Załącznik nr 2 do umowy …. z dnia …..

*projekt*

**Standardowe klauzule umowne w zakresie powierzenia danych osobowych zatwierdzone decyzją wykonawczą Komisji (UE) 2021/915 z dn. 4.06.2021 r.**

**SEKCJA I**

Klauzula 1

**Cel i zakres**

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

Klauzula 2

**Niezmienność 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.

Klauzula 3

**Wykładnia**

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

Klauzula 4

**Hierarchia**

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.

*Klauzula 5 – fakultatywna*

***Klauzula przystąpienia***

1. Każdy podmiot niebędący stroną niniejszych klauzul może za zgodą wszystkich stron przystąpić do niniejszych klauzul jako administrator lub podmiot przetwarzający w dowolnym czasie, wypełniając załączniki i podpisując załącznik I.
2. Po wypełnieniu i podpisaniu załączników wymienionych w lit. a) podmiot przystępujący jest traktowany jako strona niniejszych klauzul i ma prawa i obowiązki administratora lub podmiotu przetwarzającego, zgodnie z rolą nadaną mu w załączniku I.
3. Przed przystąpieniem do niniejszych klauzul jako ich strona podmiot przystępujący nie ma żadnych praw ani obowiązków wynikających z niniejszych klauzul.

SEKCJA II

**OBOWIĄZKI STRON**

Klauzula 6

**Opis przetwarzania**

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

Klauzula 7

**Obowiązki stron**

7.1. **Polecenia**

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.

7.2. **Ograniczenie celu**

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

7.3. **Czas trwania przetwarzania danych osobowych**

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

7.4. **Bezpieczeństwo przetwarzania**

1. 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.
2. 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.

7.5. **Dane szczególnych kategorii**

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 szczególnych kategorii”), podmiot przetwarzający stosuje szczególne ograniczenia lub dodatkowe zabezpieczenia.

7.6. **Dokumentacja i zgodność**

1. Strony są w stanie wykazać zgodność z niniejszymi klauzulami.
2. Podmiot przetwarzający niezwłocznie i odpowiednio rozpatruje zapytania administratora dotyczące przetwarzania danych zgodnie z niniejszymi klauzulami.
3. 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. 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. Podejmując decyzję w sprawie przeglądu lub audytu, administrator może wziąć pod uwagę odpowiednie certyfikaty, jakie ma podmiot przetwarzający.
4. 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.
5. Na wniosek właściwego(-ych) organu(-ów) nadzorczego(-ych) strony udostępniają mu (im) informacje, o których mowa w niniejszej klauzuli, w tym wyniki wszelkich audytów.

7.7. **Korzystanie z usług podmiotów podprzetwarzających**

1. UPRZEDNIA SZCZEGÓŁOWA ZGODA: Podmiot przetwarzający nie może podzlecać żadnych operacji przetwarzania dokonywanych w imieniu administratora zgodnie z niniejszymi klauzulami podmiotowi podprzetwarzającemu bez uprzedniej szczegółowej pisemnej zgody administratora. Podmiot przetwarzający składa wniosek o udzielenie szczegółowej zgody co najmniej 14 dni przed rozpoczęciem korzystania z usług danego pod­ miotu podprzetwarzającego wraz z informacjami niezbędnymi do tego, by administrator mógł podjąć decyzję w sprawie zgody. Załącznik IV zawiera wykaz podmiotów podprzetwarzających upoważnionych przez administratora. Strony są obowiązane do aktualizacji załącznika IV.
2. 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.
3. 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.
4. 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.
5. 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.

7.8. **Międzynarodowe przekazywanie danych**

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 klauzulą 7.7 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.

