**UMOWA POWIERZENIA**

przetwarzania danych osobowych

zawarta w Szczecinie w dniu …………………………………. r. pomiędzy:

**109 Szpitalem Wojskowym z Przychodnią SP ZOZ w Szczecinie** ul. Piotra Skargi 9-11, 70-965 Szczecin, NIP 851-25-43-558, REGON 810200960, zwanym dalej **„Administratorem”**,

reprezentowanym przez ……………………………… - ………………………………………………..

a

**………………………………………………………………………………………………………...…**, zwaną dalej **„Podmiotem przetwarzającym”**,

reprezentowaną przez ………………………………….. - …………………………………………… ,

dalej zwanymi łącznie **„Stronami”.**

**PREAMBUŁA**

Mając na uwadze, iż Strony zawarły w dniu ……………………………………r. umowę nr ……………………., zwaną w dalszej części Umową główną, której przedmiotem jest ………………………………………………………………………….. (szczegółowy zakres usługi opisano w Umowie głównej), Strony wspólnie uzgodniły, co następuje:

§ 1.

Opis przetwarzania

1. W celu spełnienia obowiązków wynikających z przepisów prawa, a w szczególności zapewnienia przestrzegania art. 28 ust. 3i4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz. Urz. UE L 119 z 04.05.2016), zwanego dalej „rozporządzeniem (UE) 2016/679”, przepisów ustawy o ochronie danych osobowych, zwanej dalej „Ustawą” oraz **właściwej realizacji postanowień Umowy Głównej**, przy uwzględnieniu **standardowych klauzul umownych** /**SKU**/, Administrator powierza w trybie art. 28 rozporządzenia (UE) 2016/679, Podmiotowi przetwarzającemu przetwarzanie danych osobowych, a Podmiot przetwarzający zobowiązuje się przetwarzać dane osobowe zgodnie z niniejszą umową, rozporządzeniem (UE) 2016/679 oraz z innymi przepisami prawa powszechnie obowiązującego, chroniącymi prawa osób, których dane dotyczą.
2. Administrator oświadcza, iż jest administratorem w rozumieniu art. 4 pkt 7) rozporządzenia (UE) 2016/679tj.podmiotem, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
3. Podmiot przetwarzający oświadcza, że jest podmiotem przetwarzającym w rozumieniu art. 4 pkt 8) rozporządzenia (UE) 2016/679 tj. podmiotem, który będzie przetwarzał dane osobowe w imieniu Administratora.
4. Na warunkach określonych w niniejszym paragrafie Administrator powierza przetwarzanie (w rozumieniu, jakie nadaje przetwarzaniu art. 4 pkt 2 rozporządzenia (UE) 2016/679) danych osobowych, których przetwarzanie jest niezbędne do należytego zrealizowania Umowy głównej.
5. Administrator poleca i upoważnia Podmiot przetwarzający do przetwarzania w jego imieniu danych osobowych wyłącznie w celu realizacji postanowień Umowy głównej.
6. Szczegóły dotyczące kategorii osób oraz kategorii danych osobowych, określono w załączniku nr 1 do niniejszej umowy, który stanowi jej integralną część.

§ 2.

Polecenia Administratora/SKU/

1. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo nie zabrania udzielenia takiej informacji z uwagi na ważny interes publiczny. Administrator może wydawać kolejne polecenia przez cały okres przetwarzania danych osobowych. Polecenia te są zawsze dokumentowane.
2. Podmiot przetwarzający bezzwłocznie powiadamia Administratora, jeżeli w opinii Podmiotu przetwarzającego polecenie wydane przez Administratora narusza rozporządzenie (UE) 2016/679 lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.

§ 3.

Ograniczenie celu i czas trwania przetwarzania danych osobowych/SKU/.

1. Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnym celu lub celach przetwarzania, określonych w preambule oraz w § 1 niniejszej umowy, chyba że otrzyma dalsze polecenia od Administratora.
2. Przetwarzanie przez podmiot przetwarzający odbywa się wyłącznie przez okres obowiązywania Umowy Głównej.

§ 4.

Bezpieczeństwo przetwarzania/SKU/

1. W celu zapewnienia bezpieczeństwa danych osobowych Podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w załączniku nr 2, który stanowi integralną część umowy.
2. Zapewnienie bezpieczeństwa danych obejmuje ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych).
3. Oceniając odpowiedni poziom bezpieczeństwa, strony należycie uwzględniają stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz związane z tym ryzyko dla osób, których dane dotyczą.
4. Podmiot przetwarzający udziela członkom swojego personelu dostępu do danych osobowych podlegających przetwarzaniu jedynie w zakresie bezwzględnie niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania.
5. Podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania otrzymanych danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.

