ZAŁĄCZNIK NR 3 DO REGULAMINU ŚWIADCZENIA USŁUG
UMOWA POWIERZENIA PRZETWARZANIA DANYCH

1. DEFINICJE

Wszelkie pojęcia pisane wielką literą mają znaczenie nadane im w Regulaminie, o ile nie nadano im wyraźnie odmiennego znaczenia w niniejszej Umowie.

1.1. **Dane Osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą), powierzone do przetwarzania na podstawie Umowy, których zakres został wskazany w Załączniku A do Umowy.

1.2. **Dni Robocze** – dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy w Polsce.

1.3. **Osoba, której Dane Dotyczą** lub **Podmiot Danych** – osoba, której dotyczą dane osobowe będące przedmiotem Umowy.

1.4. **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).

1.5. **Umowa** – niniejsza umowa powierzenia przetwarzania danych.

2. PRZEDMIOT UMOWY

2.1. Klient powierza KOChM przetwarzanie Danych Osobowych w zakresie wskazanym w Załączniku A.

2.2. Powierzenie Danych Osobowych KOChM następuje w celu świadczenia Usług na rzecz Klienta.

2.3. W przypadku modyfikacji zakresu Usług zgodnie z Regulaminem, zakres i cel powierzenia ulega stosownemu rozszerzeniu lub zmniejszeniu, w stopniu koniecznym do dalszego prawidłowego świadczenia na rzecz Klienta Usług. W przypadku zmniejszenia zakresu świadczonych Usług, dane które nie są konieczne do realizacji Usług zostają usunięte zgodnie z postanowieniami pkt 10.5.

2.4. KOChM może przetwarzać powierzone mu Dane Osobowe wyłącznie w zakresie i celu określonym w Umowie oraz w celu i zakresie niezbędnym do świadczenia Usług określonych w Zamówieniu. Przetwarzanie Danych Osobowych przez KOChM odbywa się wyłącznie w czasie obowiązywania Umowy, z uwzględnieniem postanowień rozdziału 10.

3. OŚWIADCZENIE I OBOWIĄZKI KLIENTA

3.1. Klient oświadcza i gwarantuje, że:

3.1.1. Klient posiada odpowiednią podstawę prawną przetwarzania Danych Osobowych, wymaganą odpowiednio przez art. 6 lub 9 RODO; a w przypadku i w zakresie w jakim Klient występuje w charakterze podmiotu przetwarzającego, odpowiednio – uzyskał zgodę administratora Danych Osobowych na dalsze powierzenie przetwarzania, lub administrator nie zgłosił sprzeciwu względem dalszego powierzenia przetwarzania Danych Osobowych KOChM, zgodnie z umową zawartą pomiędzy Klientem a administratorem;

3.1.2. nie istnieją przeszkody prawne uniemożliwiające powierzenie przetwarzania Danych Osobowych KOChM;

3.1.3. Klientowi znane są przepisy mające zastosowanie do przetwarzania Danych Osobowych, w tym RODO, i zobowiązuje się ich przestrzegać;

3.1.4. wyniki przeprowadzonej przez Klienta analizy ryzyka dla praw i wolności Podmiotów danych nie stoją na przeszkodzie zawarciu Umowy;

3.2. Klient zobowiązuje się niezwłocznie zawiadomić KOChM o jakichkolwiek okolicznościach, które uniemożliwiają lub mogą uniemożliwić prawidłowe wykonanie Umowy przez KOChM.

3.3. Klient zobowiązuje się, że Usługi w zakresie w jakim obejmują przetwarzanie Danych Osobowych przez KOChM na rzecz Klienta, nie będą wykorzystywane do:

3.3.1. jakiejkolwiek działalności naruszającej prawa osób trzecich;

3.3.2. jakiejkolwiek działalności niezgodnej z prawem na szkodę KOChM lub jakiejkolwiek osoby trzeciej.

4. OŚWIADCZENIA I OBOWIĄZKI KOCHM

4.1. KOChM niniejszym oświadcza, że posiada zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany personel w zakresie umożliwiającym należyte wykonanie Umowy, w zgodzie z obowiązującymi przepisami prawa. W szczególności KOChM oświadcza, że znane mu są zasady przetwarzania i zabezpieczenia Danych Osobowych wynikające z RODO.

