POLITYKA OCHRONY DANYCH OSOBOWYCH

w Doktor Krasicki Sp. z o.o.

Spis treści

I. WSTĘP

Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) powstał w celu określenia standardów bezpiecznego przetwarzania danych osobowych w przedsiębiorstwie Administratora.

W związku z przetwarzaniem danych przez Administratora powołano niniejszą Politykę, której zadaniem jest zapewnienie przestrzegania podczas przetwarzania danych praw i wolności osób fizycznych, a w szczególności ich prawa do ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Niniejsza Polityka jest jednym z głównych środków organizacyjnych, stanowi zestaw wymogów, zasad i regulacji ochrony danych osobowych powołanych w celu zapewnienia oraz wykazania przetwarzania tych danych zgodnie z ogólnym rozporządzeniem o ochronie danych - RODO.

II. DEFINICJE

Przez użyte w Polityce określenia należy rozumieć:

Administrator - Doktor Krasicki Sp. z o.o. z siedzibą w Gdyni przy ul. Zakręt do Oksywia 3, numer NIP 586-19-33-859.

Czynność przetwarzania - oznacza mniejszy lub większy (krótszy lub dłuższy) wycinek procesu „biznesowego" (procesu przetwarzania danych) realizowanego w konkretnym celu przetwarzania danych. Czynności przetwarzania danych składają się z operacji przetwarzania danych.

Dane dotyczące zdrowia - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia. Zgodnie z Preambułą w motywie (35) - do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

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

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Dane wrażliwe - oznaczają dane o szczególnych kategoriach oraz dane karne.

Incydent bezpieczeństwa informacji - jest zdarzeniem, którego bezpośrednim lub pośrednim skutkiem jest lub może być naruszenie ochrony danych osobowych.

IOD lub Inspektor - oznacza Inspektora Ochrony Danych Osobowych w rozumieniu RODO.

Naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. W ISO konsekwencja, rezultat zdarzenia.

Ocena skutków dla ochrony danych - jeżeli planowany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres,

kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Jest to sformalizowana analiza ryzyka przetwarzania danych dla sytuacji, w których to ryzyko zostało ustalone przez organizację jako wysokie.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców.

Ograniczenie przetwarzania - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Osoba - oznacza osobę fizyczną, której dane dotyczą.

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Podmiot przetwarzający jest odrębnym bytem prawnym. Może wykonywać operacje przetwarzania jedynie na udokumentowane polecenie Administratora. W obszarze ISO podmiot ten najczęściej nazywany jest - procesorem.

Polityka - oznacza niniejszą Politykę ochrony danych osobowych.

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

Przetwarzanie - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Rejestr Czynności Przetwarzania Danych - (**RCPD**) stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności. Pełni również funkcję informacyjną, w tym stanowi źródło informacji o procesach przetwarzania danych w danej organizacji dla organu nadzorczego.

RODO - oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

Spółka - Doktor Krasicki Sp. z o.o. z siedzibą w Gdyni przy ul. Zakręt do Oksywia 3, numer NIP 586-19-33-859.

Szczególne kategorie danych - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Zagrożenie - jest to potencjalna przyczyna niepożądanego incydentu, który może powodować szkody dla systemu lub organizacji. Incydenty powstają wskutek zagrożeń. Na zagrożenie i jego prawdopodobieństwo mają wpływ: okoliczności, stan prawny, stan faktyczny, działania, zaniechanie działań i wydarzenia zewnętrzne oraz wewnętrzne, które mogą ale nie muszą wywołać ryzyko wystąpienia incydentu.

Zgoda - osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

III.OGÓLNE ZASADY OCHRONA DANYCH OSOBOWYCH

1. Zawartość polityki

Polityka zawiera:

a) opis wymogów, zasad i regulacji ochrony danych osobowych powołanych w celu zapewnienia oraz wykazania przetwarzania danych Spółki zgodnie z RODO;

b) odwołania do załączników uszczegóławiających (procedury, rejestry, wzory dokumentów lub instrukcje dotyczące poszczególnych obszarów, procesów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

