. nie ma uprawnień do udostępniania przetwarzanych danych osobowych innym nieupoważnionych osobom/podmiotom, w tym poprzez:
   1) umożliwienie wglądu do danych,
   2) weryfikację danych,
   3) usunięcie danych z dokumentacji,
   4) dalsze powierzenie przetwarzania danych,
   5) ustne przekazanie informacji o danych,
   6) przekazanie informacji o danych na nośnikach elektronicznych,
   7) upublicznienie danych;
6. nie ma uprawnień do wykonywania nieuzasadnionych, wykonywaniem zadań służbowych, kopii, gromadzenia, przechowywania jakichkolwiek danych osobowych.

Przetwarzanie danych osobowych będzie odbywało się w siedzibie Spółki PCZ z wykorzystaniem materiałów oraz infrastruktury (w tym: urządzeń, sprzętu i aparatury medycznej, sprzętu i systemu teleinformatycznego) należących do Spółki PCZ.
W przypadku naruszenia zasad bezpieczeństwa w zakresie poufności lub integralności danych osobowych osoba upoważniona do ich przetwarzania obowiązana jest podjąć stosowne działania odpowiednie dla zaistniałego incydentu i zgłoszenia go bezpośredniemu zwierzchnikowi służbowemu lub Działowi Informatyzacji i Baz Danych.

Przyjęłam/przyjąłem do wiadomości
Poddębice,

.....
podpis osoby upoważnionej

„COFNIĘCIE UPOWAŻNIENIA" nr

do przetwarzania danych osobowych

w Poddębickim Centrum Zdrowia Spółce z o.o. z siedzibą w Poddębicach (Spółce PCZ)

Działając na podstawie „Polityki ochrony danych osobowych", w celu zapewnienia realizacji postanowień Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, (dalej RODO), Administrator Danych Osobowych **z dniem cofa Panu/ni uprawnienia do przetwarzania danych osobowych, których Administratorem w rozumieniu art. 4. pkt 7. RODO jest Spółka PCZ, lub które zostały jej powierzone, a nadane Mu/Jej upoważnieniem nr z dnia**

Cofnięcie uprawnień dotyczy przetwarzania danych osobowych w postaci papierowej oraz w ramach nadanych dostępów do systemów informatycznych służących do przetwarzania danych osobowych w zakresie zgodnym z zakresem powierzonych czynności służbowych.

Poddębice,

.....

podpis i pieczątka
Administratora Danych Osobowych

potwierdzam otrzymanie niniejszego cofnięcia upoważnienia

.....

data, czytelny podpis osoby, której cofnięto upoważnienie

Oświadczenie o poufności, złożone przez osobę, której udzielono upoważnienia do przetwarzania danych osobowych

załącznik do „Upoważnienia do przetwarzania danych osobowych" nr

imię:
nazwisko:
stanowisko:
komórka organizacyjna:

OŚWIADCZENIE

o zachowaniu w poufności danych osobowych

W związku z wydanym mi przez Administratora Danych Osobowych (Poddębickie Centrum Zdrowia Spółkę z o.o. z siedzibą w Poddębicach) upoważnieniem do przetwarzania danych osobowych oświadczam, że:

1. Zapoznałam/łem się:
   1) z przepisami 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, zwanego dalej RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
   2) z obowiązującymi u Administratora Danych Osobowych przepisami wewnętrznymi dotyczącymi przetwarzania danych osobowych, w tym w szczególności z „Polityką ochrony danych osobowych"

   i zobowiązuję się do przestrzegania obowiązków wynikających z tych przepisów.
2. Zapewnię bezpieczeństwo przetwarzanych danych osobowych poprzez ich ochronę przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem.
3. Zachowam w tajemnicy dane osobowe oraz sposoby ich zabezpieczeń, do których uzyskam dostęp w trakcie współpracy z Administratorem Danych Osobowych, tak w trakcie łączącego mnie z nim stosunku prawnego, jak i po jego zakończeniu.
4. Będę wykonywać polecenia Inspektora Ochrony Danych oraz innych przedstawicieli Administratora Danych Osobowych odpowiedzialnych za bezpieczeństwo danych osobowych, które będą związane z zachowaniem bezpieczeństwa danych osobowych i sposobów ich zabezpieczenia w poufności.
5. W razie uzyskania nieuprawnionego dostępu do danych osobowych lub wykrycia incydentu godzącego w bezpieczeństwo danych osobowych, zobowiązuję się powiadomić o tym bezpośredniego przełożonego lub Dział Informatyzacji i Baz Danych.
6. Są mi znane zasady monitorowania sposobu używania sprzętu służbowego, w tym m.in. telefonu komórkowego, komputerów, poczty elektronicznej, obowiązujące u Administratora Danych Osobowych. Zostałem poinformowany o zakresie i sposobach prowadzenia ww. monitoringu.
7. Są mi znane zasady odpowiedzialności prawnej za niezgodne z przepisami o ochronie danych osobowych przetwarzanie danych osobowych oraz mam świadomość, że za

niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać prawnie na podstawie regulacji wewnętrznych obowiązujących u Administratora Danych Osobowych, kodeksu pracy, kodeksu karnego lub kodeksu cywilnego.

