

POLITYKA OCHRONY DANYCH OSOBOWYCH W
CENTRUM ZDROWIA PSYCHICZNEGO I LECZENIA UZALEŻNIEŃ FAMILIA
SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ
Z SIEDZIBĄ W GLIWICACH

1. Wprowadzenie

Niniejszy dokument stanowi zbiór wymogów, zasad i regulacji ochrony danych osobowych Centrum Zdrowia Psychicznego i Leczenia Uzależnień Familia spółka z ograniczoną odpowiedzialnością z siedzibą w Gliwicach przy ul. Dębowej 5, wpisanego do rejestru przedsiębiorców, prowadzonego przez Sąd Rejonowy w Gliwicach - Wydział Gospodarczy Rejestrowy pod numerem KRS 0000041546, zwaną w dalszej części dokumentu Spółką.

Celem Polityki Ochrony Danych Osobowych, zwanej dalej „Polityką” jest uzyskanie optymalnego i zgodnego z wymogami 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 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych Dz.U. 2018 poz. 1000 - sposobu i systemu przetwarzania w Spółce informacji zawierających dane osobowe.

Polityka określa zasady przetwarzania danych osobowych we wszystkich komórkach organizacyjnych Spółki, w formie dokumentacji papierowej jak również zapisów w systemach informatycznych oraz przechowywanych na elektronicznych nośnikach danych, przez wszystkie osoby przetwarzające dane w imieniu i na odpowiedzialność Spółki.

W tym dotyczących pojedynczych informacji osobowych i w ramach zbiorów danych:

- a) dokumentacji medycznej pacjentów, o której mowa w przepisach ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz wydanych na jej podstawie aktach wykonawczych, a także określonej w przepisach odrębnych,
- b) dokumentacji pracowniczej, w tym pracowników i osób zatrudnionych na podstawie umów-zleceń, osób wykonujących w imieniu Spółki świadczenia zdrowotne na podstawie umów innych niż umowa o pracę, praktykantów, stażystów, kandydatów do pracy,
- c) usługodawców i usługobiorców oraz oferentów,
- d) dokumentacji finansowo-księgowej.

2. Definicje

Określenia użyte w Polityce Ochrony Danych Osobowych oznaczają:

1. **spółka** – Centrum Zdrowia Psychicznego i Leczenia Uzależnień Familia spółka z ograniczoną odpowiedzialnością z siedzibą w Gliwicach przy ul. Dębowa 5,
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;
3. **dane osobowe dotyczące zdrowia** - wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym, przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą, zbierane podczas jej rejestracji do usług opieki zdrowotnej, podczas świadczenia jej usług opieki zdrowotnej, w tym numer, symbol lub oznaczenie przypisane danej osobie fizycznej, informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, których źródłem może być pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne,
4. **pacjent** - osoba zwracająca się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub osobę wykonującą zawód medyczny, oraz osoba, która korzystała z takich świadczeń w przeszłości
5. **podmiot danych** – osoba fizyczna, której dane dotyczą
6. **przetwarzanie danych osobowych** – 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;
7. **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;

8. **zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
9. **administrator** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
10. **podmiot przetwarzający** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
11. **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 jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania – 4.5.2016 PL Dziennik Urzędowy Unii Europejskiej L 119/33;
12. **strona trzecia** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
13. **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;
14. **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;
15. **dane genetyczne** – oznaczają dane osobowe dotyczące dziedziczonych 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;

16. **dane biometryczne** – oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
przedstawiciel – oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z rozporządzenia parlamentu;
17. **przedsiębiorca** – oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
18. **organ nadzorczy** – oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51; L 119/34 PL Dziennik Urzędowy Unii Europejskiej 4.5.2016 „organ nadzorczy, którego sprawa dotyczy” oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ:
 - administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego;
 - przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub - wniesiono do niego skargę;
 - w myśl ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych – organem nadzoru jest Prezes Urzędu Ochrony Danych Osobowych.
19. **zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.
20. **mający znaczenie dla sprawy i uzasadniony sprzeciw** – oznacza sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia niniejszego rozporządzenia lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z niniejszym rozporządzeniem, który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii;

