ZASADY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

załącznik do regulaminu świadczenia usług

§1. Postanowienia ogólne

1. Niniejszy dokument określa zasady powierzenia przetwarzania danych osobowych w związku z korzystaniem przez Usługobiorcę z Platformy MindCare i świadczeniem Usług za pośrednictwem Platformy.
2. Usługobiorca oświadcza, że jest uprawniony do dokonania powierzenia przetwarzania danych osobowych i działa jako administrator danych, zgodnie z postanowieniami RODO.
3. Usługobiorca powierza Usługodawcy przetwarzanie danych osobowych na zasadach określonych poniżej.

§2. Definicje

Ilekroć w niniejszej umowie powierzenia przetwarzania danych osobowych mowa o:

1. **"Administratorze"** - rozumie się przez to Usługobiorcę, czyli osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
2. **"danych osobowych"** - rozumie się przez to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"),
3. **"naruszenie ochrony danych osobowych**" - rozumie się przez to 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;
4. **"Ogólnym rozporządzeniu o ochronie danych"** lub **"RODO"** - rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,
5. **"Procesorze"** - rozumie się przez to Usługodawcę,
6. **"przetwarzaniu danych"** - rozumie się przez to 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. **"systemie informatycznym"** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
8. **"Umowie"** - rozumie się przez to Umowę dotyczącą korzystania z Platformy,
9. **"Ustawie o ochronie danych osobowych"** - rozumie się przez to Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 z późn. zm.),

§3. Przedmiot Umowy

1. Administrator powierza procesorowi przetwarzanie danych osobowych, w związku z wykonaniem Umowy dotyczącej korzystania z Platformy.
2. Administrator oświadcza, że jest administratorem danych powierzonych Procesorowi do przetwarzania, na mocy niniejszej Umowy, a Procesor zobowiązuje się do ich przetwarzania zgodnie z prawem, niniejszymi zasadami i Umową.

§4. Powierzenie przetwarzania danych osobowych

1. Procesor będzie przetwarzał dane osobowe wyłącznie w zakresie i celu przewidzianym w Umowie.
2. Szczegółowy opis powierzenia w tym: przedmiot, czas trwania, charakter, cel oraz rodzaj danych i kategorie osób, których dotyczy powierzenie określa **Załącznik nr 1**.

§5. Obowiązki Procesora

1. Procesor będzie przetwarzał powierzone mu dane osobowe na warunkach i zgodnie z treścią obowiązujących w tym zakresie przepisów prawa. W szczególności przetwarzanie powierzonych danych odbywało się będzie w zgodzie z postanowieniami: RODO, Ustawy o ochronie danych osobowych oraz innych właściwych w zakresie przetwarzania danych osobowych przepisów prawa.
2. W związku z powierzeniem przetwarzania danych osobowych Procesor zobowiązuje się do:
   - 2.1. przetwarzania danych osobowych na podstawie udokumentowanego polecenia Administratora, za jakie uważa się polecenie przekazane drogą pisemną i / lub elektroniczną, jak również zasady określone w niniejszym dokumencie,
   - 2.2. zapewnienia by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
   - 2.3. podjęcia odpowiednich środków gwarantujących bezpieczeństwo powierzonych do przetwarzania danych osobowych, w tym m.in. do wdrożenia, przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, odpowiednich środków technicznych i organizacyjnych, w celu zapewnienia stopnia bezpieczeństwa odpowiadającemu temu ryzyku, w tym między innymi w stosownym przypadku:
     - 2.3.1. pseudonimizacji i szyfrowania danych osobowych,
     - 2.3.2. zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
     - 2.3.3. zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
     - 2.3.4. regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

     (Szczegółowy wykaz przyjętych przez Procesora środków technicznych i organizacyjnych opisuję **Załącznik nr 2)**
   - 2.4. przestrzegania określonych w §7 warunków podpowierzenia przetwarzania danych osobowych innemu podmiotowi,
   - 2.5. aktywnej współpracy z Administratorem przez cały okres trwania powierzenia przetwarzania danych osobowych, która w szczególności polega na tym, iż Procesor biorąc pod uwagę charakter przetwarzania, poprzez odpowiednie środki techniczne i organizacyjne, w miarę możliwości będzie

pomagał Administratorowi wywiązywać się z obowiązków względem osób, których dane dotyczą oraz, uwzględniając charakter przetwarzania oraz dostępne mu informacje, będzie pomagał Administratorowi wywiązywać się z obowiązków w zakresie zagwarantowania bezpieczeństwa danych osobowych oraz w wykonywaniu obowiązków określonych w art. 32-36 RODO.