4.2. KOChM jest zobowiązany:

4.2.1. przetwarzać Dane Osobowe zgodnie z RODO, polskimi przepisami przyjętymi w celu umożliwienia stosowania RODO, innymi obowiązującymi przepisami prawa oraz Umową;

4.2.2. przetwarzać Dane Osobowe wyłącznie na udokumentowane polecenie Klienta, chyba że obowiązek taki nakłada na niego obowiązujące prawo krajowe lub unijne. W sytuacji, gdy obowiązek przetwarzania Danych Osobowych przez KOChM wynika z przepisów prawa, informuje on Klienta drogą elektroniczną – przed rozpoczęciem przetwarzania – o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny; za udokumentowane polecenie Klienta uważa się w szczególności Zamówienie;

4.2.3. udzielać dostępu do Danych Osobowych wyłącznie osobom, które ze względu na zakres wykonywanych zadań otrzymały od KOChM upoważnienie do ich przetwarzania, oraz wyłącznie w celu wykonywania obowiązków wynikających z Umowy, jak również podjąć działania mające na celu zapewnienie, by każda osoba fizyczna działająca z upoważnienia KOChM, która ma dostęp do Danych Osobowych, przetwarzała je wyłącznie na polecenie Klienta, chyba że przetwarzanie jest wymagane przez właściwe przepisy krajowe lub unijne;

4.2.4. zapewnić, aby osoby upoważnione do przetwarzania Danych Osobowych zobowiązały się do zachowania tajemnicy, chyba że osoby te podlegają ustawowemu obowiązkowi zachowania tajemnicy;

4.2.5. wdrożyć, zgodnie z rozdziałem 5 Umowy, odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których Dane Osobowe będą przetwarzane na podstawie Umowy;

4.2.6. wspierać Klienta (poprzez stosowanie odpowiednich środków technicznych i organizacyjnych) w realizacji obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO;

4.2.7. pomagać Klientowi wywiązać się z obowiązków określonych w RODO (w tym w szczególności w art. 32–36 RODO);

4.2.8. prowadzić w formie pisemnej (w tym elektronicznej) rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Klienta; udostępniać Klientowi na jego uzasadnione żądanie informacje niezbędne do wykazania spełnienia przez Klienta obowiązków wynikających z właściwych przepisów prawa, w szczególności z RODO, w tym przekazywać informacje o stosowanych zabezpieczeniach w obszarze ochrony danych osobowych;

4.2.9. umożliwić Klientowi lub audytorowi upoważnionemu przez Klienta przeprowadzanie audytów na zasadach określonych w rozdziale 7 Umowy;

4.2.10. niezwłocznie informować Klienta, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów krajowych albo unijnych o ochronie danych;

4.2.11. bez zbędnej zwłoki informować (o ile nie doprowadzi to do naruszenia przepisów obowiązującego prawa) Klienta o postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez KOChM Danych Osobowych, o skierowanej do KOChM decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania Danych Osobowych;

4.2.12. przechowywać Dane Osobowe jedynie przez okres świadczenia Usług zgodnie z Zamówieniem i Regulaminem, a po zakończeniu świadczenia Usług niezwłocznie usunąć lub zanonimizować Dane osobowe zgodnie z postanowieniami rozdziału 10.

4.3. Postanowienia zawarte w pkt 4.2 nie rozszerzają zakresu obowiązków KOChM w odniesieniu do świadczenia Usług zgodnie z Regulaminem.

5. ŚRODKI ORGANIZACYJNE I TECHNICZNE

5.1. W celu przechowywania Danych Osobowych KOChM wykorzystuje centra danych, które zlokalizowane są na terytorium Rzeczypospolitej Polskiej.

5.2. KOChM wdraża i stosuje odpowiednie środki techniczne i organizacyjne w celu zapewnienia stopnia bezpieczeństwa odpowiedniego do ryzyka naruszenia praw lub wolności osób fizycznych, których Dane Osobowe są przetwarzane na podstawie Umowy. Wykaz środków, które zobowiązany jest wdrożyć KOChM, został określony w Załączniku C. W szczególności:

5.2.1. Szyfrowanie danych at rest - szyfrowanie środowiska realizowane jest mechanizmami dostarczanymi przez dostawcę chmury obliczeniowej. Przy czym kluczami kryptograficznymi zarządza KOChM.