21. **usługa społeczeństwa informacyjnego** – oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (1);
22. **inspektor ochrony danych (IOD)**-wyznaczona przez Zarząd Spółki osoba bezpośrednio nadzorująca i odpowiedzialna za realizację przepisów w zakresie ochrony danych osobowych w Spółce;
23. **GIODO** – Generalny Inspektor Ochrony Danych Osobowych, polski państwowy organ powołany do spraw ochrony danych osobowych;
24. **Prezes Urzędu** – Prezes Urzędu Ochrony Danych Osobowych, polski państwowy organ powołany do spraw ochrony danych osobowych, zgodnie z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych Dz.U. 2018 poz. 1000;

3. Podstawa prawna

Przepisy prawne stanowiące szczegółową podstawę przetwarzania danych w Spółce: w zakresie:

1. Świadczeń zdrowotnych

- 1) Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej,
- 2) Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania,
- 3) Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych,
- 4) Rozporządzenie Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych,
- 5) Ustawa z dnia 12 kwietnia 2019 r. o opiece zdrowotnej nad uczniami.
- 6) Ustawa z dnia 27 czerwca 1997 r. o służbie medycyny pracy,
- 7) Rozporządzenie Ministra Zdrowia z dnia 26 sierpnia 2014 r. w sprawie badań lekarskich kandydatów do szkół ponadgimnazjalnych lub wyższych i na kwalifikacyjne kursy zawodowe, uczniów tych szkół, studentów, słuchaczy kwalifikacyjnych kursów zawodowych oraz uczestników studiów doktoranckich.
- 8) Rozporządzenie Ministra Zdrowia z dnia 29 lipca 2009r. w sprawie rodzajów dokumentacji

medycznej służby medycyny pracy, sposobów jej prowadzenia i przechowywania oraz wzorów stosowanych dokumentów.

- 9) Ustawa z dnia 22 sierpnia 1997 r. o publicznej służbie krwi
- 10) Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe,
- 11) Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi,
- 12) Ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego,

2. Realizacji innych obowiązków prawnych

- 1) Ustawa z dnia 6 czerwca 1997 r. kodeks postępowania karnego
- 2) Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach
- 3) Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia
- 4) Rozporządzenie Ministra Zdrowia i Ministra Spraw Wewnętrznych i Administracji z dnia 28 grudnia 2018 r. w sprawie badań na zawartość alkoholu w organizmie,

3. Spraw pracowniczych i finansowych

- 1) Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy,
- 2) Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych,
- 3) Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze
- 4) Ustawa z dnia 23 maja 1991 r. o związkach zawodowych,
- 5) Ustawa z dnia 1 lipca 2011 r. o samorządzie pielęgniarek i położnych,
- 6) Ustawa z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych,
- 7) Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych;
- 8) Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych
- 9) Ustawa z dnia 29 września 1994 r. o rachunkowości

4. Ochrona danych osobowych w Spółce- zasady ogólne

Niniejsza Polityka zawiera opis zasad ochrony danych osobowych obowiązujących w Spółce oraz opis systemu zabezpieczenia systemu ochrony danych osobowych wprowadzony w Spółce.

Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki jest Centrum Zdrowia

Psychicznego i Leczenia Uzależnień Familia spółka z ograniczoną odpowiedzialnością z siedzibą w Gliwicach, będąca równocześnie Administratorem danych osobowych przetwarzanych w Spółce.

Przedstawicielem, Administratora tj. spółki jest *Pan Maciej Brzozowski*, e-mail: maciej.brzozowski@familia.pl, tel: 513522058

Utrzymanie bezpieczeństwa przetwarzanych przez Spółkę informacji/danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.

Spółka zapewnia także zgodność postępowania jej kontrahentów z niniejszą Polityką w odpowiednim zakresie gdy dochodzi do przekazania im danych osobowych przez Spółkę. Spółka zawiera w tym zakresie ze swoimi kontrahentami – umowy powierzenia przetwarzania danych osobowych.