Zostałam/łem poinformowana/y o tym, że:

1) Administratorem moich danych osobowych jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach, adres: ul. Mickiewicza nr 16., 99-200 Poddębice;
2) Administrator Danych Osobowych wyznaczył Inspektora Ochrony Danych, z którym mogę się kontaktować w sprawach przetwarzania moich danych osobowych za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*;
3) Administrator Danych Osobowych będzie przetwarzał moje dane w celu niezbędnym do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora, w szczególności w zakresie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;
4) moje dane osobowe są przetwarzane na podstawie przepisów prawa;
5) moje dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi Administrator Danych Osobowych zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);
6) mam prawo uzyskać kopię swoich danych osobowych w siedzibie Administratora Danych Osobowych;
7) moje dane osobowe będą przechowywane do upływu okresu przewidzianego przepisami prawa;
8) przysługuje mi prawo dostępu do treści moich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;
9) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji celu ich przetwarzania, a konsekwencją niepodania danych osobowych jest brak możliwości realizacji umowy;
10) Administrator Danych Osobowych nie podejmuje decyzji w sposób zautomatyzowany mając dostęp do moich danych osobowych.

Niniejsze oświadczenie składam w trzech jednobrzmiących egzemplarzach, dwa z nich przedkładam Administratorowi Danych Osobowych, z mocą obowiązującą od

Poddębice,

.....

podpis składającego oświadczenie

Oświadczenie o poufności, złożone przez osobę, której nie udzielono upoważnienia do przetwarzania danych osobowych

załącznik do umowy o pracę

Poddębice, dnia

imię:
nazwisko:
stanowisko:
komórka organizacyjna:

OŚWIADCZENIE
o zachowaniu w poufności danych osobowych

TREŚĆ OŚWIADCZENIA

1. Zapoznałam się:
   1) z przepisami 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, zwanego dalej RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
   2) z obowiązującymi u Administratora Danych Osobowych przepisami wewnętrznymi dotyczącymi przetwarzania danych osobowych, w tym w szczególności z „Polityką ochrony danych osobowych"

   i zobowiązuję się do przestrzegania obowiązków wynikających z tych przepisów.
2. Zachowam w tajemnicy dane osobowe oraz sposoby ich zabezpieczeń, do których uzyskam dostęp w trakcie współpracy z Administratorem Danych Osobowych, tak w trakcie łączącego mnie z nim stosunku prawnego, jak i po jego zakończeniu.
3. Będę wykonywać polecenia Inspektora Ochrony Danych oraz innych przedstawicieli Administratora Danych Osobowych odpowiedzialnych za bezpieczeństwo danych osobowych, które będą związane z zachowaniem bezpieczeństwa danych osobowych i sposobem ich zabezpieczenia w poufności.
4. W razie uzyskania nieuprawnionego dostępu do danych osobowych lub wykrycia incydentu godzącego w bezpieczeństwo danych osobowych, zobowiązuję się powiadomić o tym bezpośredniego przełożonego lub Dział Informatyzacji i Baz Danych.
5. Znane mi są zasady monitorowania sposobu używania sprzętu służbowego, w tym m.in. telefonu komórkowego, komputerów, poczty elektronicznej, obowiązujące u Administratora Danych Osobowych. Zostałem poinformowany o zakresie i sposobach prowadzenia ww. monitoringu.
6. Są mi znane zasady odpowiedzialności prawnej za niezgodne z przepisami o ochronie danych osobowych przetwarzanie danych osobowych oraz mam świadomość, że za niedopełnienie obowiązków wynikających z niniejszego oświadczenia mogę odpowiadać

prawnie na podstawie regulacji wewnętrznych obowiązujących u Administratora Danych Osobowych, kodeksu pracy, kodeksu karnego lub kodeksu cywilnego.

Zostałam/łem poinformowana/y o tym, że:

1) Administratorem moich danych osobowych jest Poddębickie Centrum Zdrowia Sp. z o.o. z siedzibą w Poddębicach, adres: ul. Mickiewicza nr 16., 99-200 Poddębice;
2) Administrator Danych Osobowych wyznaczył Inspektora Ochrony Danych, z którym mogę się kontaktować w sprawach przetwarzania moich danych osobowych za pośrednictwem poczty elektronicznej: *sekretariat@nzozpcz.pl*;
3) Administrator Danych Osobowych będzie przetwarzał moje dane w celu niezbędnym do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora, w szczególności w zakresie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;
4) moje dane osobowe są przetwarzane na podstawie przepisów prawa;
5) moje dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi Administrator Danych Osobowych zawarł umowę powierzenia przetwarzania danych w związku z realizacją usług na rzecz Administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);
6) mam prawo uzyskać kopię swoich danych osobowych w siedzibie Administratora Danych Osobowych;
7) moje dane osobowe będą przechowywane do upływu okresu przewidzianego przepisami prawa;
8) przysługuje mi prawo dostępu do treści moich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;
9) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji celu ich przetwarzania. Konsekwencją niepodania danych osobowych jest brak możliwości realizacji umowy;
10) Administrator Danych Osobowych nie podejmuje decyzji w sposób zautomatyzowany mając dostęp do moich danych osobowych.