3. Procesor zobowiązuje się niezwłocznie zawiadomić Administratora o:

   3.1. każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia Administratora wynika z przepisów prawa, a w szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienie poufności wszczętego dochodzenia,

   3.2. każdym żądaniu otrzymanym bezpośrednio od osoby, której dane przetwarza, w zakresie przetwarzania dotyczącej jej danych osobowych, powstrzymując się jednocześnie od odpowiedzi na żądanie, chyba, że zostanie do tego upoważniony przez Administratora.

4. Procesor, na każdy wniosek Administratora, zobowiązany jest do udzielenia kompleksowej, odpowiedzi, na skierowane przez Administratora pytania dotyczące kwestii związanych z przetwarzaniem powierzonych danych osobowych. Jeśli wniosek Administratora zostanie złożony w formie pisemnej Procesor jest zobowiązany do złożenia odpowiedzi w takiej samej formie.

5. Odpowiedzi, o której mowa w ust. 4 powyżej, Procesor udzieli niezwłocznie, jednakże nie później niż w terminie 7 dni od dnia otrzymania wniosku Administratora.

6. W przypadku wystąpienia naruszenia ochrony danych osobowych lub zdarzenia które może stanowić takie naruszenie, dotyczącego danych osobowych powierzonych Procesorowi do przetwarzania, Procesor jest zobowiązany:

   6.1. niezwłocznie po powzięciu wiadomości o takim zdarzeniu, jednak w każdym przypadku nie później niż w ciągu 36 godzin, powiadomić o nim Administratora oraz przekazać mu informacje na jego temat dotyczące:

      6.1.1. daty i miejsca wystąpienia,

      6.1.2. kategorii danych oraz przybliżonej liczby osób, których dotyczy,

      6.1.3. opisu,

      6.1.4. możliwych konsekwencji,

      6.1.5. ewentualnego podjęcia środków zaradczych,

   6.2. zapewnić wszelką niezbędną pomoc Administratorowi i przekazywać mu wszelkie dalsze informacje dotyczące takiego zdarzenia, o które wystąpi Administrator lub które mimo braku takiego żądania ze strony Administratora w ocenie Procesora mogą być dla niego konieczne,

   6.3. niezwłocznie po powzięciu wiadomości o takim zdarzeniu przeprowadzić dochodzenie wyjaśniającego jego przyczyny oraz szczegółowy przebieg,

   6.4. podjąć uzgodnione z Administratorem działania mające na celu usunięcie lub zminimalizowanie negatywnych skutków takiego zdarzenia, a także zminimalizowania ryzyka ponownego wystąpienia podobnego zdarzenia w przyszłości,

   6.5. w przypadkach, gdy będzie to wymagane i wyłącznie, jeżeli zostanie to uprzednio zaakceptowane przez Administratora, powiadomić o naruszeniu osoby, na które miał on wpływ

7. Pomaganie Administratorowi w przypadkach wystąpienia naruszenia ochrony danych osobowych może polegać, w szczególności na podjęciu przez Procesora na podstawie instrukcji otrzymanych od Administratora niezbędnych działań w celu usunięcia skutków naruszenia takich jak np. prowadzenie korespondencji mailowej lub pocztowej z osobami których dotyczyło naruszenie ochrony danych lub udzielanie wyjaśnień tym osobom. Decyzję odnośnie zwrócenia się o pomoc w tym zakresie do Procesora Administrator będzie podejmował uwzględniając okoliczności danego naruszenia.

8. Procesor ma obowiązek niezwłocznie poinformować Administratora jeśli jego zdaniem wydane mu polecenie stanowi naruszenie przepisów RODO lub innych przepisów prawa z zakresu ochrony danych osobowych.