2. Odpowiedzialność

Polityka Administratora oparta jest na zasadzie odpowiedzialności:

a) odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest Administrator reprezentowany przez Zarząd Spółki;

b) Zarząd Spółki samodzielnie nadzoruje obszar ochrony danych osobowych w celu zapewnienia zgodności przetwarzania danych zgodnie z wymogami RODO oraz Polityką;

c) za nadzór i monitorowanie przestrzegania Polityki odpowiada powołany Inspektor Ochrony Danych (IOD);

d) za stosowanie niniejszej Polityki odpowiedzialni są:

   a. Spółka reprezentowana przez Zarząd;

   b. Wszyscy członkowie personelu Spółki;

e) Administrator zapewnia by w przypadkach, w których zachodzi powierzenie danych, Spółka korzystać będzie z usług tylko takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane im powierzono.

3. Cztery fundamenty Polityki Spółki

Polityka ochrony danych Spółki oparta została na czterech fundamentalnych zasadach:

1) **Zasada legalności** - Spółka dba by przetwarzanie danych odbywało się zgodnie z prawem dbając o ochronę prywatności.
2) **Zasada respektowania praw jednostki** - Spółka umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
3) **Zasada bezpiecznego przetwarzania** - Spółka zapewnia odpowiedni poziom bezpieczeństwa przetwarzania danych, analizując i monitorując ryzyko oraz zapewniając i wdrażając odpowiednie środki bezpieczeństwa.
4) **Zasada rozliczalności** - Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

3.1. Realizacja zasady legalności

Spółka przetwarza dane osobowe w poszanowaniu i realizacji następujących zasad:

a) **Legalność** - Spółka przetwarza dane tylko w oparciu o podstawę prawną, zapewniając rzetelność i przejrzystość dla i wobec osoby, której dane dotyczą.

b) **Celowość** - Spółka zbierane dane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami.

c) **Adekwatność** - Spółka zbiera dane adekwatnie, stosownie oraz ograniczając się do danych niezbędnych do realizacji celów, w których są przetwarzane.

d) **Merytoryczna poprawności** - Spółka gromadzi i przetwarza dane z dbałością o ich merytoryczną poprawność i prawidłowość.

e) **Ograniczenie czasowe** - Spółka zapewnia by przechowywanie danych w formie umożliwiającej identyfikację osoby, nie trwało przez okres dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

f) **Właściwe zabezpieczenie** - Spółka dokłada wszelkiej staranności by sposób przetwarzania przez nią danych zapewniał dla nich odpowiedni poziom bezpieczeństwa, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem ("integralność i poufność").

Administrator na bieżąco prowadzi inwentaryzację czynności przetwarzania danych analizując przestrzeganie powyższych zasad legalności. Aktualny stan zasobów oraz bieżące zmiany Spółka prowadzi w Rejestrze Czynności Przetwarzania Danych w zakresie wymaganym przez RODO – **Złącznik nr 2 do Polityki - „Rejestr Czynności Przetwarzania Danych”.**

3.2. Realizacja zasady respektowania praw jednostki

3.2.1. Spółka realizuje obowiązek spełnienia praw osób, których dane dotyczą poprzez:

a) dbanie o czytelność, przejrzystość, rzetelność oraz zwięzłość przekazywanych informacji w komunikacji z osobami, których dane przetwarza;

b) ułatwianie osobom w korzystaniu z ich praw poprzez różne działania, w tym zamieszczenie na stronie internetowej Spółki oraz tablicy ogłoszeń informacji o prawach osób, sposobie skorzystania z nich, kanałach kontaktu ze Spółką oraz ewentualnym cenniku żądań „dodatkowych” itp.;

c) dbanie o dotrzymywanie prawnych terminów realizacji obowiązków względem osób;

d) zapewnienie właściwej realizacji obowiązku informacyjnego przy zbieraniu danych i w innych sytuacjach - **Załączniki nr 1A do 1E do Polityki - „Klauzule informacyjne”**;

e) stosowania procedury pozwalającej na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych - **Załącznik**

nr 3 do Polityki - „Procedura - zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych".

