

Umowa powierzenia przetwarzania danych osobowych

zawarta dniapomiędzy:

10 Wojskowym Szpitalem Klinicznym z Polikliniką S.P.Z.O.Z. w Bydgoszczy
reprezentowaną przez:

płk dr n. med. Sławomir WAWRZYŃIAK – Komendanta Szpitala

zwanym w dalszej części umowy „**Administratorem Danych**” lub „**Administratorem**”,

a

....., z siedzibą w, ul., wpisaną do Rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla M.St. Warszawy w Warszawie XIII Wydział Gospodarczy Krajowego Rejestru Sądowego nr KRS:, REGON, NIP

zwanym w dalszej części umowy „**Podmiotem przetwarzającym**”

zwane w treści umowy łącznie również Stronami, o następującej treści:

§ 1

Preambuła

Niniejsza umowa została sporządzona w oparciu o wymogi wskazane w art. 28 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 w oparciu o Decyzję wykonawczą komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679.

§ 2

Definicje

1. „Dane osobowe” - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”) zebrane w celu realizacji umowy z dnia.....
2. „Dane osobowe szczególnej kategorii” – zakres danych osobowych wskazanych w art. 9 ust. 1 RODO.
3. „Państwo trzecie” – państwo nienależące do Europejskiego Obszaru Gospodarczego.
4. „Podmiot trzeci” - 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.
5. „Przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
6. „Rozporządzenie” - 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 – RODO.
7. „Ustawa” – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
8. „Decyzja” - DECYZJA WYKONAWCZA KOMISJI (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725.

§ 3

Standardowe klauzule umowne

A. Cel i zakres

1. Celem niniejszych standardowych klauzul umownych („klauzule”) jest zapewnienie przestrzegania art. 28 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 (ogólne rozporządzenie o ochronie danych).
2. Administratorzy i podmioty przetwarzające wymienieni w załączniku I uzgodnili niniejsze klauzule w celu zapewnienia przestrzegania art. 28 rozporządzenia (UE) 2016/679 lub art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725.
3. Niniejsze klauzule mają zastosowanie do przetwarzania danych osobowych określonego w załączniku II.
4. Załączniki I–III stanowią integralną część umowy.
5. Niniejsze klauzule pozostają bez uszczerbku dla obowiązków, którym podlega administrator danych na mocy rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.
6. Niniejsze klauzule same w sobie nie zapewniają wypełnienia obowiązków związanych z międzynarodowym przekazywaniem danych zgodnie z rozdziałem V rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725.

B. Niezmiennność klauzul

1. Strony zobowiązują się nie zmieniać klauzul z wyjątkiem dodawania informacji do załączników lub aktualizowania zawartych w nich informacji.
2. Postanowienie to nie uniemożliwia stronom umieszczania standardowych klauzul umownych określonych w niniejszych klauzulach w treści umowy o szerszym zakresie ani dodawania innych klauzul lub dodatkowych zabezpieczeń, pod warunkiem, że nie będą one bezpośrednio lub pośrednio sprzeczne z klauzulami umownymi ani nie będą naruszały podstawowych praw lub wolności osób, których dane dotyczą.

C. Wykładnia

1. Jeżeli w niniejszych klauzulach użyto terminów zdefiniowanych w rozporządzeniu (UE) 2016/679 - RODO, terminy te mają takie samo znaczenie jak w rozporządzeniu.
2. Niniejsze klauzule odczytuje się i interpretuje w świetle odpowiednio przepisów rozporządzenia (UE) 2016/679 - RODO.
3. Niniejszych klauzul nie interpretuje się w sposób sprzeczny z prawami i obowiązkami przewidzianymi w rozporządzeniu (UE) 2016/679 - RODO ani w sposób naruszający podstawowe prawa lub wolności osób, których dane dotyczą.

D. Hierarchia

1. W razie sprzeczności między niniejszymi klauzulami a postanowieniami powiązanych umów między stronami istniejących w chwili uzgadniania niniejszych klauzul lub zawartych po ich uzgodnieniu, pierwszeństwo mają niniejsze klauzule.