Niniejsze oświadczenie składam w dwóch jednobrzmiących egzemplarzach, jeden z nich przedkładam Administratorowi Danych Osobowych, z mocą obowiązującą od dnia

Poddębice,

.....

podpis składającego oświadczenie

załącznik nr 5.

Informacja przekazywana przez Dział Prawno-Organizacyjny Głównemu Specjaliście ds. Informatyzacji i Baz Danych

Poddębice, dnia .....

Dział Prawno-Organizacyjny
Poddębickie Centrum Zdrowia Sp. z o.o.
Poddębice

INFORMACJA
o osobie wykonującej czynności służbowe na podstawie umowy cywilno-prawnej

W Poddębickim Centrum Zdrowia Spółce z o.o. z siedzibą w Poddębicach czynności służbowe wykonuje:

imię i nazwisko:
PESEL:
data zawarcia umowy cywilno-prawnej:
służbowe stanowisko:
jednostka/komórka organizacyjna:
nr prawa wykonywania zawodu:
tytuł zawodowy:

.....
podpis pracownika
Działu Prawno-Organizacyjnego

Potwierdzam przekazanie Działowi ds. Informatyzacji i Baz Danych Spółki PCZ „Informacji o osobie wykonującej czynności służbowe na podstawie umowy cywilno -prawnej".

Poddębice,

.....
podpis pracownika
Działu ds. Informatyzacji i Baz Danych

druga strona Informacji

Wniosek

bezpośredniego zwierzchnika osoby wykonującej czynności na podstawie umowy cywilno-prawnej

Proszę o nadanie uprawnień do dostępu do systemów informatycznych w części medycznej/administracyjnej*.

Poddębice, ...

.....

podpis zwierzchnika służbowego
osoby, której dotyczy Informacja

INFORMACJA o WYDANYM DOSTĘPIE**

ZAŁOŻENIE KONTA		
1.	*2.*	*3.*
1.	**login**	
2.	**data i godzina**	
3.	**konto założył**	
4.	**numer w ewidencji kont i wydanych dostępów**	
potwierdzam przyjęcie dostępu		
5.	**data i godzina**	
6.	**czytelny podpis**	

**niepotrzebne skreślić*

** wypełnia pracownik Działu ds. Informatyzacji i Baz Danych

Informacja przekazywana przez Dział Prawno-Organizacyjny Głównemu Specjaliście ds. Informatyzacji i Baz Danych

Poddębice, dnia .....

Dział Prawno-Organizacyjny
Poddębickie Centrum Zdrowia Sp. z o.o.
Poddębice

INFORMACJA
o osobie, której zakres wykonywanych czynności służbowych na podstawie umowy cywilno-prawnej uległ zmianie

W Poddębickim Centrum Zdrowia Spółce z o.o. z siedzibą w Poddębicach z dniem ..... uległ zmianie zakres czynności służbowych:

imię i nazwisko:
PESEL:
stanowisko służbowe zajmowane po zmianie:
jednostka/komórka organizacyjna po zmianie zakresu czynności:
nr prawa wykonywania zawodu:
tytuł zawodowy:

.....
podpis pracownika
Działu Prawno-Organizacyjnego

Potwierdzam przekazanie Działowi ds. Informatyzacji i Baz Danych Spółki PCZ „Informacji o osobie, której zakres wykonywanych czynności służbowych na podstawie umowy cywilno-prawnej uległ zmianie".

Poddębice,

.....
podpis pracownika
Działu ds. Informatyzacji i Baz Danych

INFORMACJA o ZMIANIE w KONCIE

ZMIANA UPRAWNIEŃ		
1.	*2.*	*3.*
1.	**login**	
2.	**data i godzina zmiany uprawnień**	
3.	**zmiany uprawnień dokonał**	
4.	**numer w ewidencji kont i wydanych dostępów**	
potwierdzam przyjęcie zmiany w dostępie		
5.	**data i godzina**	
6.	**czytelny podpis**	

Informacja przekazywana przez Dział Prawno-Organizacyjny Głównemu Specjaliście ds. Informatyzacji i Baz Danych

Poddębice, dnia .....

Dział Prawno-Organizacyjny
Poddębickie Centrum Zdrowia Sp. z o.o.
Poddębice

INFORMACJA
o osobie, która zaprzestała wykonywania czynności służbowych na podstawie umowy cywilno-prawnej

W Poddębickim Centrum Zdrowia Spółce z o.o. z siedzibą w Poddębicach z dniem ..... nie wykonuje czynności służbowych:

imię i nazwisko:
PESEL:
stanowisko służbowe:
jednostka/komórka organizacyjna:
nr prawa wykonywania zawodu:
tytuł zawodowy:

.....
podpis pracownika
Działu Prawno-Organizacyjnego

Potwierdzam przekazanie Działowi ds. Informatyzacji i Baz Danych Spółki PCZ „Informacji o osobie, która zaprzestała wykonywania czynności służbowych na podstawie umowy cywilno-prawnej".