§ 5.

Dane wrażliwe/SKU/

Jeżeli przetwarzanie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne do celów jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby, bądź dane dotyczące wyroków skazujących i czynów zabronionych („dane wrażliwe”), podmiot przetwarzający stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia

§ 6.

Dokumentacja i zgodność/SKU/

1. Strony są w stanie wykazać zgodność z niniejszymi zapisami umownymi.
2. Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania Administratora dotyczące przetwarzania danych zgodnie z niniejszymi zapisami umownymi.
3. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, które są określone w niniejszej umowie i wynikają bezpośrednio z rozporządzenia (UE) 2016/679.
4. Na wniosek Administratora Podmiot przetwarzający zezwala również na audyty czynności przetwarzania objętych niniejszą umową i uczestniczy w tych audytach.
5. Audyty te przeprowadza się w rozsądnych odstępach czasu lub jeżeli istnieją przesłanki wskazujące na niezgodność. Podejmując decyzję w sprawie przeglądu lub audytu, Administrator może wziąć pod uwagę odpowiednie certyfikaty, jakie ma podmiot przetwarzający.
6. Administrator może przeprowadzić audyt samodzielnie lub upoważnić do jego przeprowadzenia niezależnego audytora.
7. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego.
8. Audyt przeprowadza się, informując o nich w stosownych przypadkach, z odpowiednim wyprzedzeniem w terminie nie krótszym niż 14 dni przed planowanym terminem jego przeprowadzenia.
9. Na wniosek właściwego(-ych) organu(-ów) nadzorczego(-ych) strony udostępniają mu (im) informacje, o których mowa w niniejszym paragrafie, w tym wyniki wszelkich audytów.

§ 7.

Korzystanie z usług Podmiotów podprzetwarzających- uprzednia szczegółowa zgoda/SKU/

1. Podmiot przetwarzający nie może podzlecać żadnych operacji przetwarzania dokonywanych w imieniu Administratora zgodnie z niniejszą umową Podmiotowi podprzetwarzającemu bez uprzedniej szczegółowej pisemnej zgody Administratora. Podmiot przetwarzający składa wniosek o udzielenie szczegółowej zgody co najmniej 10 dni przed rozpoczęciem korzystania z usług danego Podmiotu podprzetwarzającego wraz z informacjami niezbędnymi do tego, by Administrator mógł podjąć decyzję w sprawie zgody.
2. Załącznik nr 3 zawiera wykaz Podmiotów podprzetwarzających upoważnionych przez Administratora i stanowi integralną część umowy. Strony są obowiązane do aktualizacji załącznika nr 3.
3. Jeżeli Podmiot przetwarzający korzysta z usług Podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu Administratora), dokonuje tego w drodze umowy, która nakłada na Podmiot podprzetwarzający zasadniczo takie same obowiązki w zakresie ochrony danych jak obowiązki nałożone na Podmiot przetwarzający dane zgodnie z niniejszą umową.
4. Podmiot przetwarzający zapewnia, aby Podmiot podprzetwarzający wypełniał obowiązki, którym podlega Podmiot przetwarzający na mocy niniejszej umowy oraz rozporządzenia (UE) 2016/679.
5. Na wniosek Administratora Podmiot przetwarzający przekazuje Administratorowi kopię umowy, jaką zawarł z Podmiotem podprzetwarzającym, a w razie wprowadzenia zmian przekazuje administratorowi jej zaktualizowaną wersję. W zakresie niezbędnym do ochrony tajemnicy handlowej lub innych informacji poufnych, w tym danych osobowych, Podmiot przetwarzający może utajnić tekst umowy przed jej udostępnieniem.
6. Podmiot przetwarzający pozostaje w pełni odpowiedzialny przed Administratorem za wykonanie obowiązków Podmiotu podprzetwarzającego zgodnie z jego umową z Podmiotem przetwarzającym. Podmiot przetwarzający powiadamia Administratora o każdym przypadku niewywiązania się przez Podmiot podprzetwarzający z jego zobowiązań umownych.
7. Podmiot przetwarzający uzgadnia z Podmiotem podprzetwarzającym klauzulę dotyczącą beneficjenta będącego osobą trzecią, zgodnie z którą to klauzulą – jeżeli Podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub stanie się niewypłacalny – Administrator ma prawo rozwiązać umowę z Podmiotem podprzetwarzającym i nakazać mu usunięcie lub zwrot danych osobowych.