5.2.2. Szyfrowanie danych in transit – cała komunikacja jest szyfrowana TLS z wykorzystaniem szyfrów uznanych za bezpieczne.

5.2.3. Źródłem tożsamości dla systemu jest oprogramowanie dziedzinowe

5.2.4. Regularne wykonywanie szyfrowanych kopii bezpieczeństwa

5.3. Wdrażając środki organizacyjne i techniczne określone w Załączniku C, KOChM powinien uwzględnić stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, jak również ryzyko naruszenia praw lub wolności osób fizycznych, których Dane Osobowe będzie przetwarzał na podstawie Umowy, z uwzględnieniem prawdopodobieństwa ich wystąpienia i wagi zagrożenia.

5.4. W przypadku stwierdzenia przez Klienta konieczności zastosowania dodatkowych środków zabezpieczających, Strony uzgodnią zakres, sposób i termin ich wdrożenia oraz podział kosztów wdrożenia.

6. DOSTĘP DO DANYCH ZA ZGODĄ KLIENTA

6.1. Klient wyraża zgodę na dalsze powierzenie przez KOChM przetwarzania Danych Osobowych innym podmiotom przetwarzającym wskazanym w Załączniku B w zakresie oraz celu zgodnym z Umową np. w celach serwisu serwerów lub napraw. KOChM jest zobowiązany do informowania o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia dalszych podmiotów przetwarzających. Klient może sprzeciwić się dalszemu powierzeniu przez KOChM danych osobowych w terminie 3 Dni Roboczych od otrzymania informacji, o której mowa w zdaniu poprzedzającym. Brak wyrażonego sprzeciwu we wskazanym terminie jest równoznaczny z wyrażeniem przez Klienta zgody. W przypadku wyrażenia sprzeciwu przez Klienta KOChM nie jest uprawniony do zawarcia umowy z dalszym podmiotem przetwarzającym, którego dotyczy sprzeciw. W takim wypadku, bez uszczerbku dla pkt 10.2, KOChM nie będzie ponosić odpowiedzialności za brak możliwości świadczenia Usług, jeżeli do ich świadczenia niezbędne okazało się korzystanie z dalszego podmiotu przetwarzającego, którego dotyczy sprzeciw.

6.2. KOChM zapewnia, że będzie korzystał wyłącznie z usług takich dalszych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz innych przepisów obowiązującego prawa z zakresu ochrony danych osobowych, a także chroniło prawa osób, których dane dotyczą.

6.3. Strony postanawiają, że osoby fizyczne współpracujące z KOChM na podstawie umów cywilno-prawnych są traktowane jak członkowie personelu KOChM i nie są uznawane za dalsze podmioty przetwarzające.

6.4. Strony postanawiają, że osoby fizyczne współpracujące z dalszymi podmiotami przetwarzającymi KOChM, wskazanymi w Załączniku B, na podstawie umów cywilno-prawnych są traktowane jak członkowie personelów tych dalszych podmiotów przetwarzających i nie są uznawane za odrębne dalsze podmioty przetwarzające.

6.5. KOChM zobowiązany jest zapewnić, że każda osoba przetwarzająca Dane Osobowe na jego rzecz przetwarza je wyłącznie na polecenie Klienta.

6.6. KOChM jest uprawniony do przekazania Danych Osobowych do państwa trzeciego, które znajduje się poza Europejskim Obszarem Gospodarczym wyłącznie, gdy spełnione zostały łącznie następujące warunki:

6.6.1. Klient lub KOChM spełnia wymogi dotyczące przekazania Danych Osobowych opisane w art. 44 - 49 RODO;

6.6.2. KOChM zawiadomił Klienta o zamiarze przekazywania Danych Osobowych do państwa trzeciego z wyprzedzeniem co najmniej 14 Dni Roboczych, wskazując instrument prawny, który zamierza stosować w celu legalizacji transferu, a Klient nie zgłosił sprzeciwu względem takiego przekazania w ciągu kolejnych 7 Dni Roboczych. W przypadku wyrażenia sprzeciwu przez Klienta KOChM nie jest uprawniony do przekazania danych do państwa trzeciego, którego dotyczy sprzeciw. W takim wypadku, bez uszczerbku dla pkt 10.2 KOChM nie będzie ponosić odpowiedzialności za brak możliwości świadczenia Usług, jeżeli do ich świadczenia niezbędne okazało się przekazanie danych do państwa trzeciego, którego dotyczy sprzeciw.