§ 4

OBOWIĄZKI STRON

A. Opis przetwarzania

1. Szczegóły dotyczące operacji przetwarzania, w szczególności kategorie danych osobowych i cele, dla których dane osobowe są przetwarzane w imieniu administratora, określono w załączniku II.

B. Obowiązki stron

1. Polecenia.

- a) 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.
- b) Poprzez zawarcie Umowy Administrator poleca przetwarzanie danych osobowych Przetwarzającemu, a także każdej osobie działającej z upoważnienia Podmiotu przetwarzającego mającej dostęp do danych osobowych, co stanowi udokumentowane polecenie w rozumieniu art. 28 ust. 3 lit. a) w związku z art. 29 RODO.
- c) Podmiot przetwarzający bezzwłocznie - w ciągu 48 godzin powiadamia administratora, jeżeli w opinii podmiotu przetwarzającego polecenie wydane przez administratora narusza rozporządzenie (UE) 2016/679 - RODO lub obowiązujące przepisy Unii lub państwa członkowskiego o ochronie danych.

2. Ograniczenie celu.

- a) Podmiot przetwarzający przetwarza dane osobowe wyłącznie w konkretnym celu lub celach przetwarzania, określonych w załączniku II, chyba że otrzyma dalsze polecenia od administratora.

3. Czas trwania przetwarzania danych osobowych.

- a) Przetwarzanie przez podmiot przetwarzający odbywa się wyłącznie przez okres określony w załączniku II.

4. Bezpieczeństwo przetwarzania (art. 32 RODO).

- a) W celu zapewnienia bezpieczeństwa danych osobowych podmiot przetwarzający wdraża co najmniej środki techniczne i organizacyjne określone w załączniku III. 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). 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.
- b) 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. 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 – dane osobowe szczególnej kategorii.

- a) 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.

- a) Strony są w stanie wykazać zgodność z niniejszymi klauzulami.
- b) Podmiot przetwarzający niezwłocznie (nie później niż w terminie 7 dni) i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszymi klauzulami.

- c) Podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, które są określone w niniejszych klauzulach i wynikają bezpośrednio z rozporządzenia (UE) 2016/679 – RODO. Na wniosek administratora podmiot przetwarzający zezwala również na audyty czynności przetwarzania objętych niniejszymi klauzulami i uczestniczy w tych audytach. Audyty te przeprowadza się w rozsądnych odstępach czasu lub jeżeli istnieją przesłanki wskazujące na niezgodność.
- d) Administrator może przeprowadzić audyt samodzielnie lub upoważnić do jego przeprowadzenia niezależnego audytora. Audyty mogą również obejmować inspekcje w pomieszczeniach lub obiektach fizycznych podmiotu przetwarzającego. Audyty te przeprowadza się, informując o nich, w stosownych przypadkach, z odpowiednim wyprzedzeniem.
- e) Na wniosek właściwego(-ych) organu(-ów) nadzorczego(-ych) strony udostępniają mu (im) informacje, o których mowa w niniejszej klauzuli, w tym wyniki wszelkich audytów.

7. Korzystanie z usług podmiotów podprzetwarzających.

a) OGÓLNA PISEMNA ZGODA:

Podmiot przetwarzający ma ogólną zgodę administratora na korzystanie z usług podmiotów podprzetwarzających wpisanych do uzgodnionego wykazu. Podmiot przetwarzający informuje administratora na piśmie o wszelkich zamierzonych zmianach, w tym wykazie polegających na dodaniu lub zastąpieniu podmiotów podprzetwarzających z wyprzedzeniem co najmniej 14 dniowym, dając tym samym administratorowi wystarczająco dużo czasu na wyrażenie sprzeciwu wobec takich zmian przed rozpoczęciem korzystania z usług danego podmiotu podprzetwarzającego (podmiotów podprzetwarzających). Podmiot przetwarzający przekazuje administratorowi niezbędne informacje umożliwiające mu skorzystanie z prawa sprzeciwu.

- b) 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 niniejszymi klauzulami. Podmiot przetwarzający zapewnia, aby podmiot podprzetwarzający wypełniał obowiązki, którym podlega podmiot przetwarzający na mocy niniejszych klauzul oraz rozporządzenia (UE) 2016/679 – RODO.
- c) 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.
- d) 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.
- e) 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 zgodnie z art. 28 ust.3 pkt g RODO.