Filarami ochrony danych osobowych w Spółce są:

7. **Legalność** – Spółka dba o ochronę prywatności i przetwarza dane zgodnie z prawem,
8. **Bezpieczeństwo** – Spółka zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stałe działania w tym zakresie,
9. **Prawa jednostki** – Spółka umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje,
10. **Rozliczność**- Spółka dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

Spółka przetwarza dane osobowe z poszanowaniem następujących zasad:

1. **Legalizm** – w oparciu o podstawę prawną i zgodnie z prawem,
2. **Rzetelność** – rzetelnie i uczciwie;
3. **Transparentność** – w sposób przejrzysty dla osoby, której dotyczą,
4. **Minimalizacja** – w konkretnych celach,
5. **Adekwatność** – nie więcej niż potrzeba,
6. **Prawidłowość** – z dbałością o prawidłowość danych,
7. **Czasowość** – nie dłużej niż potrzeba,
8. **Bezpieczeństwo** – zapewniając odpowiednie środki ochrony danych osobowych.

5. System Ochrony Danych Osobowych

W systemie informacyjnym Spółki przetwarzane są dane osobowe służące do wykonywania zadań statutowych Spółki niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z umów zawartych z kontrahentami Spółki.

Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

1. Inwentaryzacja danych:

Spółka dokonuje identyfikacji zasobów danych osobowych, ich klas, zależności pomiędzy nimi w także identyfikacji sposobów wykorzystania danych osobowych w tym:

- przypadków przetwarzania danych szczególnych kategorii np. danych wrażliwych;
- przypadków przetwarzania danych osób, których Spółka nie identyfikuje (dane niezidentyfikowane);
- profilowania;
- współadministrowania danymi.

1. Przetwarzanie danych:

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

2. Przetwarzanie danych może odbywać się również na podstawie zgody podmiotu danych. Zgoda ta powinna mieć formę pisemną, wskazywać datę jej udzielenia oraz określać cele jakich dotyczy. Przed wyrażeniem zgody podmiot danych otrzymuje informację o przetwarzaniu jego danych.

Zgoda w formie pisemnej nie jest wymagana gdy działanie podmiotu danych potwierdzające zgodę jest wyraźne i jednoznaczne. Poprzez wyraźne działanie rozumie się, w szczególności, wybór przez podmiot danych określonych ustawień technicznych w systemie informatycznym, własnoręczne wypełnienie pól formularzy, przekazanie danych osobowych przez pacjenta w celu rejestracji do świadczeń medycznych oraz wysłanie lub zatwierdzenie wprowadzonych zmian.

Zgoda może być wycofana w każdym czasie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Podmiot danych, jest o tym informowany przed wyrażeniem zgody.

Podmiot danych powinien uzyskać informacje, jakie są konsekwencje niewyrażenia zgody na przetwarzanie danych, w odniesieniu do pacjentów nie może to mieć wpływu na możliwość uzyskania świadczeń zdrowotnych i ich jakość.

3. Szczególne kategorie danych mogą być przetwarzane jeżeli:

- osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych, przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez ADO lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
- jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń,
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa,
- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa
- przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych,
- przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

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

Dane te mogą być przetwarzane również w celu rejestracji do świadczeń zdrowotnych, weryfikacji uprawnień do tych świadczeń, zarządzania systemami i usługami opieki

zdrowotnej, w tym rozliczeń z płatnikami, wykonywania innych czynności pomocniczych przy udzielaniu świadczeń zdrowotnych, utrzymania systemu informatycznego oraz przekazywania danych pacjentów do rejestrów publicznych prowadzonych na podstawie ustawy przez inne osoby.