Poddębice,

.....
podpis pracownika
Działu ds. Informatyzacji i Baz Danych

INFORMACJA o ZMIANIE w KONCIE

UTRATA UPRAWNIEŃ		
1.	*2.*	*3.*
1.	**login**	
2.	**data i godzina utraty uprawnień**	
3.	**utraty uprawnień dokonał**	
4.	**numer w ewidencji kont i wydanych dostępów**	
potwierdzam przyjęcie utraty dostępu		
5.	**data i godzina**	
6.	**czytelny podpis**	

Informacja przekazywana przez Dział Kadrowo-Płacowy Głównemu Specjaliście ds. Informatyzacji i Baz Danych

Poddębice, dnia .....

Dział Kadrowo-Płacowy
Poddębickie Centrum Zdrowia Sp. z o.o.
Poddębice

INFORMACJA

o osobie wykonującej czynności służbowe na podstawie umowy cywilno-prawnej

W Poddębickim Centrum Zdrowia Spółce z o.o. z siedzibą w Poddębicach czynności służbowe wykonuje:

imię i nazwisko:
PESEL:
data zawarcia umowy cywilno-prawnej:
służbowe stanowisko:
jednostka/komórka organizacyjna:
nr prawa wykonywania zawodu:
tytuł zawodowy:

.....
podpis pracownika
Działu Kadrowo-Płacowego

Potwierdzam przekazanie Działowi ds. Informatyzacji i Baz Danych Spółki PCZ „Informacji o osobie wykonującej czynności służbowe na podstawie umowy cywilno -prawnej".

Poddębice,

.....
podpis pracownika
Działu ds. Informatyzacji i Baz Danych

Wniosek

bezpośredniego zwierzchnika osoby wykonującej czynności na podstawie umowy cywilno-prawnej

Proszę o nadanie uprawnień do dostępu do systemów informatycznych w części medycznej/administracyjnej*.

Poddębice, ...

.....
podpis zwierzchnika służbowego
osoby, której dotyczy Informacja

INFORMACJA o WYDANYM DOSTĘPIE

ZAŁOŻENIE KONTA		
1.	*2.*	*3.*
1.	**login**	
2.	**data i godzina**	
3.	**konto założył**	
4.	**numer w ewidencji kont i wydanych dostępów**	
potwierdzam przyjęcie dostępu		
5.	**data i godzina**	
6.	**czytelny podpis**	

Poddębice, dnia .....

Dział Kadrowo-Płacowy
Poddębickie Centrum Zdrowia Sp. z o.o.
Poddębice

INFORMACJA

o osobie wykonującej czynności służbowe na podstawie umowy o pracę

W Poddębickim Centrum Zdrowia Spółce z o.o. z siedzibą w Poddębicach czynności służbowe wykonuje:

imię i nazwisko:
PESEL:
data zatrudnienia na podstawie umowy o pracę:
stanowisko służbowe:
jednostka/komórka organizacyjna:
nr prawa wykonywania zawodu:
tytuł zawodowy:

.....
podpis pracownika
Działu Kadrowo-Płacowego

Potwierdzam przekazanie Działowi ds. Informatyzacji i Baz Danych Spółki PCZ „Informacji o osobie wykonującej czynności służbowe na podstawie umowy o pracę".

Poddębice,

.....
podpis pracownika
Działu ds. Informatyzacji i Baz Danych

Wniosek

bezpośredniego zwierzchnika osoby wykonujących czynności służbowe na podstawie umowy o pracę

Proszę o nadanie uprawnień do dostępu do systemów informatycznych w części medycznej/administracyjnej.*

Poddębice, ...

.....

podpis zwierzchnika służbowego
osoby, której dotyczy

INFORMACJA o WYDANYM DOSTĘPIE

ZAŁOŻENIE KONTA		
1.	*2.*	*3.*
1.	**login**	
2.	**data i godzina**	
3.	**konto założył**	
4.	**numer w ewidencji kont i wydanych dostępów**	
potwierdzam przyjęcie dostępu		
5.	**data i godzina**	
6.	**czytelny podpis**	

**niepotrzebne skreślić*

Poddębice, dnia .....

Dział Kadrowo-Płacowy
Poddębickie Centrum Zdrowia Sp. z o. o.
Poddębice

INFORMACJA

o osobie, której zakres wykonywanych czynności służbowych na podstawie umowy cywilno-prawnej uległ zmianie

W Poddębickim Centrum Zdrowia Spółce z o.o. z siedzibą w Poddębicach z dniem ..... uległ zmianie zakres czynności służbowych :

imię i nazwisko:
PESEL:
stanowisko służbowe zajmowane po zmianie:
jednostka/komórka organizacyjna po zmianie zakresu czynności:
nr prawa wykonywania zawodu:
tytuł zawodowy:

.....
podpis pracownika
Działu Kadrowo-Płacowego

Potwierdzam przekazanie Działowi ds. Informatyzacji i Baz Danych Spółki PCZ „Informacji o osobie, której zakres wykonywanych czynności służbowych na podstawie umowy cywilno-prawnej uległ zmianie".