§6. Prawo kontroli

1. Administrator ma prawo do kontroli przetwarzania przez Procesora powierzonych mu danych osobowych z punktu widzenia zgodności tego przetwarzania z przepisami prawa oraz postanowieniami Umowy w postaci audytu realizowanego przez Administratora lub audytora upoważnionego przez Administratora.
2. Informacja o terminie i zakresie audytu, o którym mowa w ust. 1 powyżej, będzie przekazana Procesorowi z co najmniej 7 dniowym wyprzedzeniem.
3. Procesor umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora, przeprowadzanie audytu, o którym mowa w ust. 1 i przyczynia się do niego. W szczególności, Procesor zobowiązany jest udostępnić wgląd do wszystkich materiałów oraz systemów, w których realizowane jest przetwarzanie danych Administratora oraz umożliwić dostęp do pracowników zaangażowanych w ich przetwarzanie.
4. Administrator lub audytor upoważniony przez Administratora, przed rozpoczęciem czynności audytowych podpisze zobowiązanie o zachowaniu w poufności wszelkich informacji uzyskanych podczas realizacji audytu, w tym danych osobowych, których administratorem danych jest Procesor.
5. Sposób wykonywania audytu lub kontroli nie może naruszyć ochrony danych osobowych przetwarzanych na zlecenie innych podmiotów.

§7. Podpowierzenie i transfer do państw trzecich

1. Procesor ma prawo podpowierzania danych osobowych, o których mowa w §4 ust. 1, w zakresie i celu niezbędnym do realizacji powierzenia przetwarzania danych osobowych.
2. Administrator niniejszym wyraża zgodę Procesorowi na dalsze powierzenia przetwarzania danych podmiotom wskazanym w **Załączniku nr 3** dostępnym na stronie: Lista podwykonawców
3. Procesor poinformuje Administratora o zamierzonych zmianach dotyczących dodania lub zastąpienia podmiotów przetwarzających. Administratorowi przysługuje prawo zgłoszenia sprzeciwu w terminie 3 dni od uzyskania informacji o planowanej zmianie.
4. Procesor może dokonywać transferów danych do państw trzecich w przypadku zapewnienia zgodności transferu z RODO.

§8. Odpowiedzialność Procesora

1. Procesor jest odpowiedzialny za szkody będące następstwem przetwarzania powierzonych mu danych osobowych, zgodnie z postanowieniami RODO.

§9. Usunięcie lub zwrot danych osobowych

1. Po rozwiązaniu Umowy Procesor jest zobowiązany do usunięcia powierzonych mu danych osobowych oraz usunięcia wszelkich ich istniejących kopii, chyba, że obowiązujące przepisy prawa nakazują przechowywanie tych danych osobowych, z zastrzeżeniem postanowień poniżej.
2. Usunięcie danych osobowych nastąpi w terminie 90 dni.

§10. Czas trwania i wypowiedzenie Umowy

1. Powierzenie przetwarzania danych osobowych obowiązuje przez czas określony odpowiadający okresowi obowiązywania Umowy, zgodnie z postanowieniami Regulaminu.

§11. Pozostałe postanowienia

1. Komunikacja między stronami następuje za pośrednictwem udostępnionych adresów poczty e-mail.

§12. Postanowienia końcowe

1. W sprawach nieuregulowanych postanowieniami Umowy zastosowanie będą mieć właściwe przepisy prawa.

ZAŁĄCZNIK NR 1

OPIS PRZETWARZANIA

Przedmiot przetwarzania	Świadczenie usług, zgodnie z Umową.
Czas trwania przetwarzania	Okres świadczenia usług, czas trwania Umowy.
Cel przetwarzania	wykonanie Umowy.
1. Kategorie osób, których dane dotyczą	*Pacjenci - osoby korzystające z usług świadczonych przez Specjalistów.*
1 a) Kategorie przetwarzanych danych osobowych	*Zwykłe: imię, nazwisko, adres e-mail, wizerunek, głos, zgody.* *Dotyczące zdrowia psychicznego (zawarte w opisach, diagnozach, wypowiedziach, notatkach, wynikach testów, itp.).*
2. **Kategorie osób, których dane dotyczą**	Specjaliści - osoby świadczące usługi (dotyczy Usługobiorców).
2 a) Kategorie osób, których dane dotyczą	Zwykłe: imię, nazwisko, dane kontaktowe, *adres e-mail, wizerunek, głos, aktywność na Platformie.*
Charakter przetwarzania	*Ciągły - trwanie Umowy.*
Sposób przetwarzania	Zautomatyzowany i częściowo zautomatyzowany.
Operacje przetwarzania	Zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie, udostępnienie, usuwanie, niszczenie *(wybrać właściwe na podstawie katalogu operacji wskazanych w art. 4 pkt 2 RODO)*