3.2.2. W celu realizacji praw jednostki Spółka zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Spółkę, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

3.2.3. Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób - **Załącznik nr 4 do Polityki - „Rejestr obsługi zgłoszeń osób, których dane dotyczą".**

Prawa osób, których dane dotyczą:

a) Prawo dostępu do informacji,
b) Prawo do sprostowania danych,
c) Prawo do usunięcia danych („prawo do bycia zapomnianym"),
d) Prawo do ograniczenia przetwarzania,
e) Prawo o powiadomieniu przez Administratora o sprostowaniu, usunięciu, ograniczeniu,
f) Prawo do przenoszenia danych,
g) Prawo do sprzeciwu,
h) Prawo do niepodleganiu zautomatyzowanej decyzji.

3.3. Realizacja zasady bezpiecznego przetwarzania

Zapewnienie odpowiedniego bezpieczeństwa przetwarzania danych osobowych Spółka realizuje w oparciu o system ochrony danych osobowych składający się z następujących elementów:

1) **Inwentaryzacja danych.** Spółka dokonuje inwentaryzacji zasobów danych osobowych w kontekście czynności przetwarzania ze szczególnym uwzględnieniem: procesów biznesowych, klas danych, zależności między zasobami, okresem przechowywania danych, identyfikacją oraz skutecznością aktualnych środków bezpieczeństwa, prawnych przesłanek przetwarzania danych, obszarów przetwarzania.

    a. pierwszą inwentaryzację Spółka dokonuje poprzez przeprowadzenie **„Audytu zgodności przetwarzania danych z RODO"** który stanowi **Załącznik nr 5 do Polityki**;

    b. aktualny stan zasobów oraz bieżące zmiany Spółka prowadzi w RCPD - **Załącznik nr 2 do Polityki - „Rejestr Czynności Przetwarzania Danych"**.

2) **RCPD** - Spółka opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych („Rejestr") zgodnie z zapisami art. 30 RODO. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Spółce.

    a. RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której

opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

b. Spółka prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

c. Rejestr jest jednym z podstawowych narzędzi umożliwiających Spółce rozliczanie większości obowiązków ochrony danych.

d. W Rejestrze dla każdej czynności przetwarzania danych, którą Spółka uznała za odrębną dla potrzeb Rejestru oraz wymagająca opisania, Spółka odnotowuje co najmniej:

- nazwę czynności,
- zakres przetwarzania,
- cel przetwarzania,
- podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Spółki, jeśli podstawą jest uzasadniony interes,
- kontekst oraz charakter przetwarzania,
- opis kategorii osób,
- opis kategorii danych,
- okres przechowywania,
- sposób realizacji spełnienia obowiązku informacyjnego,
- opis kategorii odbiorców danych (w tym przetwarzających),
- opis aktualnych procedur organizacyjnych,
- ogólny opis technicznych i organizacyjnych środków ochrony danych.

e. Rejestr stanowi **Załącznik nr 2 do Polityki – „Rejestr Czynności Przetwarzania Danych”.** Rejestr zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Spółka rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

f. W ramach RCPD Spółka identyfikuje oraz weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

- utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

- inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Spółka przetwarza dane na podstawie prawnie uzasadnionego interesu Spółki.

3) Minimalizacja. Spółka posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

a. zasady zarządzania adekwatnością danych - **minimalizacja zakresu**:

- Spółka każdorazowo weryfikuje zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania;

- Spółka dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

b. zasady reglamentacji i zarządzania **dostępem** do danych - **minimalizacja dostępu** (dostępu do danych):

- Spółka stosuje ograniczenia dostępu do danych osobowych:
  - prawne *(zobowiązania do poufności, zakresy upoważnień),*
  - fizyczne *(kontrola dostępu do pomieszczeń),*
  - logiczne *(ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).*

- Spółka nadaje dostęp do przetwarzanych danych osobowych wyłącznie tym osobom, które:
  - zostały skutecznie zapoznane z wyciągiem z podstawowych zasad bezpieczeństwa danych osobowych oraz standardowymi procedurami postępowania dla użytkowników - **Załącznik nr 12 do Polityki**,
  - zobowiązały się do jego przestrzegania w drodze oświadczenia, oraz do zachowania do zachowania poufności - **Załącznik nr 13 do Polityki**,
  - oraz otrzymały upoważnienie - **Załącznik nr 14 do Polityki**, ściśle precyzujące zakres czynności, które związane są z dostępem do danych osobowych.