Poddębice,

.....
podpis pracownika
Działu ds. Informatyzacji i Baz Danych

INFORMACJA o ZMIANIE w KONCIE

ZMIANA UPRAWNIEŃ		
1.	*2.*	*3.*
1.	**login**	
2.	**data i godzina zmiany uprawnień**	
3.	**zmiany uprawnień dokonał**	
4.	**numer w ewidencji kont i wydanych dostępów**	
potwierdzam przyjęcie zmiany w dostępie		
5.	**data i godzina**	
6.	**czytelny podpis**	

Poddębice, dnia .....

Dział Kadrowo-Płacowy
Poddębickie Centrum Zdrowia Sp. z o.o.
Poddębice

INFORMACJA

o osobie, której zakres wykonywanych czynności służbowych na podstawie umowy o pracę uległ zmianie

W Poddębickim Centrum Zdrowia Spółce z o.o. z siedzibą w Poddębicach z dniem ..... uległ zmianie zakres czynności służbowych:

imię i nazwisko:
PESEL:
stanowisko służbowe zajmowane po zmianie:
jednostka/komórka organizacyjna po zmianie zakresu czynności:
nr prawa wykonywania zawodu:
tytuł zawodowy:

.....
podpis pracownika
Działu Kadrowo-Płacowego

Potwierdzam przekazanie Działowi ds. Informatyzacji i Baz Danych Spółki PCZ „Informacji o osobie, której zakres wykonywanych czynności służbowych na podstawie umowy o pracę uległ zmianie".

Poddębice,

.....
podpis pracownika
Działu ds. Informatyzacji i Baz Danych

INFORMACJA o ZMIANIE w KONCIE

ZMIANA UPRAWNIEŃ		
1.	*2.*	*3.*
1.	**login**	
2.	**data i godzina zmiany uprawnień**	
3.	**zmiany uprawnień dokonał**	
4.	**numer w ewidencji kont i wydanych dostępów**	
potwierdzam przyjęcie zmiany w dostępie		
5.	**data i godzina**	
6.	**czytelny podpis**	

Poddębice, dnia .....

Kadrowo-Płacowy
Poddębickie Centrum Zdrowia Sp. z o.o.
Poddębice

INFORMACJA

o osobie, która zaprzestała wykonywania czynności służbowych na podstawie umowy o pracę

W Poddębickim Centrum Zdrowia Spółce z o.o. z siedzibą w Poddębicach z dniem ..... nie wykonuje czynności służbowych:

imię i nazwisko:
PESEL:
stanowisko służbowe:
jednostka/komórka organizacyjna:
nr prawa wykonywania zawodu:
tytuł zawodowy:

.....
podpis pracownika
Działu Kadrowo-Płacowego

Potwierdzam przekazanie Działowi ds. Informatyzacji i Baz Danych Spółki PCZ „Informacji o osobie, która zaprzestała wykonywania czynności służbowych na podstawie umowy o pracę".

Poddębice,

.....
podpis pracownika
Działu ds. Informatyzacji i Baz Danych

INFORMACJA o ZMIANIE w KONCIE

UTRATA UPRAWNIEŃ		
1.	*2.*	*3.*
1.	**login**	
2.	**data i godzina utraty uprawnień**	
3.	**utraty uprawnień dokonał**	
4.	**numer w ewidencji kont i wydanych dostępów**	
potwierdzam przyjęcie utraty dostępu		
5.	**data i godzina**	
6.	**czytelny podpis**	

Poddębice, dnia .....

Dział Kadrowo-Płacowy
Poddębickie Centrum Zdrowia Sp. z o.o.
Poddębice

INFORMACJA

o osobie, która zaprzestała wykonywania czynności służbowych na podstawie umowy cywilno-prawnej

W Poddębickim Centrum Zdrowia Spółce z o.o. z siedzibą w Poddębicach z dniem ..... nie wykonuje czynności służbowych:

imię i nazwisko:
PESEL:
stanowisko służbowe:
jednostka/komórka organizacyjna:
nr prawa wykonywania zawodu:
tytuł zawodowy:

.....
podpis pracownika
Działu Kadrowo-Płacowego

Potwierdzam przekazanie Działowi ds. Informatyzacji i Baz Danych Spółki PCZ „Informacji o osobie, która zaprzestała wykonywania czynności służbowych na podstawie umowy cywilno-prawnej".

Poddębice,

.....
podpis pracownika
Działu ds. Informatyzacji i Baz Danych

INFORMACJA o ZMIANIE w KONCIE

UTRATA UPRAWNIEŃ		
1.	*2.*	*3.*
1.	**login**	
2.	**data i godzina utraty uprawnień**	
3.	**utraty uprawnień dokonał**	
4.	**numer w ewidencji kont i wydanych dostępów**	
potwierdzam przyjęcie utraty dostępu		
5.	**data i godzina**	
6.	**czytelny podpis**	

załącznik nr 6.