§ 8.

Międzynarodowe przekazywanie danych/SKU/

1. Wszelkie przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej przez Podmiot przetwarzający odbywa się wyłącznie na udokumentowane polecenie Administratora lub w celu spełnienia szczególnego wymogu na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega podmiot przetwarzający i odbywa się zgodnie z rozdziałem V rozporządzenia (UE) 2016/679.
2. Jeżeli zgodnie z § 7 Podmiot przetwarzający korzysta z usług Podmiotu podprzetwarzającego w celu przeprowadzenia określonych czynności przetwarzania (w imieniu Administratora), które wiążą się z przekazywaniem danych osobowych w rozumieniu rozdziału V rozporządzenia (UE) 2016/679, Administrator wyraża zgodę na to, by podmioty te mogły zapewnić zgodność z rozdziałem V rozporządzenia (UE) 2016/679 za pomocą standardowych klauzul umownych przyjętych przez Komisję zgodnie z art. 46 ust. 2 rozporządzenia (UE) 2016/679, pod warunkiem, że spełnione są warunki stosowania tych standardowych klauzul umownych.

§ 9.

Pomoc dla Administratora /SKU/

1. Podmiot przetwarzający niezwłocznie zawiadamia Administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Podmiot przetwarzający nie odpowiada na taki wniosek samodzielnie, chyba że Administrator wyraził na to zgodę.
2. Podmiot przetwarzający pomaga Administratorowi w wypełnianiu jego obowiązków dotyczących udzielania odpowiedzi na wnioski osób, których dane dotyczą o skorzystanie z przysługujących im praw z uwzględnieniem charakteru przetwarzania.
3. Wypełniając swoje obowiązki zgodnie z ust. 1. i 2., Podmiot przetwarzający stosuje się do poleceń Administratora.
4. Oprócz spoczywającego na Podmiocie przetwarzającym obowiązku pomagania Administratorowi zgodnie z ust. 2., Podmiot przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje podmiot przetwarzający:
5. obowiązek przeprowadzenia oceny wpływu planowanych operacji przetwarzania na ochronę danych osobowych („ocena skutków dla ochrony danych”), jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;
6. obowiązek skonsultowania się z właściwym(-i) organem(-ami) nadzorczym(-i) przed rozpoczęciem przetwarzania, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu jego ograniczenia;
7. obowiązek zapewnienia prawidłowości i aktualności danych osobowych poprzez niezwłoczne poinformowanie Administratora, jeżeli podmiot przetwarzający stwierdzi, że przetwarzane przez niego dane osobowe są nieprawidłowe lub nieaktualne;
8. obowiązki określone w art. 32 rozporządzenia (UE) 2016/679.
9. Strony określają w załączniku nr 2 odpowiednie środki techniczne i organizacyjne, za pomocą których Podmiot przetwarzający jest zobowiązany pomagać Administratorowi, jak również zakres wymaganej pomocy.

§ 10.

Zgłaszanie naruszenia ochrony danych osobowych/SKU/.

1. W przypadku naruszenia ochrony danych osobowych Podmiot przetwarzający współpracuje z Administratorem i pomaga mu w wypełnianiu jego obowiązków wynikających z art. 33 i 34 rozporządzenia (UE) 2016/679 z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje Podmiot przetwarzający.
2. W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez Administratora Podmiot przetwarzający wspomaga Administratora:
3. przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu(-ym) organowi(-om) nadzorczemu(-ym) niezwłocznie po tym, jak Administrator dowiedział się o naruszeniu, w stosownych przypadkach (chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych);
4. przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 rozporządzenia (UE) 2016/679 powinny być zawarte w zgłoszeniu Administratora i obejmować co najmniej:
   1. charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   2. możliwe konsekwencje naruszenia ochrony danych osobowych;
   3. środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków;
   4. jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki;
5. przy wypełnianiu, zgodnie z art. 34 rozporządzenia (UE) 2016/679, obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.
6. W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez Podmiot przetwarzający Podmiot przetwarzający zgłasza naruszenie Administratorowi niezwłocznie po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać co najmniej:
   1. opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);
   2. dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
   3. wskazanie prawdopodobnych konsekwencji naruszenia oraz środków, które zostały lub mają zostać wprowadzone w celu zaradzenia naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków;
   4. jeżeli przekazanie wszystkich informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.
7. Strony określają w załączniku nr 2 wszystkie inne elementy, które ma przedstawić Podmiot przetwarzający, wspomagając Administratora w wypełnianiu jego obowiązków określonych w art. 33 i 34 rozporządzenia (UE) 2016/679.