§ 5

Pomoc dla administratora

- a) 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 pisemną zgodę.
- b) 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. Wypełniając swoje obowiązki zgodnie z lit. a) i b), podmiot przetwarzający stosuje się do poleceń administratora.
- c) Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie § 4 lit. b) podmiot przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje podmiot przetwarzający:
 - 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;
 - 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;
 - 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;
 - obowiązki określone w art. 32 rozporządzenia (UE) 2016/679 – RODO.
- d) Strony określają w załączniku III odpowiednie środki techniczne i organizacyjne, za pomocą których podmiot przetwarzający jest zobowiązany pomagać administratorowi w stosowaniu niniejszej klauzuli, jak również zakres wymaganej pomocy.

§ 6

Zgłaszanie naruszenia ochrony danych osobowych

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 – RODO z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje podmiot przetwarzający.

§ 7

A. Naruszenie ochrony danych dotyczące danych przetwarzanych przez administratora.

1. W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający wspomaga administratora:
 - a) 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);
 - b) Przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 Rozporządzenia (UE) 2016/679 RODO powinny być zawarte w zgłoszeniu administratora i obejmować co najmniej:
 - datę czas trwania oraz lokalizację naruszenia ochrony danych;
 - 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;
 - możliwe konsekwencje naruszenia ochrony danych osobowych;
 - dane kontaktowe osoby mogącej udzielić dalszych informacji o naruszeniu;

- 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.
2. 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;
 3. Przy wypełnianiu – zgodnie z art. 34 Rozporządzenia (UE) 2016/679 RODO – 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.

B. Naruszenie ochrony danych dotyczące danych przetwarzanych przez podmiot przetwarzający.

1. W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez podmiot przetwarzający podmiot przetwarzający zgłasza naruszenie administratorowi niezwłocznie nie później niż w ciągu **24 godzin** po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać co najmniej:
 - datę czas trwania oraz lokalizację naruszenia ochrony danych;
 - 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;
 - możliwe konsekwencje naruszenia ochrony danych osobowych;
 - dane kontaktowe osoby mogącej udzielić dalszych informacji o naruszeniu;
 - 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.
2. 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.
3. Strony określają w **załączniku III** wszystkie inne elementy, które ma przedstawić podmiot przetwarzający, wspomagając administratora w wypełnianiu jego obowiązków określonych w art. 33 i 34 rozporządzenia (UE) 2016/679 – RODO.

§ 8

Postanowienia końcowe

1. Naruszenie klauzul (zapisów umowy) i rozwiązanie umowy.

- a) Bez uszczerbku dla przepisów rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725, w przypadku, gdy podmiot przetwarzający narusza swoje obowiązki wynikające z niniejszych klauzul, administrator może polecić mu, by zawiesił przetwarzanie danych osobowych do czasu, gdy podmiot przetwarzający zapewni zgodność z niniejszymi klauzulami, lub umowa ulega rozwiązaniu. Podmiot przetwarzający niezwłocznie zawiadamia administratora, jeżeli z jakiegokolwiek powodu nie jest w stanie zastosować się do niniejszych klauzul.
- b) Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli:
 - administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z lit. a) i jeżeli zgodność z niniejszymi klauzulami nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;
 - podmiot przetwarzający poważnie lub stale narusza niniejsze klauzule lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679 – RODO;
 - podmiot przetwarzający nie stosuje się do wiążącej decyzji właściwego sądu lub właściwego

(-ych) organu(-ów) nadzorczego(-ych) dotyczącej jego obowiązków wynikających z niniejszych klauzul lub z rozporządzenia (UE) 2016/679 – RODO.

- c) Podmiot przetwarzający ma prawo rozwiązać umowę w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli po zawiadomieniu administratora o tym, że jego polecenie narusza obowiązujące wymogi prawne zgodnie z § 4.B.1.b) administrator nalega na wypełnienie polecenia.
- d) Po rozwiązaniu umowy podmiot przetwarzający, zależnie od decyzji administratora, usuwa wszystkie dane osobowe przetwarzane w imieniu administratora i poświadcza pisemnie 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 niniejszych klauzul do czasu usunięcia lub zwrotu danych.
- e) Wykonanie w/w czynności przez podmiot przetwarzający następuje natychmiast po rozwiązaniu umowy/ po okresie 30 dni od rozwiązania umowy*.