6.7. Zawierając Umowę, Klient udziela KOChM pełnomocnictwa oraz upoważnia KOChM do udzielania dalszych pełnomocnictw do zawarcia w imieniu Klienta umowy w oparciu o standardowe klauzule umowne zatwierdzone decyzją Komisji Europejskiej nr 2010/87/EU. O zamiarze zawarcia umowy oraz jej treści KOChM poinformuje Klienta w trybie określonym w pkt 6.6.2.

6.8. Klient wyraża zgodę na transfer Danych Osobowych w przypadkach wskazanych w Załączniku B, z zachowaniem zabezpieczeń tam określonych.

7. AUDYT

7.1. Klient jest upoważniony do przeprowadzenia audytu zgodności przetwarzania przez KOChM Danych Osobowych z Umową oraz obowiązującymi przepisami prawa.

7.2. Audyt może być przeprowadzony w przypadkach, gdy nie jest możliwe zweryfikowanie zgodności przetwarzania przez KOChM Danych Osobowych z Umową oraz obowiązującymi przepisami prawa innymi metodami, np. poprzez przedstawienie przez KOChM wewnętrznej dokumentacji z zakresu ochrony danych osobowych.

7.3. Klient zawiadomi KOChM o zamiarze przeprowadzenia audytu co najmniej 14 Dni Roboczych przed planowaną datą jego przeprowadzenia. Jeżeli w ocenie KOChM audyt nie

może zostać przeprowadzony we wskazanym terminie, KOChM powinien niezwłocznie poinformować o tym fakcie Klienta. W takim przypadku Klient i KOChM wspólnie ustalą późniejszy termin audytu.

7.4. Audyty mogą być wykonywane przez Klienta (osoby przez niego wyznaczone) w siedzibie KOChM w Dni Robocze w godzinach od 9.00 do 17.00.

7.5. Klient zobowiązany jest zapewnić, by osoby wykonujące czynności w ramach audytu zostały zobowiązane do zachowania w poufności wszelkich informacji, które uzyskają w związku z wykonywaniem audytu, a stanowiących tajemnicę przedsiębiorstwa KOChM. Klient zobowiązany jest zapewnić, że osoby wykonujące czynności w ramach audytu nie są zatrudnione, nie są wspólnikami, akcjonariuszami lub członkami organów podmiotów wykonujących działalność konkurencyjną w stosunku do działalności gospodarczej prowadzonej przez KOChM.

7.6. KOChM w zakresie niezbędnym do przeprowadzenia audytu będzie współpracować z Klientem i upoważnionymi przez niego audytorami, w szczególności zapewniać im dostęp do pomieszczeń i dokumentów obejmujących Dane Osobowe oraz informacje o sposobie przetwarzania Danych Osobowych, infrastruktury teleinformatycznej oraz systemów IT, a także do osób mających wiedzę na temat procesów przetwarzania Danych Osobowych realizowanych przez KOChM, z zastrzeżeniem konieczności zapewnienia ciągłości działań związanych z bieżącą działalnością gospodarczą KOChM. KOChM jest uprawniony do odmowy udzielenia informacji w zakresie, w jakim prowadziłoby to do ujawnienia informacji poufnych co do których nieujawniania jest zobowiązany na mocy umów zawartych z innymi Klientami.

7.7. KOChM samodzielnie dokonuje audytu (w tym inspekcji) dalszych podmiotów przetwarzających. KOChM na żądanie Klienta, w rozsądnym terminie ustalonym wspólnie z Klientem, przedstawia wyniki takich audytów oraz udziela wszelkich informacji niezbędnych do wykazania zgodności przetwarzania Danych Osobowych przez dalszy podmiot przetwarzający z Umową.