§ 11.

Szkolenia jako element zapewnienia bezpieczeństwa danych osobowych

1. Administrator i Podmiot przetwarzający podejmują skuteczne działania mające na celu osiągnięcie i utrzymanie odpowiedniego poziomu kwalifikacji personelu w zakresie przetwarzania danych osobowych, w tym środowiska teleinformatycznego i bezpieczeństwa informacji przetwarzanych w tym środowisku.
2. Administrator i podmiot przetwarzający utrzymują kwalifikacje całego personelu na poziomie odpowiednim dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych, w tym danych przetwarzanych w środowisku teleinformatycznym i umożliwienia właściwego korzystania ze sprzętu i systemów informatycznych. Poziom ten powinien być zróżnicowany w zależności m.in. od ryzyka związanego z poziomem uprawnień i kompetencji poszczególnych pracowników oraz pełnionej przez nich roli przy przetwarzaniu danych osobowych, w tym w systemie zarządzania bezpieczeństwem środowiska teleinformatycznego.
3. W celu zapewnienia odpowiedniego poziomu kwalifikacji personelu w zakresie określonym w ust. 2, Administrator i Podmiot przetwarzający stosują adekwatne formy szkoleń.

§ 12.

Współdziałanie stron

1. Strony ustalają, że podczas realizacji Umowy będą ze sobą ściśle współpracować za pośrednictwem:

1) ze strony Administratora - …………………………………………………………………………..,

tel. ……………………, e-mai: ………………………. ;

2) ze strony Podmiotu przetwarzającego - ……….…………………………………………….………..,

tel. ……………………, e-mail:……………………………. .

2. Strony ustalają, że podczas realizacji Umowy będą informować się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na wykonanie niniejszej Umowy.

§ 13.

Naruszenie zapisów umownych i rozwiązanie umowy/SKU/

* 1. Bez uszczerbku dla przepisów rozporządzenia (UE) 2016/679, w przypadku gdy Podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszej Umowy, Administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy Podmiot przetwarzający zapewni zgodność lub umowa ulega rozwiązaniu. Podmiot przetwarzający niezwłocznie zawiadamia Administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszych zapisów umownych.
  2. Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi zapisami umownymi, jeżeli:

1. Administrator zawiesił przetwarzanie danych osobowych przez Podmiot przetwarzający zgodnie z ust. 1 i jeżeli zgodność nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;
2. Podmiot przetwarzający poważnie lub stale narusza niniejsze zapisy umowne lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679;
3. Podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego(-ych) organu(-ów) nadzorczego(-ych) dotyczącej jego obowiązków wynikających z niniejszych Umowy lub z rozporządzenia (UE) 2016/679;
4. Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszą Umową, jeżeli po zawiadomieniu Administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie zapisami § 2 ust. 2, a Administrator nalega na wypełnienie polecenia.
5. Po rozwiązaniu umowy Podmiot przetwarzający, zależnie od decyzji Administratora, usuwa wszystkie dane osobowe przetwarzane w imieniu Administratora i poświadcza Administratorowi, że tego dokonał, lub zwraca Administratorowi wszystkie dane osobowe i usuwa istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Podmiot przetwarzający zapewnia przestrzeganie niniejszej Umowy do czasu usunięcia lub zwrotu danych.

§ 14.

Postanowienia końcowe

1. Wszelkie decyzje dotyczące przetwarzania danych, odbiegające od ustaleń i instrukcji zawartych w niniejszej Umowie, powinny być przekazywane drugiej stronie w formie pisemnej pod rygorem nieważności i wymagają jej pisemnej akceptacji w formie aneksu.
2. W sprawach nieuregulowanych niniejszą Umową, zastosowanie mają odpowiednio przepisy prawa w tym odpowiednio przepisy Ustawy, rozporządzenia(UE) 2016/679 oraz przepisy Kodeksu cywilnego.
3. Spory wynikające z niniejszej Umowy będą rozstrzygane przez właściwy rzeczowo sąd powszechny w Szczecinie.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, jeden dla Podmiotu przetwarzającego, jeden dla Administratora.