Wzór formularza oceny skutków:

OCENA SKUTKÓW PLANOWANYCH OPERACJI PRZETWARZANIA DLA OCHRONY DANYCH OSOBOWYCH		
I. Informacje ogólne		
Administrator danych osobowych:		
Oceniane operacje przetwarzania[i]:		[opis ocenianych operacji]
Data przeprowadzenia oceny:		data przeprowadzenia pierwszej oceny
Daty aktualizacji oceny:		data pierwszej i kolejnych aktualizacji oceny
Powód aktualizacji oceny:		powód pierwszej i kolejnych aktualizacji oceny
II. Opis planowanych operacji przetwarzania danych osobowych		
1. Uwagi ogólne		
2. Charakter przetwarzania danych osobowych[ii]		
3. Zakres przetwarzania danych osobowych[iii]		
4. Kontekst przetwarzania danych osobowych[iv]		
5. Cele przetwarzania danych osobowych[v]		
6. Podmioty uczestniczące w przetwarzaniu	**Podmioty przetwarzające dane**	
	Osoby upoważnione	
7. Okres przetwarzania		
8. Aktywa wykorzystywane do przetwarzania danych osobowych[vi]		
9. Stosowanie zatwierdzonych kodeksów postępowania[vii]		
III. Ocena niezbędności i proporcjonalności przetwarzania danych osobowych		
1. Czy dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach?[viii]		
2. Czy dane osobowe są przetwarzane zgodnie z prawem?[ix]		
3. Czy dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane?		
4. Czy okres przechowywania danych osobowych został stosownie ograniczony?		
IV. Ocena wdrożenia środków pozwalających na realizację praw podmiotów danych		
1. Czy zapewnione są odpowiednie środki, aby udzielić podmiotowi danych osobowych wszelkich wymaganych przez prawo informacji?		
2. Czy zapewnione są odpowiednie środki, aby umożliwić podmiotowi danych	**prawo dostępu do danych osobowych**	
	prawo do przenoszenia danych osobowych	
	prawo do sprostowania danych osobowych	

osobowych realizację:	**prawo do przenoszenia danych osobowych**	
	prawo do sprzeciwu	
	prawo do ograniczenia przetwarzania danych osobowych	
3. Czy ograniczono liczbę odbiorców danych osobowych? **4. Czy zapewniono odpowiednie relacje z podmiotami przetwarzającymi dane osobowe?[x]**		
5. Czy zapewniono odpowiednie zabezpieczenia przy międzynarodowym przekazywaniu danych osobowych (z uwzględnieniem stopnia ochrony występującego w państwie, do którego przekazywane są dane osobowe)?		
6. Czy przeprowadzono uprzednie konsultacje z organem nadzorczym?		
V. Zaangażowanie zainteresowanych stron		
1. Czy administrator danych dostatecznie ograniczył zidentyfikowane ryzyko? Czy środki zaplanowane są wystarczające do ograniczenia ryzyka do dopuszczalnego poziomu?		
2. Czy przetwarzanie danych odbywa się w celu wykonania zadania realizowanego w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym?		
3. W przypadku odpowiedzi negatywnej na pytanie V.1 lub odpowiedzi pozytywnej na pytanie V.2, czy skonsultowano się z inspektorem ochrony danych w celu uzyskania zaleceń?		
4. Czy udokumentowano decyzję inspektora ochrony danych i wprowadzono konkretne rozwiązanie do oceny skutków dla ochrony danych?		
5. Czy skonsultowano się z użytkownikiem bądź jego		

przedstawicielem w celu zasięgnięcia opinii w zakresie planowanego przetwarzania danych?	
VI. Monitorowanie i przegląd ryzyka	
1. Za pomocą jakich narzędzi prowadzone jest monitorowanie ryzyka?	
2. Jaka jest częstotliwość przeglądu ryzyka?	
3. W jaki sposób dokonuje się przeglądu ryzyka?	
4. Czy po przeprowadzeniu monitoringu i przeglądu ryzyka miała miejsce zmiana klasyfikacji ryzyka?	
5. Czy po zmianie klasyfikacji ryzyka opracowano odpowiednią strategię postępowania w celu jego ograniczenia?	
Podpis osób odpowiedzialnych	
imię i nazwisko - stanowisko	***imię i nazwisko - stanowisko***

---

[1] **Do operacji wymagających przeprowadzenia oceny skutków przetwarzania dla ochrony danych osobowych zalicza się w szczególności (lecz nie wyłącznie):**

1. Ocena lub punktacja, w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą" (motyw 71 i 79 RODO).
2. Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku wobec osoby fizycznej (art. 35 ust. 3 lit. a RODO).
3. Systematyczne monitorowanie, tj. przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, w tym gromadzenie danych za pośrednictwem sieci lub systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie (art. 35. ust. 3. lit. c RODO).

   Grupa Robocza Art. 29 wskazuje, iż „systematycznie" uzyskuje jedno z następujących znaczeń:

   a) przeprowadzane w ramach określonego systemu;

   b) wcześniej zaplanowane, zorganizowane lub mające metodyczny charakter;

   c) odbywające się w ramach ogólnego planu gromadzenia danych;

   d) realizowane jako część strategii.