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

5. Dane dotyczące przekonań religijnych pacjentów mogą być przetwarzane wyłącznie w trybie art. 37 Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Wymogu zgody w formie pisemnej w tym przypadku nie stosuje się.
6. Dane dotyczące pracowników w zakresie określonym przez Kodeks pracy mogą być przetwarzane wyłącznie w celu prowadzenia akt pracowniczych, w tym ewidencji czasu pracy, rozliczeń z pracownikami, naliczania obciążeń, składek i świadczeń, zapewnienia warunków i narzędzi pracy, doskonalenia zawodowego, zgłoszeń do organów wobec których obowiązek taki wynika z ustawy.
7. Dane dotyczące kandydatów do pracy w zakresie określonym przez Kodeks pracy mogą być przetwarzane wyłącznie w celu przeprowadzenia rekrutacji, chyba że kandydat wyraża zgodę na udział w przyszłych rekrutacjach.
8. Dane dotyczące stażystów i praktykantów mogą być przetwarzane wyłącznie w celu zapewnienia odbycia praktyki lub stażu, oraz dochodzenia roszczeń lub obrony przed roszczeniami.
9. Dane dotyczące zdrowia pracowników mogą być przetwarzane wyłącznie do celów profilaktyki zdrowotnej lub medycyny pracy oraz do oceny zdolności pracownika do pracy.
10. Dane dotyczące zdrowia osób wykonujących w imieniu Spółki świadczenia zdrowotne mogą być przetwarzane wyłącznie w zakresie zdolności zdrowotnej do wykonywania świadczeń.
11. Dane dotyczące przynależności do związków zawodowych mogą być przetwarzane wyłącznie na podstawie zgody podmiotu danych w zakresie określonym ustawą z dnia 23 maja 1991 r. o związkach zawodowych oraz kodeks pracy.
12. Dane dotyczące sytuacji rodzinnej i materialnej oraz życiowej pracowników i innych osób mogą być przetwarzane w celu realizacji zadań zakładowego funduszu świadczeń socjalnych określonych w ustawie, za zgodą podmiotu danych.
13. Dane dotyczące sytuacji rodzinnej pracownika mogą być przetwarzane w przypadku korzystania przez pracownika ze szczególnych uprawnień określonych w prawie pracy za zgodą pracownika wyrażoną poprzez złożenie wniosku o te świadczenia.

2. Przechowywanie danych

- Dane osobowe przetwarzane zarówno w formie papierowej, jak też na elektronicznych nośnikach danych.
- Dokumenty i elektroniczne nośniki danych, na których są wykonywane bieżące operacje przetwarzania, mogą znajdować się poza szafą, jedynie na czas tego przetwarzania
- Zbędne kopie, wydruki, zapiski, nie będące dokumentem źródłowym, powinny być niszczone niezwłocznie, poprzez nioszczarkę lub fizyczne rozkawałkowanie nośnika w sposób uniemożliwiający odtworzenie danych.
- Przechowywanie dokumentów po okresie ich bieżącego przetwarzania oraz niszczenie dokumentów źródłowych, po upływie okresu przechowywania, odbywa się na podstawie polityki archiwizacji Spółki.

Dane osobowe gromadzone w formie papierowej i przetwarzane manualnie, poza zabezpieczeniami wskazanymi powyżej, są zabezpieczone także poprzez ogólne środki bezpieczeństwa wprowadzone w Spółce.

Środki bezpieczeństwa wprowadzone w Spółce to:

- ograniczenia dostępu do budynku siedziby Spółki – domofon, monitoring, alarm;
- nie pozostawianie drzwi do pomieszczenia niezamkniętych;
- nie pozostawianie klucza w zamku od zewnątrz, zarówno podczas pobytu w pomieszczeniu jak również po opuszczeniu go i zamknięciu zamka,
- nie pozostawianie otwartych okien w pomieszczeniach, zwłaszcza na porterce; w razie konieczności, za wyjątkiem pierwszej kondygnacji, okna mogą na czas chwilowej nieobecności pozostać uchylone,
- nie pozostawiania w pomieszczeniu osoby postronnej, bez nadzoru,
- nie pozostawiania bez nadzoru dokumentacji zawierającej dane

3. Udostępnianie danych

1. Dane osobowe mogą być udostępniane innym podmiotom tylko na podstawie ustawy i w zakresie określonym ustawą.
2. Dane zawarte w dokumentacji medycznej mogą być udostępniane podmiotom wykonującym działalność leczniczą, w celu zapewnienia kontynuacji świadczeń opieki zdrowotnej.
3. Dane zawarte w dokumentacji medycznej mogą być udostępniane innym podmiotom i osobom za zgodą Inspektora Ochrony Danych Osobowych.