**Administrator Podmiot Przetwarzający**

|  |  |
| --- | --- |
| Podpis, pieczątka imienna | Podpis, pieczątka imienna |
| Pieczęć firmowa | Pieczęć firmowa |

**Załącznik nr 1** do umowy powierzenia przetwarzania danych osobowych – opis przetwarzania.

* + 1. Rodzaj danych osobowych **-** dane zwykłe

|  |  |
| --- | --- |
| **Kategorie osób których dane dotyczą** | **Kategorie danych osobowych** |
|  |  |
|  |  |

* + 1. Rodzaj danych osobowych: dane szczególnych kategorii art. 9 ust. 1 rozporządzenia(UE) 2016/679.

|  |  |
| --- | --- |
| **Kategorie osób których dane dotyczą** | **Kategorie danych osobowych** |
|  |  |

* + 1. Przetwarzanie danych osobowych o których mowa w art. 10 ust. 1rozporządzenia(UE) 2016/679.

|  |  |
| --- | --- |
| **Kategorie osób których dane dotyczą** | **Kategorie danych osobowych** |
| N |  |

**Charakter przetwarzania***( okres, skala, częstotliwość i powtarzalność przetwarzania danych).*

* …………………………………………………………………………………………………….

**Cel(e), w którym(-ych) dane osobowe są przetwarzane w imieniu administratora:**

* Tak jak w umowie głównej.

**Czas trwania przetwarzania:**

* Tak jak w umowie głównej

*(W przypadku przetwarzania przez podmioty podprzetwarzające należy również określić przedmiot, charakter i czas trwania przetwarzania).*

**Załącznik nr 2** do umowy powierzenia przetwarzania danych osobowych – środki organizacyjne i techniczne stosowane przez Podmiot przetwarzający w celu zapewnienia bezpieczeństwa danych.