ZAŁĄCZNIK NR 2

WYKAZ ŚRODKÓW ORGANIZACYJNYCH I TECHNICZNYCH

BEZPIECZEŃSTWO OPROGRAMOWANIA

W systemach Podmiotu Przetwarzającego stosowane są następujące zabezpieczenia techniczne:

1. **Zabezpieczenia dotyczące uwierzytelniania i tożsamości:**
   - 1.1. stosowane są mechanizmy uwierzytelniania użytkowników, obejmujące co najmniej weryfikację danych logowania oraz możliwość zastosowania dodatkowego składnika uwierzytelnienia;
   - 1.2. procesy logowania, resetu i zmiany hasła realizowane są w sposób kontrolowany, z wykorzystaniem wydzielonych mechanizmów uwierzytelniania;
   - 1.3. komunikacja między usługami systemowymi jest uwierzytelniania, tak aby dostęp uzyskiwały wyłącznie uprawnione komponenty.
2. **Zabezpieczenia dotyczące zarządzania sesją i dostępu:**
   - 2.1. sesje użytkowników utrzymywane są z wykorzystaniem zabezpieczonych mechanizmów sesyjnych ograniczających ryzyko nieuprawnionego dostępu do sesji;
   - 2.2. dostęp do danych osobowych ograniczany jest zgodnie z zakresem uprawnień oraz relacją użytkownika z kontem i danymi;
   - 2.3. stosowane są reguły kontroli dostępu na poziomie aplikacji i bazy danych, ograniczające dostęp wyłącznie do uprawnionych użytkowników i ról.
3. **Zabezpieczenia dotyczące ochrony danych w transmisji i spoczynku:**
   - 3.1. transmisja danych realizowana jest z użyciem połączeń chronionych kryptograficznie, zapewniających poufność i integralność przesyłanych informacji;
   - 3.2. dane przechowywane w bazach danych i magazynach plików objęte są ochroną kryptograficzną w spoczynku zapewnianą przez dostawców infrastruktury.
4. **Zabezpieczenia dotyczące integracji i usług zewnętrznych:**
   - 4.1. stosowana jest weryfikacja autentyczności i integralności żądań przychodzących z usług zewnętrznych, w tym powiadomień zwrotnych;
   - 4.2. integracje realizowane są z użyciem adekwatnych mechanizmów uwierzytelniania i autoryzacji, odpowiednich do charakteru danej integracji.
5. **Zabezpieczenia dotyczące plików i artefaktów danych:**
   - 5.1. dostęp do nagrań, transkrypcji i raportów realizowany jest w sposób ograniczony czasowo i powiązany z uprawnieniami do danego zasobu;
   - 5.2. udostępnienie plików poprzedzone jest weryfikacją uprawnień użytkownika do danego zasobu.
6. **Zabezpieczenia dotyczące walidacji danych wejściowych i tokenów:**

6.1. operacje wrażliwe wymagają uprzedniej walidacji uprawnień oraz parametrów wejściowych;

6.2. przed uruchomieniem wybranych procesów weryfikowany jest stan rekordu oraz warunki dopuszczalności operacji, aby ograniczyć ryzyko nieuprawnionych działań.

7. **Zabezpieczenia dotyczące monitorowania procesów i zdarzeń bezpieczeństwa:**

7.1. system przetwarza zdarzenia statusowe procesów oraz sygnały krytyczne przekazywane przez zaufane usługi wewnętrzne i zewnętrzne;

7.2. komunikacja dla takich zdarzeń realizowana jest po kanałach chronionych oraz z zastosowaniem mechanizmów uwierzytelnienia usług.

8. **Zabezpieczenia dotyczące minimalizacji ekspozycji danych:**

8.1. przetwarzanie i udostępnianie danych realizowane jest zgodnie z zasadą niezbędności oraz zakresem uprawnień;

8.2. publiczny, trwały dostęp do zasobów zawierających dane osobowe nie jest wykorzystywany jako domyślny mechanizm udostępniania.

9. **Zabezpieczenia dotyczące aktualizacji i utrzymania oprogramowania:** stosowane jest bieżące monitorowanie komponentów oprogramowania oraz utrzymywanie ich w aktualnych wersjach, w zakresie uzasadnionym bezpieczeństwem, w celu ograniczania ryzyka podatności.