4. Rejestr czynności

Spółka prowadzi, opracowuje i utrzymuje Rejestr Czynności Danych Osobowy zwany „Rejestrem”. Rejestr jest narzędziem rozliczania zgodności z ochroną danych osobowych w Spółce.

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.

- Spółka prowadzi Rejestr Czynności Przetwarzania Danych Osobowych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe,
- Rejestr jest jedną z podstawowych narzędzi umożliwiających Spółce rozliczanie większości obowiązków ochrony danych osobowych,

5. Podstawy prawne

Spółka zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

- a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
- b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Spółka przetwarza dane na podstawie prawnie uzasadnionego interesu Spółki,

6. Dostęp do danych osobowych

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Spółce zasad ochrony danych osobowych.

Spółka wdraża i przeprowadza szkolenia swoich pracowników w powyższym zakresie.

Pracownicy Spółki zostali poinformowani o funkcjonującej w Spółce Polityce Ochrony Danych Osobowych.

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

Z podmiotami, które w ramach swojej działalności gospodarczej przetwarzają dane osobowe powierzone im przez Spółkę, Spółka zawiera stosowne, dopasowane do konkretnych wymogów gospodarczych – umowy o powierzenie przetwarzania danych osobowych.

Pomieszczenia, w których przetwarzane są dane osobowe, są zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

Dostęp do danych osobowych, poza Administratorem oraz pracownikami Spółki, mają wyłącznie podmioty, z którymi Spółka zawarła umowy o powierzenie przetwarzania danych osobowych.

7. Źródła danych

1. Źródłem danych osobowych przetwarzanych przez Spółkę jest podmiot danych albo osoba reprezentująca jego prawa lub działająca z jego upoważnienia.
2. Źródłem danych osobowych członków rodziny jest pracownik korzystający ze szczególnych świadczeń przewidzianych przez Kodeks pracy.
3. Źródłem danych osobowych może być oferent lub kontrahent w odniesieniu do danych, których jest administratorem.
4. W szczególnych, uzasadnionych przypadkach, źródłem danych może być inna osoba niż podmiot danych.
5. Źródłem danych osobowych pacjentów może być również pracownik służby zdrowia, urządzenie medyczne lub badanie laboratoryjne lub diagnostyczne. albo inny podmiot wykonujący działalność leczniczą udostępniający dane pacjentów w trybie art. 26 ust. 3 pkt. 1 Ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta lub podmiot powierzający je na podstawie umowy
6. Źródłem danych osobowych osób upoważnionych przez pacjenta w trybie art 14 ust. 1 pkt.1 oraz art 26 ust.3 pkt.1 jest pacjent.
7. Źródłem danych pacjentów w zakresie weryfikacji uprawnień do świadczeń zdrowotnych jest EWUŚ.
8. W Spółce nie są zbierane ani przetwarzane dane osobowe pochodzące z innych źródeł.

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

8. Obsługa praw jednostki - informacje

Spółka spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania w tym:

- a) obowiązki informacyjne – Spółka przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków,
- b) możliwość wykonania żądań – Spółka weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających,
- c) obsługa żądań – Spółka zapewnia odpowiednie nakłady i procedury aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane,
- d) zawiadamianie o naruszeniach – Spółka stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

W przypadku zgłoszenia przez osobę trzecią, pracownika, pacjenta lub kontrahenta Spółki przypadku naruszenia ochrony ich danych osobowych, Spółka natychmiastowo, nie później niż w terminie 7 dni od wykrycia naruszenia, podejmie kroki w celu ustalenia źródła tych naruszeń i w przypadku uznania, iż wynika to z naruszenia Polityki przez Spółkę, niezwłocznie naruszenia zostaną usunięte a rodzaj naruszeń, system ich wykrycia oraz sposób usunięcia zostanie udokumentowany w Rejestrze incydentów ochrony danych osobowych, prowadzonym przez Spółkę. O sposobie załatwienia ewentualnego zgłoszenia osoba dotknięta zidentyfikowanym naruszeniem ochrony danych zostanie powiadomiona w terminie 7 dni od dnia usunięcia naruszenia.