7.8. W szczególnie uzasadnionych wypadkach, na wniosek Klienta, KOChM dołoży rozsądnych starań by umożliwić Klientowi przeprowadzenie audytu (w tym inspekcji) u dalszego podmiotu przetwarzającego, z uwzględnieniem postanowień umowy zawartej pomiędzy KOChM a dalszym podmiotem przetwarzającym. W takim przypadku:

7.8.1. audyt odbywa się w obecności przedstawiciela KOChM;

7.8.2. audyt odbywa się na zasadach i w zakresie uzgodnionym pomiędzy Klientem, KOChM oraz dalszym podmiotem przetwarzającym;

7.8.3. na Klienta może zostać nałożona adekwatna rozsądna opłata odpowiadająca kosztom przeprowadzenia audytu.

Powyższe postanowienie nie stanowi gwarancji możliwości przeprowadzenia audytu dalszego podmiotu przetwarzającego bezpośrednio przez Klienta.

7.9. Po przeprowadzonym audycie z udziałem przedstawiciela Klienta, przedstawiciel Klienta sporządza protokół pokontrolny. Protokół pokontrolny podpisują przedstawiciele Klienta i KOChM. KOChM zobowiązuje się w rozsądnym czasie, w terminie uzgodnionym z Klientem,

dostosować do zaleceń pokontrolnych zawartych w protokole, mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania Danych Osobowych. W przypadku, gdy wdrożenie tych zaleceń będzie wiązać się z dodatkowymi kosztami, Klient i KOChM wspólnie ustalą sposób ich ponoszenia przez Klienta i KOChM.

7.10. Koszty związane z przeprowadzeniem audytu ponosi Klient i KOChM w swoim zakresie; w szczególności KOChM nie jest zobowiązany do zwrotu Klientowi jakichkolwiek kosztów związanych z wykonanym audytem, niezależnie od jego wyniku.

8. ZGŁASZANIE NARUSZEŃ

8.1. KOChM jest zobowiązany do wdrożenia i stosowania procedur służących wykrywaniu naruszeń ochrony Danych Osobowych oraz wdrażaniu właściwych środków naprawczych.

8.2. Po stwierdzeniu naruszenia ochrony Danych Osobowych KOChM bez zbędnej zwłoki zgłasza je za pośrednictwem poczty elektronicznej na adres e-mail Koordynatora Klienta, informując o okolicznościach naruszenia i potencjalnych zagrożeniach dla ochrony Danych Osobowych.

8.3. KOChM bez zbędnej zwłoki podejmuje wszelkie rozsądne działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.

8.4. KOChM nie jest uprawniony do samodzielnego powiadamiania o naruszeniu:

8.4.1. Osób, których Dane Dotyczą; ani

8.4.2. organu nadzorczego.

9. ODPOWIEDZIALNOŚĆ

9.1. KOChM ponosi odpowiedzialność za szkody lub krzywdy związane z przetwarzaniem Danych Osobowych w granicach wynikających z Regulaminu, z zastrzeżeniem, że ograniczenia te nie mają zastosowania w przypadkach, w których możliwość takich ograniczeń została wyłączona przepisami prawa bezwzględnie obowiązującego.

10. CZAS TRWANIA UMOWY

10.1. Umowa zostaje zawarta na czas obowiązywania Zamówienia. Dane Osobowe przetwarzane są przez KOChM przez czas świadczenia na rzecz Klienta Usług oraz przez czas wykonania obowiązków wskazanych w niniejszym rozdziale.

10.2. KOChM jest uprawniony do wypowiedzenia Umowy z zachowaniem 7-dniowego okresu wypowiedzenia w przypadku wyrażenia przez Klienta sprzeciwu względem dalszego powierzenia przetwarzania danych zgodnie z pkt 6.1 lub względem przekazania Danych Osobowych do państwa trzeciego zgodnie z pkt 6.6.2, jeżeli sprzeciw uniemożliwia lub znacząco utrudnia wykonanie Umowy lub świadczenie Usług. Wypowiedzenie Umowy na podstawie niniejszego punktu skutkuje jednoczesnym wypowiedzeniem Zamówienia, na podstawie którego KOChM świadczy Usługi na rzecz Klienta. KOChM nie ponosi

odpowiedzialności za szkody spowodowane wypowiedzeniem Umowy na podstawie niniejszego punktu ani następującym w związku z tym wypowiedzeniem Zamówienia.