Pojęcie „miejsca publicznie dostępne" interpretować należy jako miejsca otwarte dla każdego obywatela, np. plac, centrum handlowe, ulica, rynek, stacja kolejowa, biblioteka publiczna. Katalog miejsc publicznie dostępnych nie jest zamknięty.

4. Przetwarzanie danych wrażliwych lub danych o charakterze wysoce osobistym: w szczególności kategorii danych osobowych ujętych w art. 9 RODO oraz danych osobowych dotyczących wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10 RODO.
5. Przetwarzanie danych na dużą skalę. Przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, zaleca się wziąć pod uwagę następujące czynniki:
   a) liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;
   b) liczbę danych lub zakres poszczególnych przetwarzanych pozycji danych;
   c) czas trwania lub trwałość czynności przetwarzania danych;
   d) zakres geograficzny czynności przetwarzania.
6. Dopasowanie lub łączenie zbiorów danych, np. pochodzących z co najmniej dwóch operacji przetwarzania danych prowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.
7. Przetwarzanie danych dotyczących osób wymagających szczególnej opieki, pozbawionych przysługujących im praw i wolności oraz kontroli nad zarządzaniem ich danymi osobowymi. Do osób tych zaliczyć należy dzieci, pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl, osoby starsze, pacjenci). Uwzględnić tu należy każdą sytuację, w której można stwierdzić brak równowagi między stanowiskiem osoby, której danej dotyczą, a stanowiskiem administratora.
8. Innowacyjne wykorzystanie lub stosowanie przy przetwarzaniu danych nowych rozwiązań technologicznych lub organizacyjnych takich jak połączenie technologii rozpoznającej odcisk palca i twarzy w celu poprawienia fizycznej kontroli dostępu.
9. Przesyłanie danych poza granice Unii Europejskiej.
10. Przetwarzanie, które „uniemożliwia osobom, których dane dotyczą, wykonywanie lub korzystanie z usługi lub umowy" (art. 22 i motyw 91 RODO). Obejmuje operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu.

W przypadku, gdy operacja przetwarzania danych spełnia co najmniej dwa z ww. kryteriów, należy przeprowadzić w odniesieniu do takiej operacji ocenę skutków dla ochrony danych. W niektórych przypadkach administrator danych może uznać, że operacja przetwarzania spełniająca tylko jedno z wymienionych powyżej kryteriów będzie wymagała przeprowadzenia oceny skutków dla ochrony danych.

Kategorie operacji niewymagających przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych:

1. Operacje, które nie „powodują ryzyka naruszenia praw lub wolności osób, których dane dotyczą".
2. Operacje, których zakres, kontekst i cele przetwarzania są bardzo podobne do operacji przetwarzania, w przypadku których przeprowadzono ocenę skutków dla ochrony danych.
3. Operacje, które zostały sprawdzone przez organ nadzorczy przed majem 2018 roku, w szczególnych warunkach, które nie uległy zmianie, tj. decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE (do czasu ich zmiany, zastąpienia lub uchylenia).
4. Operacje, które mają podstawę prawną w prawie UE lub w prawie państwa członkowskiego, które reguluje dane operacje przetwarzania, oraz jeżeli oceny skutków dla ochrony danych dokonano już z przyjęciem tej podstawy prawnej, chyba że państwo członkowskie uznało za niezbędne dokonanie oceny skutków dla ochrony danych przed rozpoczęciem operacji przetwarzania.
5. Operacje przetwarzania umieszczone w opcjonalnym wykazie (utworzonym przez organ nadzorczy) operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych.

[ii] Charakter przetwarzania danych osobowych - należy wskazać, czy dane osobowe są przetwarzane w sposób całkowicie, częściowo zautomatyzowany czy w sposób inny niż zautomatyzowany; jaka jest częstotliwość przetwarzania, czy przetwarzanie ma charakter krótko- czy długoterminowy, systematyczny czy sporadyczny, na jaką skalę przetwarzanie jest prowadzone (charakter masowy, znikomy).

[iii] Zakres przetwarzania danych osobowych - należy zawrzeć w tym miejscu opis każdej z planowanych operacji przetwarzania, dokonywanych na danych osobowych.

[iv] Kontekst przetwarzania danych osobowych – w punkcie tym należy wskazać wszelkie okoliczności prawne i faktyczne planowanego przetwarzania – kategorie przetwarzanych danych, kategorie osób, których dane dotyczą, okoliczności zbierania i dalszego

przetwarzania danych osobowych (wykonanie obowiązków informacyjnych, zebranie danych na potrzeby wykonania innych czynności prawnych np. zawarcia umowy), a także otoczenie i zagrożenie dla bezpieczeństwa i integralności danych.