Administrator

Podmiot przetwarzający

.....

.....

Wykaz stron

Administrator (administratorzy): [dane identyfikacyjne i kontaktowe administratora (administratorów) oraz w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez administratora]

10 Wojskowym Szpitalem Klinicznym z Polikliniką S.P.Z.O.Z. w Bydgoszcy, ul. Powstańców Warszawy 5, 85-681 Bydgoszcz,

..... nr tel: email:

..... tel: email.

Podmiot przetwarzający (podmioty przetwarzające):

.....

Opis przetwarzania

Kategorie osób, których dane osobowe są przetwarzane:

Dane osobowe (należy wymienić jakie dane osobowe będą przetwarzane)

- DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii;

Kategorie przetwarzanych danych osobowych:

Dane osobowe zwykłej kategorii oraz dane osobowe szczególnej kategorii przetwarzane w związku z czynnościami podejmowanymi na mocy w/w przepisów. (dane osobowe szczególnej kategorii, to m.in. dane dotyczące stanu zdrowia- widoczne oznaki inwalidztwa)

Charakter przetwarzania:

Przetwarzanie danych osobowych przy wykorzystaniu systemów informatycznych (jakich np. monitoring wizyjny)przetwarzanie danych o charakterze ciągłym. Wykonywanie takich operacji jak: zbieranie, utrwalanie, przechowywanie, usuwanie.

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

Realizacja umowy głównej tj. dostęp do systemu, przechowywanie danych osobowych na serwerach podmiotu przetwarzającego, zabezpieczania dobowych kopii systemu baz danych w data-center, usuwanie nieprawidłowości w działaniu oprogramowania lub serwera.

Czas trwania przetwarzania:

Okres obowiązywania umowy głównej.

Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa danych stosowane przez podmiot przetwarzający (przykład – proszę wybrać lub wpisać swoje środki)

Środki organizacyjne:

1. *Polityka bezpieczeństwa ochrony danych osobowych – art. 25 ust. 2 RODO;*
2. *Rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania, o których mowa w art. 30 RODO;*
3. *Wytyczne dotyczące klasyfikacji naruszeń i procedurę zgłaszanie naruszenie ochrony danych do organu nadzorczego (UODO) – art. 33 ust 3 RODO;*
4. *Procedurę na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób, w zakresie ich informowaniu o działaniach jakie powinni wykonać, aby ryzyko to ograniczyć – art. 34 RODO*
5. *Procedurę prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO;*
6. *Raport z przeprowadzonej, ogólnej analizy ryzyka – art. 25 ust. 1 RODO;*
7. *Raport z ocen skutków dla ochrony danych – art. 35 ust. 7;*
8. *Procedury związane z pseudonimizacją i szyfrowaniem;*
9. *Plan ciągłości działania – art. 32 ust 1 pkt b RODO;*
10. *Procedury odtwarzania systemu po awarii oraz ich testowania – art. 32 ust 1 pkt c i d RODO.*
11. *Wyznaczona została osoba pełniąca funkcję IOD godnie z Ustawą oraz RODO;*
12. *Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych gwarantująca rozliczalność procesów przetwarzania danych osobowych, zapewnienie poufności, integralności, dostępności przetwarzanych danych osobowych oraz usług przetwarzania.*

Środki techniczne:

1. *Zastosowanie rozwiązania w zakresie ochrony przed złośliwym oprogramowaniem;*
2. *Stosowanie rozwiązań i procedur w zakresie bezpiecznego dostępu do informacji na stacjach roboczych i laptopach;*
3. *Stosowanie rozwiązań w zakresie bezpiecznego uwierzytelniania i autoryzacji oraz bezpiecznego zarządzania hasłami;*
4. *Stosowanie mechanizmów w zakresie transmisji danych;*
5. *Zapewnienie niezbędnych informacji do wyjaśnienia incydentów (np. rejestry logów, informacji z narzędzi monitorujących).*