10.3. Wypowiedzenie, wygaśnięcie lub rozwiązanie Zamówienia, niezależnie od przyczyny, skutkuje odpowiednio wypowiedzeniem, wygaśnięciem lub rozwiązaniem Umowy.

10.4. KOChM zobowiązuje się przechowywać Dane Osobowe przez okres 30 dni od dnia zakończenia obowiązywania Zamówienia, na podstawie którego KOChM świadczy usługi na rzecz Klienta, w celu umożliwienia Klientowi pobrania Danych Osobowych. Po tym okresie KOChM usuwa lub anonimizuje powierzone Dane Osobowe, oraz zapewnia usunięcie lub anonimizację powierzonych Danych Osobowych przez dalsze podmioty przetwarzające, lub umożliwia usunięcie lub anonimizację Danych Osobowych przez Klienta, chyba że właściwe przepisy prawa krajowego lub unijnego nakazują przechowywanie tych Danych Osobowych.

10.5. Wykonanie obowiązku usunięcia danych wskazanego w pkt 10.4 następuje niezwłocznie, z uwzględnieniem rozsądnego okresu, wynikającego ze względów technicznych, nie dłuższego niż 180 dni od zakończenia obowiązywania Zamówienia.

11. POSTANOWIENIA KOŃCOWE

11.1. Wszelka komunikacja Stron w sprawach związanych z Umową będzie prowadzona za pośrednictwem Koordynatorów (odpowiednio Koordynatora KOChM oraz Koordynatora Klienta) oraz przy użyciu wskazanych danych kontaktowych Koordynatorów.

11.2. Spory mające związek z Umową będą rozstrzygane przez sąd właściwy zgodnie z Regulaminem.

11.3. Zmiany Umowy są możliwe na zasadach przewidzianych dla zmiany Regulaminu.

11.4. Załączniki do UPPD stanowią jej integralną część. Lista załączników jest następująca:

11.4.1. Załącznik A – Zakres powierzenia Danych Osobowych;

11.4.2. Załącznik B – Lista dalszych podmiotów przetwarzających;

11.4.3. Załącznik C – Wykaz środków technicznych i organizacyjnych.

ZAŁĄCZNIK A

Zakres powierzenia Danych Osobowych

CEL PRZETWARZANIA:

Dane Osobowe przetwarzane są w celu świadczenia Usług na rzecz Klienta zgodnie z Regulaminem i Zamówieniem, w szczególności w zakresie przechowywania elektronicznej dokumentacji medycznej powierzanej przez Klienta.

CHARAKTER PRZETWARZANIA:

Charakter przetwarzania wynika z charakteru Usług świadczonych na rzecz Klienta i obejmuje w szczególności zbieranie, przechowywanie, łączenie, usuwanie, modyfikowanie, udostępnianie i ujawnianie danych osobowych w celu świadczenia Usług na rzecz Klienta zgodnie z Regulaminem i Zamówieniem.

RODZAJ DANYCH OSOBOWYCH:

Dane Osobowe objęte powierzeniem przetwarzania stanowią wszelkie Dane Osobowe zwykłe i szczególnej kategorii, które przekazane zostają KOChM w związku ze świadczonymi Usługami. Tymi Danymi Osobowymi mogą być w szczególności:

- w zakresie danych zwykłych: dane identyfikacyjne, kontaktowe, adresowe, dot. rodziny i osób bliskich, informacje o osobach upoważnionych, płeć, dane dot. urodzenia, PESEL, informacje o opiekunie prawnym i inne informacje, w tym nieustrukturyzowane, zawarte w dokumentacji medycznej lub w innych dokumentach przekazanych przez Klienta;
- w zakresie danych szczególnej kategorii: dane dot. zdrowia i inne informacje, w tym nieustrukturyzowane, zawarte w dokumentacji medycznej lub w innych dokumentach przekazanych przez Klienta.

Rodzaj Danych Osobowych przetwarzanych w związku ze świadczeniem Usług uzależniony jest od rodzaju i pakietu Usług, z którego korzysta Klient. Bardziej szczegółowe informacje w tym zakresie określone zostały w Załączniku nr 1 do Regulaminu (Pakiety Usług).