[v] Cel przetwarzania danych – należy wskazać konkretne, wyraźne, jednoznaczne, ograniczone i legalne cele. O celach przetwarzania danych decyduje administrator danych. Przetwarzanie danych sprzeczne z celami, dla których zostały zebrane, jest niezgodne z prawem. Przetwarzanie danych w celach nieokreślonych lub określonych nieprecyzyjnie, tj. nieograniczonych i niejasnych powoduje niezgodność przetwarzania z prawem.

[vi] Kategorie aktywów – w tym miejscu należy wyszczególnić:

1. procesy i działania biznesowe - seria powiązanych ze sobą działań lub zadań, które realizują operacje przetwarzania danych osobowych lub prowadzą do osiągnięcia celu przetwarzania danych;
2. personel - wszystkie grupy osób zaangażowane w przetwarzanie danych tj.: decydenci, użytkownicy, personel eksploatacji/utrzymania, twórcy oprogramowania;
3. sprzęt - wszelkie urządzenia fizyczne w organizacji tj.: urządzenia przenośne, stacjonarne, peryferyjne, nośniki danych;
4. siedziba - wszelkie lokalizacje wykorzystywane do przetwarzania danych oraz środki fizyczne potrzebne do ich funkcjonowania tj. siedziba, strefy bezpieczeństwa, usługi komunalne i techniczne;
5. oprogramowanie - wszelkie programy uczestniczące w operacjach przetwarzania danych tj.: systemy operacyjne, aplikacje biznesowe, oprogramowania usługowe, utrzymaniowe lub administracyjne;
6. sieć - wszystkie urządzenia telekomunikacyjne używane do połączenia wielu fizycznie oddalonych komputerów lub elementów systemu informacyjnego, tj.: media i usługi wspierające, przekaźniki aktywne lub pasywne, interfejsy komunikacyjne;
7. kanały transmisji - wszelkie rodzaje mediów służących do przekazu informacji między nadawcą a odbiorcą.

[vii] W przypadku braku kodeksów postepowania regulujących zasady przeprowadzania opisywanej operacji przetwarzania danych należy uwzględnić te informację w odpowiedzi na pytanie.

[viii] Odpowiedź powinna być oparta na analizie i porównaniu odpowiedzi z punktu 2.5. dotyczącej celu przetwarzania danych osobowych ze stanem faktycznym.

[ix] Zgodność z prawem - zgodnie z art. 5. ust. 1. RODO dane powinny być przetwarzane zgodnie z prawem, tj. z ustawami i rozporządzeniami wydanymi na podstawie ustaw z uwzględnieniem interesów podmiotów danych.

[x] Podstawowe wymagania dotyczące treści porozumienia między administratorem a podmiotem przetwarzającym dane osobowe zostały określone w art. 28. RODO.

Załączniki nr:

1. wykaz kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
2. klauzule informacyjne:
   1) dla kandydatów do pracy i ich zgody,
   2) dla pracowników,
   3) zgoda na publikację w mediach (na stronie www. i facebooku) wizerunku pracownika i osoby wykonującej zadania na rzecz Spółki PCZ na podstawie umowy cywilno -prawnej,
   4) dla osób wykonujących zadania na podstawie umowy cywilno-prawnej,
   5) dla pacjentów,
   6) dla darczyńców,
   7) dla oferentów w postepowaniu o udzielenie zamówienia publicznego
   8) dla oferentów w postepowaniach konkursowych na podstawie ustawy o działalności leczniczej,
   9) dla pracowników składających wnioski do Komisji Socjalnej,
   10) dla osób składających oświadczenia dla celów płacowych, ubezpieczeniowych i podatkowych,
   11) dla osób składających skargi lub wnioski;
3. umowa powierzenia przetwarzania danych osobowych
4. wzory:
   1) upoważnienie do przetwarzania danych wraz z za łącznikiem,
   2) cofnięcia upoważnienia,
   3) oświadczenia o poufności złożone przez osobę, której udzielono upoważnienia do przetwarzania danych osobowych,
   4) oświadczenia o poufności złożone przez osobę, której nie udzielono upoważnienia do przetwarzania danych osobowych,
5. informacje przekazywane przez:
   Dział Prawno-Organizacyjny Głównemu Specjaliście ds. Informatyzacji i Baz Danych:
   1) o osobie wykonującej czynności służbowe na podstawie umowy cywilno-prawnej,
   2) o osobie, której zakres wykonywanych czynności służbowych na podstawie umowy cywilno-prawnej uległ zmianie,
   3) o osobie, która zaprzestała wykonywania czynności służbowych na podstawie umowy cywilno-prawnej,

   Dział Kadrowo-Płacowy Głównemu Specjaliście ds. Informatyzacji i Baz Danych
   1) o osobie wykonującej czynności służbowe na podstawie umowy cywilno-prawnej,
   2) o osobie wykonującej czynności służbowe na podstawie umowy o pracę,
   3) o osobie, której zakres wykonywanych czynności służbowych na podstawie umowy o pracę uległ zmianie,
   4) o osobie, która zaprzestała wykonywania czynności służbowych na podstawie umowy o pracę
   5) o osobie, która zaprzestała wykonywania czynności służbowych na podstawie umowy cywilno-prawnej;
6. wzór formularza oceny skutków.