9. Minimalizacja

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

- a) zasady zarządzania adekwatnością danych,
- b) zasady reglamentacji oraz zarządzania dostępem do danych,
- c) zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

Spółka gromadzi wyłącznie dane osobowe niezbędne dla celów wykonania jej celów

statutowych oraz wykonania umowy łączącej ją z kontrahentem Spółki.

W ramach realizacji celów swojej działalności Spółka gromadzi dane osobowe zawierające dane wrażliwe pacjentów. W tym zakresie, jak już wspomniano powyżej, Spółka zwraca szczególną uwagę na zabezpieczenie tych danych przed dostępem osób niepowołanych. A dane te gromadzone są w sposób i zgodnie z obowiązującymi przepisami.

W przypadku umów z kontrahentami Spółki, gromadzone dane osobowe nie zawierają danych wrażliwych i gromadzone są wyłącznie w celu wykonania danej umowy.

System reglamentacji oraz zarządzania dostępem do danych w Spółce jest spójny i przejrzysty. Dostęp do danych mają wyłącznie Administrator Danych Osobowych, wyznaczeni pracownicy oraz podmioty powiązane ze Spółką umową o powierzenie przetwarzania danych osobowych. Jednakże pracownikom Spółki oraz podmiotom powiązanych ze Spółką umową o powierzenie przetwarzania danych osobowych, dane osobowe gromadzone w Spółce udostępniane są wyłącznie w celu wykonania konkretnej czynności lub usługi. Podmioty te nie posiadają stałego ani nieograniczonego dostępu do wszystkich danych osobowych gromadzonych w Spółce.

Okres przechowywania danych osobowych w Spółce i weryfikacji ich dalszej przydatności wynika wprost z przepisów prawa obowiązującego w Polsce.

Okresy te są różne w zależności od kategorii danych osobowych jakie przetwarzane są w Spółce.

Okresy przechowywania danych osobowych w tym danych wrażliwych oraz warunki weryfikacji ich dalszej przydatności określone są przepisami prawa do których Spółka się stosuje tj. Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta, Ustawa o działalności leczniczej, kodeks cywilny czy rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika, ustawa o rachunkowości itp.

8. Bezpieczeństwo

- a) Spółka zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
- przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii,
 - przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,

- dostosowuje środki ochrony danych do ustalonego ryzyka,
- stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych osobowych Urzędowi Ochrony Danych Osobowych – zarządza incydentami.

2. W tym celu:

- a) Spółka zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnątrz lub ze wsparciem podmiotów wyspecjalizowanych,
- b) Spółka kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka,
- c) Spółka przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Spółka analizuje możliwe sytuacje i scenariusze ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożeń,
- d) 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,
- e) 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.

3. Spółka dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

4. Spółka stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Spółce.

5. Spółka stosuje także fizyczne zabezpieczenia Środki: drzwi wejściowe do pokoi zamykane na klucz, zamykane na klucz szafy na dokumenty, Archiwum Spółki, stosowane zgodnie z bieżącymi potrzebami, niszczarki, zabezpieczenia komputerowe m. in. programy antywirusowe, programy szyfrujące, zmieniane hasła dostępu do komputerów, zmieniane

hasła dostępu do poczty mailowej, zabezpieczenia dysków zewnętrznych, reguły wnoszenia sprzętu komputerowego poza siedzibę spółki.

6. W przypadku naruszenia ochrony danych osobowych – tj. 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.

a) Osoba przetwarzająca, która stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązana:

1. niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu i IOD,
2. podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony,
3. zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

b) IOD po uzyskaniu informacji o stwierdzeniu naruszenia. podejmuje następujące kroki:

- odbiera relację z zaistniałego naruszenia
- dokumentuje przypadek
- wprowadza działania naprawcze i minimalizujące skutki

7. W przypadku odnotowania naruszenia ochrony danych osobowych Spółka niezwłocznie, zawiadamia osobę której dane dotyczą o takim naruszeniu i nie później niż w terminie 7 dni dokonuje zgłoszenia identyfikującego do Urzędu Ochrony Danych Osobowych.