- Spółka prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, wedle wzoru stanowiącego **Załącznik nr 8.**

- Spółka dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających.

- Spółka dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

c. zasady reglamentacji i zarządzania **dostępem** do danych - **minimalizacja czasu** (okres przechowywania danych):

- Spółka wdraża mechanizmy kontroli cyklu życia danych osobowych w Spółce, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.
- Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów produkcyjnych Spółki, jak też z akt podręcznych i głównych.

4) Bezpieczeństwo. Spółka zapewnia odpowiedni poziom bezpieczeństwa danych, poprzez:

a. przeprowadzanie analizy ryzyka dla czynności przetwarzania danych - **Załącznik nr 10 do Polityki**;

- Spółka zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania - wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
- Spółka kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
- Spółka przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Spółka analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
- Spółka ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Spółka ustala przydatność i stosuje takie środki i podejście jak:

  - pseudonimizacja,

  - szyfrowanie danych osobowych,

  - inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

  - środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

b. przeprowadzanie w określonych prawem sytuacjach oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie.

c. dostosowywanie odpowiednich środki ochrony do ustalonego ryzyka.

d. monitorowanie właściwego działania zabezpieczeń oraz cykliczne audyty bezpieczeństwa.

e. stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych - zarządza incydentami.

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

Spółka zapewnia by w przypadkach, w których zachodzi powierzenie danych, korzystać będzie z usług tylko takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane im powierzono.

Spółka przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **Załącznik nr 11 do Polityki - „Wzór umowy powierzenia przetwarzania danych”**.

Spółka rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

Spółka prowadzi rejestr umów powierzenia - **Załącznik nr 9 do polityki.**

3.4. Realizacja zasady rozliczalności

Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

Wszystkie działania dotyczące realizacji zasad bezpieczeństwa w Spółce są dokumentowane. Szczególnymi dokumentami służącymi do potwierdzenia rozliczalności Spółki są:

1) Raport z audytu zgodności przetwarzania danych z RODO.

2) Analiza ryzyka dotycząca czynności przetwarzania danych.

3) Rejestr czynności Przetwarzania Danych.

4) Ocena skutków dla ochrony danych przeprowadzana w razie podejrzenia zaistnienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

5) Rejestr naruszeń.

6) Rejestr incydentów.

7) Rejestr wydanych upoważnień.

8) Rejestr umów powierzenia przetwarzania.

9) Rejestr obsługi zgłoszeń osób fizycznych.

4. Lista załączników

- Załącznik 1A - Klauzula informacyjna dla kontrahentów w języku polskim.
- Załącznik 1B - Klauzula informacyjna dla pracowników.
- Załącznik 1C - Klauzula informacyjna dla kandydatów do pracy.
- Załącznik 1D - Klauzula informacyjna dla pacjentów.
- Załącznik 1E - Klauzula informacyjna dla osób objętych monitoringiem.
- Załącznik 2 - Wzór rejestru czynności przetwarzania danych.
- Załącznik 3 - Procedura - zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.
- Załącznik 4 - Rejestr obsługi zgłoszeń osób, których dane dotyczą.
- Załącznik 5 - Audyt zgodności przetwarzania danych osobowych z RODO.
- Załącznik 6 - Rejestr naruszeń ochrony danych.
- Załącznik 7 - Rejestr incydentów bezpieczeństwa informacji oraz działań korygujących i zapobiegawczych.
- Załącznik 8 - Rejestr upoważnień.
- Załącznik 9 - Rejestr umów powierzenia przetwarzania danych.
- Załącznik 10 - Arkusz oceny ryzyka.
- Załącznik 11 - Wzór umowy powierzenia przetwarzania danych.
- Załącznik 12 - Wyciąg z polityki ochrony danych osobowych.
- Załącznik 13 - Wzór oświadczenia dla osoby upoważnionej.
- Załącznik 14 - Wzór upoważnienia do przetwarzania danych osobowych.
- Załącznik 15 - Wzór ogólny zgody na przetwarzanie danych osobowych.
- Załącznik 16 - Ocena skutków dla ochrony danych.
- Załącznik 17 - Dziennik IOD.
- Załącznik 18 - Procedura szkoleń stanowiskowych z zakresu ochrony danych osobowych.