KATEGORIE OSÓB, KTÓRYCH DANE DOTYCZĄ:

Osobami, których Dane Dotyczą są wszelkie osoby, których Dane Osobowe, które przekazane zostają KOChM w związku ze świadczonymi Usługami. Do osób tych w szczególności należą:

- Pracownicy i współpracownicy Klienta,
- Klienci Klienta,
- Pacjenci Klienta,
- Opiekunowie prawni Pacjentów,
- Osoby upoważnione przez Pacjentów.

Zakres osób, których Dane Osobowe przetwarzane są w związku ze świadczeniem Usług uzależniony jest od rodzaju Usług, z których korzysta Klient. Bardziej szczegółowe informacje w tym zakresie określone zostały w Załączniku nr 1 do Regulaminu (Pakiety Usług).

ZAŁĄCZNIK B

Lista dalszych podmiotów przetwarzających

KOChM może korzystać z usług następujących dalszych podmiotów przetwarzających:

1. **Asseco Poland S.A. z siedzibą w Rzeszowie** oraz jego dalsze podmioty przetwarzające. Aktualna lista dalszych podmiotów przetwarzających Asseco Poland S.A. jest dostępna pod adresem: https://pl.asseco.com/partnerzy-chmuradlazdrowia/.

2. **Operator Chmury Krajowej sp. z o.o. z siedzibą w Warszawie** (OChK) oraz jego dalsze podmioty przetwarzające, w tym **Google Cloud Poland sp. z o.o. z siedzibą w Warszawie** oraz jego dalsze podmioty przetwarzające. Aktualna lista dalszych podmiotów przetwarzających Google Cloud Poland sp. z o.o. jest dostępna pod adresem: https://cloud.google.com/terms/third-party-suppliers. Podstawą prawną transferu danych są standardowe klauzule umowne zatwierdzone decyzją Komisji Europejskiej, dostępne pod adresem: https://cloud.google.com/terms/eu-model-contract-clause.

3. Inne dalsze podmioty przetwarzające KOChM. Aktualna lista dalszych podmiotów przetwarzających KOChM jest dostępna pod adresem: https://www.chmuradlazdrowia.pl/dalsze-podmioty-przetwarzajace.

ZAŁĄCZNIK C

Wykaz środków technicznych I organizacyjnych, które zobowiązany jest wdrożyć KOChM

RODZAJ ZABEZPIECZENIA	LP.	OPIS STOSOWANYCH ZABEZPIECZEŃ
Lokalizacja przetwarzania	**1)**	Lokalizacja przetwarzania danych została ustalona na region położony na terenie Polski. Możliwe jest wskazanie dokładnych lokalizacji data center.
Zabezpieczenia fizyczne, techniczne, organizacyjne GCP	**2) włó włó**	Opis ogólnych środków bezpieczeństwa danych stosowanych w usługach GCP (Google Cloud Platform): https://cloud.google.com/terms/data-processing-terms/partner
Szyfrowanie danych (at rest i in transit)	**3)**	at rest - szyfrowanie środowiska realizowane jest mechanizmami dostarczanymi przez dostawcę chmury obliczeniowej. Przy czym kluczami kryptograficznymi zarządza KOChM.
	4)	in transit – cała komunikacja jest szyfrowana TLS z wykorzystaniem szyfrów uznanych za bezpieczne.
Konta techniczne i serwisowe oraz poświadczenia dla aplikacji	**5)**	Dane uwierzytelniające wykorzystywane w aplikacji przechowywane są w menadżerze haseł dostarczanym przez operatora chmury obliczeniowej.
	6)	Konta serwisowe zostały utworzone z minimalnymi uprawnieniami, niezbędnymi do działania aplikacji
	7)	Konta wbudowane (default) zostały wyłączone
Interfejsy zarządzania usługami chmury obliczeniowej i dostęp administracyjny/uprzywilejowany	**8)**	Zostały określone interfejsy zarządzania usługami chmury obliczeniowej a dostęp jest przydzielany w oparciu o zasadę minimalnych wymaganych uprawnień
	9)	Została zaimplementowana polityka na poziomie organizacji dla środowiska uruchomionego w GCP
	10)	Połączenia do interfejsów administracyjnych zostały zabezpieczone dodatkową warstwą dostarczającą niezależny proces uwierzytelniania i autoryzacji wykorzystujący 2FA
	11)	Wyłączono bezpośredni dostęp do środowiska z zewnętrznych adresów IP a dostęp możliwy jest tylko przez stację przesiadkową (bastion host) z dodatkową wbudowaną warstwą ochrony oferowaną przez operatora chmury obliczeniowej (2FA).
Uprawnienia, poziomy dostępu i zarządzanie tożsamością	**12)**	Zdefiniowano role użytkowników w oparciu o hierarchię organizacyjną wraz z przypisaniem do nich uprawnień
	13)	Zarządzanie tożsamością zrealizowano w oparciu o mechanizmy dostarczane przez operatora chmury obliczeniowej GCP
	14)	Role przypisywane są do grup przez pracownika spółki posiadającego uprawnienia administratora GCP
	15)	Została globalnie włączona polityka dla haseł (enforce strong, nie zezwalająca na ponowne użycie, min. 12 znaków, wygasanie co 365 dni) i wymuszająca stosowanie 2FA.