9. Przetwarzający

1. Spółka posiada zasady doboru przetwarzających dane w Spółce i na rzecz Spółki, wymogów co do warunków przetwarzania, zasad weryfikacji wykonywania umów powierzenia.
2. Podstawą do przetwarzania danych, jest pisemne upoważnienie wydane przez Administratora które określa zbiór danych, zakres przetwarzania oraz termin ważności. Wzór upoważnienia stanowi załącznik nr 1.
3. Dział Spraw Pracowniczych jest zobowiązany informować IOD o zatrudnieniu pracownika lub zawarciu innej umowy skutkującej przetwarzaniem danych osobowych przez osobę niebędącą pracownikiem.
4. IOD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
5. Wymóg złożenia pisemnego oświadczenia nie dotyczy osób, dla których obowiązek zachowania w tajemnicy danych osobowych uzyskanych w związku z wykonywaniem

zawodu został określony w ustawie, chyba że ustawa tak stanowi.

6. Z podmiotami z którymi Spółka dokonuje powierzenia przetwarzania danych osobowych, Spółka zawiera umowy powierzenia przetwarzania danych osobowych określające warunki i zasady przetwarzania tych danych.

Wzór umowy stanowi załącznik nr 2

10. Sposób obsługi praw jednostki i obowiązków informacyjnych.

1. Spółka dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza,
2. Spółka ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczania na stronie internetowej Spółki linków do informacji o prawach osób, sposobie skorzystania z nich w Spółce, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze Spółką,
3. Spółka dba o dotrzymanie prawnych terminów realizacji obowiązków względem osób,
4. Spółka wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych, 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,
5. Spółka dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

11. Obowiązki informacyjne

1. Spółka określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych,
2. Spółka niezwłocznie informuje o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby,
3. Spółka informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych tej osoby,
4. Spółka określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie jest to możliwe np. tabliczka o objęciu obszaru monitoringiem wizyjnym, regulamin przetwarzania danych osobowych uzyskanych za pośrednictwem monitoringu wizyjnego,
5. Spółka informuje osobę o planowanej zmianie celu przetwarzania danych osobowych,
6. Spółka informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu

przetwarzania danych – chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe,

7. Spółka informuje osobę o prawie sprzeciwu względem przetwarzania jej danych osobowych, najpóźniej przy pierwszym kontakcie z tą osobą,
8. Spółka niezwłocznie zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

12. Żądania osób

1. Prawa osób trzecich

Realizując prawa osób, których dane dotyczą, Spółka wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), Spółka może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

2. Nieprzetwarzanie

Spółka informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

3. Odmowa

Spółka informuje osobę w ciągu miesiąca od otrzymania żądania o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

4. Dostęp do danych

1. Na żądanie osoby dotyczące dostępu do jej danych, Spółka informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być realizowany przez wydanie kopii danych.

2. Dane osobowe przetwarzane w Spółce są upubliczniane tylko w przypadkach gdy obowiązek taki wynika z ustawy i w zakresie określonym ustawą. Dane osobowe dotyczące pacjentów nie są upubliczniane w żadnym trybie ani zakresie. Dane osobowe pracowników mogą być upubliczniane w zakresie niezbędnym do realizacji zadań i obowiązków pracodawcy związanych z prowadzeniem zakładu.
3. W stanach nagłych pacjenta Spółka może podjąć kontakt z osobą trzecią, która nie została przez pacjenta upoważniona w rozumieniu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w celu przekazania lub uzyskania danych, w tym danych o stanie zdrowia Pacjenta, niezbędnych dla ochrony żywotnych interesów Pacjenta lub innej osoby, w szczególności ochrony zdrowia lub życia tych osób, w przypadku, w którym Pacjent nie jest fizycznie albo prawnie zdolny do wyrażenia zgody w odpowiednim czasie, a w szczególności w przypadku:
 - a) nagłej utraty przytomności przez Pacjenta, gdy niezbędne jest uzyskanie dodatkowych informacji o stanie zdrowia Pacjenta w celu udzielania świadczeń zdrowotnych lub przekazanie informacji o pacjencie,
 - b) gdy Pacjent znajduje się w stanie uniemożliwiającym mu świadome wyrażenie zgody lub udzielenie wiarygodnych informacji a niezbędne jest uzyskanie dodatkowych informacji o stanie zdrowia Pacjenta w celu udzielania świadczeń zdrowotnych,
 - c) uzyskania wyniku badania diagnostycznego, które wymaga podjęcia pilnych działań medycznych, przy braku możliwości kontaktu z Pacjentem w odpowiednim czasie przy wykorzystaniu standardowych środków komunikacji.