|  |  |  |
| --- | --- | --- |
| **Opis technicznych i organizacyjnych środków bezpieczeństwa wdrożonych przez podmiot przetwarzający (podmioty przetwarzające) (w tym wszelkie stosowne certyfikaty) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania, a także ryzyka naruszenia praw i wolności osób fizycznych.** | **ODPOWIEDŹ** | |
| **Proszę zaznaczyć znak „x” w odpowiedniej rubryce** | **Uwagi2** |
| Czy Wykonawca**[[1]](#footnote-2)** wprowadził udokumentowane polityki ochrony danych osobowych? | Tak  Nie |  |
| Czy Wykonawca wprowadził procedury zabezpieczania systemów informatycznych dotyczące ochrony danych osobowych? | Tak  Nie |  |
| Czy Wykonawca zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych jest odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa? | Tak  Nie |  |
| Czy pracownicy Wykonawcy, którzy uczestniczą w operacjach przetwarzania danych osobowych zostali zobowiązani do zachowania ich w tajemnicy? | Tak  Nie |  |
| Czy Wykonawca korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? | Tak  Nie |  |
| Czy Wykonawca stosuje środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? | Tak  Nie |  |
| Czy dostęp do pomieszczeń pozostających w dyspozycji Wykonawcy po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany? | Tak  Nie |  |
| Czy każdy pracownik Wykonawcy jako otrzymuje imienny identyfikator do systemów informatycznych? | Tak  Nie |  |
| Czy w organizacji Wykonawcy jest stosowana polityka haseł? | Tak  Nie |  |
| Czy w organizacji Wykonawcy jest stosowana polityka czystego ekranu? | Tak  Nie |  |
| Czy w organizacji Wykonawcy jest stosowana polityka czystego biurka? | Tak  Nie |  |
| Czy Wykonawca przeprowadza okresowe analizy ryzyka utraty integralności, dostępności, poufności oraz podejmuje działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy? | Tak  Nie |  |
| Czy Wykonawca wdraża nowe rozwiązania zgodnie z zasadą prywatności w fazie projektowania (privacy by design) w kontekście przetwarzania danych przekazanych przez Administratora? | Tak  Nie |  |
| Czy Wykonawca prowadzi ocenę skutków dla ochrony danych – art.35rozporządzeniem (UE) 2016/679? | Tak  Nie |  |
| Czy Wykonawca zapewnienia odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, polegający w szczególności na:  a) dbałości o aktualizację oprogramowania,  b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,  c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,  d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,  e) zapewnieniu bezpieczeństwa plików systemowych,  f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,  g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,  h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa. | Tak Nie  Tak Nie  Tak Nie  Tak Nie  Tak Nie  Tak Nie  Tak Nie  Tak Nie |  |
| Czy Wykonawca podejmuje działania zapewniające, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia oraz uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa? | Tak  Nie |  |
| Czy rozliczalność w systemach teleinformatycznych Wykonawcy podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów (logach)? | Tak  Nie |  |
| Czy Wykonawca stosuje podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu danych w systemie mobilnym i pracy na odległość? | Tak  Nie |  |
| Czy Wykonawca wdrożył środki zapewniające minimalizację danych? | Tak  Nie |  |
| Czy Wykonawca zapewnienia odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych, w których prowadzona jest dokumentacja medyczna, w tym zapewnia co najmniej:  1) integralność treści dokumentacji i metadanych polegającą na zabezpieczeniu przed wprowadzaniem zmian, z wyjątkiem zmian wprowadzanych w ramach udokumentowanych procedur;  2) stały dostęp do dokumentacji dla osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych;  3) wymagalność identyfikacji osoby sporządzającej dokumentację oraz dokonującej wpisu lub innej zmiany i zakresu dokonanych zmian w dokumentacji lub metadanych;  4) informację o czasie sporządzenia dokumentacji oraz dokonania wpisu lub innej zmiany;  5) przyporządkowanie cech informacyjnych dla odpowiednich rodzajów dokumentacji, zgodnie z § 10 pkt 3 Rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania;  6) możliwość prowadzenia i udostępniania dokumentacji w formatach i standardach wydanych na podstawie art.  11 ust. 1a i 1b ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2021 r. poz. 666.), a  w  przypadku ich braku – możliwość prowadzenia i  udostępniania dokumentacji w  standardach HL7 oraz DICOM lub innych standardach i formatach;  7) możliwość wydruku dokumentacji;  8) możliwość eksportu całości danych w standardach i formatach, o których mowa w pkt 6, w sposób umożliwiający odtworzenie ich w innym systemie teleinformatycznym. | Tak Nie  Tak Nie  Tak Nie  Tak Nie  Tak Nie  Tak Nie  Tak Nie  Tak Nie |  |
| Czy Wykonawca wdrożył środki umożliwiające identyfikację i autoryzację użytkowników? | Tak  Nie |  |
| Czy Wykonawca zapewnia ochronę danych w czasie ich przechowywania? | Tak  Nie |  |
| Czy Wykonawca stosuje środki zapewniające ograniczone zatrzymywanie danych? | Tak  Nie |  |
| Czy Wykonawca wdrożył środki umożliwiające przenoszenie danych i zapewnienie ich usuwania? | Tak  Nie |  |
| Czy Wykonawca zapewnia ochronę danych w czasie ich przekazywania? | Tak  Nie |  |
| Czy Wykonawca zapewnia rozliczalność w rozumieniu art.5 ust.2 rozporządzenia (UE) 2016/679? | Tak  Nie |  |
| Czy Wykonawca wdrożył środki umożliwiające pseudoanonimizację i/lub szyfrowanie danych? | Tak  Nie |  |
| Czy Wykonawca stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 Rozporządzenia lub zatwierdzony mechanizm certyfikacji o którym mowa w art. 42 Rozporządzenia? | Tak  Nie |  |
| Czy Wykonawca posiada Certyfikat ISO/IEC 27001? | Tak  Nie |  |

**Załącznik nr 3** do umowy powierzenia przetwarzania danych osobowych - wykaz podmiotów Podprzetwarzających.

|  |  |  |
| --- | --- | --- |
|  | **Dane podmiotu podprzetwarzającego:** | |
|  | Imię i nazwisko lub nazwa: | Podmiot przetwarzający nie powierza danych osobowych objętych niniejszą umową podmiotom podprzetwarzającym. |
| Adres: |  |
| Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: |  |
| Opis przetwarzania (w tym jasne określenie odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających): |  |

1. Wykonawca wypełnia zadania zgodnie z definicją „podmiotu przetwarzającego” w trybie art. 4 pkt 8 RODO.

   2 Administrator prosi uzupełnić rubrykę w przypadku kiedy odpowiedź wymaga dodatkowego komentarza; kiedy Wykonawca jest zwolniony na podstawie przepisu prawa z realizacji zadania bądź zadanie Wykonawcy nie dotyczy. [↑](#footnote-ref-2)