Dostępność systemów i usług przetwarzania	**16)**	System został uruchomiony w regionie zlokalizowanym na terenie Polski w skład, którego wchodzą 3 Data Center. Możliwe jest wskazanie dokładnych lokalizacji.
	17)	Środowiska zbudowane zostało w oparciu o skalowalną infrastrukturę kontenerową
Logowanie i audyt	**18)**	Włączono logi audytowe (historia zmian, historia logowania)
	19)	Włączono zbieranie logów na poziomie organizacji i objęto monitoringiem w SIEM OChK
	20)	Wszystkie predefiniowane alerty z systemu dostarczanego przez operatora chmury obliczeniowej objęte zostały monitoringiem w SIEM OChK
Sieć	**21)**	Nie stosuje się domyślnych ustawień sieciowych dostarczanych przez operatora chmury obliczeniowej
	22)	Przydzielono dla środowiska adresację IP przynależną do regionu w którym się znajduje (Polska).
	23)	Interfejsy aplikacji zostały zabezpieczone systemem Web App Firewall (WAF, DDoS)
	24)	Uruchomiono mikrosegmentacja na poziomie distributed Firewall
CI/CD	**25)**	Środowisko jest powoływane a jego wszelkie zmiany wprowadzane automatycznie za pomocą skryptów i mechanizmów dostarczanych przez operatora chmury obliczeniowej.
	26)	Kod przechowywany jest w prywatnym repozytorium Github
		Zaimplementowano rozdzielność środowisk na Dev, Test i Prod
GKE, środowisko kontenerowe	**27)**	Zaimplementowano dedykowaną adresację IP dla środowiska kontenerowego
	28)	Środowisko kontenerowe zostało uruchomione w usłudze zarządzalnej, oferowanej przez operatora chmury obliczeniowej i zabezpieczone zgodnie z best practise GCP.
Bezpieczeństwo aplikacji	**29)**	Źródłem tożsamości dla systemu jest oprogramowanie dziedzinowe, które pełni rolę IdP w asercji SAML
	30)	Komunikacja z usługami jest możliwa wyłącznie poprzez szyfrowany kanał HTTPS, a do szyfrowania został wykorzystany protokół TLS
	31)	Zastosowano mTLS jako mechanizm uwierzytelnienia dwustronnego
	32)	Do zabezpieczenia integralności treści komunikatów zastosowano mechanizm WS-Security
	33)	Aplikacja jest aktualizowane w zakresie poprawek bezpieczeństwa
	34)	Aplikacja posiada środowisko testowe do weryfikowania zmian wprowadzanych na środowisku produkcyjnym
	35)	Aplikacja, przed udostępnieniem jej klientom, została poddana testowi bezpieczeństwa. Zaplanowane są cykliczne testy bezpieczeństwa

Kopie bezpieczeństwa	**36)**	Dla danych medycznych wykonywane są kopie bezpieczeństwa
	37)	Dla logów aplikacyjnych i audytowych wykonywane są kopie bezpieczeństwa
	38)	Kopie zapasowe są szyfrowane