Działania określone powyżej podejmowane są jedynie w sytuacjach wyjątkowych, gdy nie jest możliwe udostępnienie lub uzyskanie danych od osób upoważnionych zgodnie z przepisami prawa.

5. Kopie danych

Na żądanie Spółka wydaje osobie kopię danych, w tym danych o stanie zdrowia zgodnie z właściwymi przepisami i odnotowuje fakt wydania takiej kopii.

Spółka prowadzi wykaz udostępnianej dokumentacji zgodnie z art. 27 ustawy prawa pacjenta (...) Dokumentacja jest udostępniana w trybie zapewniającym zachowanie poufności i ochrony danych osobowych, w następujący sposób:

- o do wglądu,
- o przez sporządzenie jej wyciągu, odpisu, kopii lub wydruku,
- o przez wydanie oryginału,
- o za pośrednictwem środków komunikacji elektronicznej,

- o na informatycznym nośniku danych.

6. Sprostowanie danych

Spółka dokonuje sprostowania nieprawidłowych danych na żądanie uprawnionej osoby. Spółka ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowość danych, których sprostowania się domaga.

7. Uzupełnienie danych

Spółka uzupełnia i aktualizuje dane na żądanie osoby. Spółka ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celem przetwarzania danych. Wystarczającym do uzupełniania danych jest oświadczenie osoby której dotyczą.

8. Usunięcie danych

Na żądanie osoby, Spółka usuwa dane, gdy:

- dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych, zgodnych z prawem celach,
- zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
- osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
- dane były przetwarzane niezgodnie z prawem,
- konieczność ich usunięcia wynika z obowiązku prawnego,

9. Ograniczenie przetwarzania

Spółka dokonuje ograniczenia przetwarzania danych na żądania osoby, gdy:

- osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość, z poszanowaniem interesu prawnego tej osoby,
- przetwarzanie jest niezgodne z prawem, a osoba której dane dotyczą sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich przetwarzania,
- Spółka nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia dochodzenia lub obrony roszczeń,

- osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia czy po stronie Spółki zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania, Spółka przechowuje dane, natomiast nie przetwarza ich, bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania.

10. Przenoszenie danych

Na żądanie osoby, Spółka wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Spółce, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Spółki.

11. Sprzeciw w szczególnej sytuacji

Jeżeli osoba zgłosi, umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes Spółki lub o powierzone Spółce zadanie w interesie publicznym, Spółka uwzględni sprzeciw jeżeli nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

12. Sprzeciw względem marketingu bezpośredniego

Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Spółkę na potrzeby marketingu bezpośredniego, Spółka uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

6. Postanowienia końcowe

Spółka oświadcza i gwarantuje, iż w przypadku zmiany prawa dotyczącego ochrony danych osobowych, niezwłocznie dostosuje ona niniejszą Politykę oraz istniejące w Spółce procedury do zachodzących zmian.

Wszelkie zmiany w niniejszej Polityce muszą mieć formę pisemną pod rygorem nieważności. W przypadku zaistnienia jakichkolwiek sporów cywilnych na tle ochrony danych osobowych, Spółka gwarantuje podjęcie się ich rozwiązania pierwszoplanowo w drodze ugodowych negocjacji. Sądem właściwym dla rozstrzygnięcia ewentualnych sporów cywilnych na tle ochrony danych osobowych jest sąd w Gliwicach. jest w przypadku Spółki – Sąd właściwy dla miasta Gliwice.