Klauzula 8

**Pomoc dla administratora**

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. Wypełniając swoje obowiązki zgodnie z lit. a) i b), podmiot przetwarzający stosuje się do poleceń administratora.
3. Oprócz spoczywającego na podmiocie przetwarzającym obowiązku pomagania administratorowi zgodnie z klauzulą 8 lit. b) podmiot przetwarzający pomaga mu ponadto w zapewnieniu wypełniania następujących obowiązków, z uwzględnieniem charakteru przetwarzania danych oraz informacji, którymi dysponuje podmiot przetwarzający:
4. 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;
5. 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;
6. 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;
7. obowiązki określone w art. 32 rozporządzenia (UE) 2016/679.
8. 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.

Klauzula 9

**Zgłaszanie naruszenia ochrony danych osobowych**

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.

9.1. **Naruszenie ochrony danych dotyczące danych przetwarzanych przez administratora**

1. W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez administratora podmiot przetwarzający wspomaga administratora:
2. 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);
3. 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:
4. 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;
5. możliwe konsekwencje naruszenia ochrony danych osobowych;
6. 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.
7. 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;
8. 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.

9.2. **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 po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać co najmniej:
2. opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);
3. dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
4. 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.
5. 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.
6. 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.

SEKCJA III

**POSTANOWIENIA KOŃCOWE**

Klauzula 10

**Naruszenie klauzul i rozwiązanie umowy**

1. Bez uszczerbku dla przepisów rozporządzenia (UE) 2016/679, 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.
2. Administrator jest uprawniony do rozwiązania umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych zgodnie z niniejszymi klauzulami, jeżeli:
3. administrator zawiesił przetwarzanie danych osobowych przez podmiot przetwarzający zgodnie z pkt 1 i jeżeli zgodność z niniejszymi klauzulami nie zostanie przywrócona w rozsądnym terminie, a w każdym razie w terminie jednego miesiąca od zawieszenia;
4. podmiot przetwarzający poważnie lub stale narusza niniejsze klauzule lub swoje obowiązki wynikające z rozporządzenia (UE) 2016/679;
5. 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.
6. 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 klauzulą 7.1 lit. b), administrator nalega na wypełnienie polecenia.
7. 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 niniejszych klauzul do czasu usunięcia lub zwrotu danych.

ZAŁĄCZNIK I

**Wykaz stron**

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

 Imię i nazwisko lub nazwa: ...............................................................

Adres: ...............................................................................................

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

Sławomir Mazur, tel. 727931623, e-mail: iod@sokolniki.pl

Podpis i data przystąpienia: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Podmiot przetwarzający (podmioty przetwarzające):** [dane identyfikacyjne i kontaktowe podmiotu przetwarzającego (podmiotów przetwarzających) oraz, w stosownych przypadkach, inspektora ochrony danych wyznaczonego przez podmiot przetwarzający]

Imię i nazwisko lub nazwa: ……………………………………………………………

Adres: ……………………………………………………………………………………………

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów:

………………………………………………………………………………………………………

Podpis i data przystąpienia: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ZAŁĄCZNIK II

**Opis przetwarzania**

Kategorie osób, których dane osobowe są przetwarzane:

**Właściciele posesji**

Kategorie przetwarzanych danych osobowych:

Dane zwykłe dotyczące **właścicieli posesji w zakresie danych identyfikacyjnych, adresowych, kontaktowych, w ramach realizacji zadań związanych z budową przydomowych oczyszczalni ścieków**

Przetwarzane dane szczególnych kategorii (w stosownych przypadkach) oraz stosowane ograniczenia lub zabezpieczenia, które w pełni uwzględniają charakter danych i związane z nimi zagrożenia, takie jak na przykład ścisłe ograniczenie celu, ograniczenia dostępu (w tym dostęp wyłącznie dla personelu, który odbył specjalistyczne szkolenie), prowadzenie rejestru dostępu do danych, ograniczenia dotyczące dalszego przekazywania danych lub dodatkowe środki bezpieczeństwa.

**Dane szczególnych kategorii nie będą przetwarzane**

Charakter przetwarzania:

**Przetwarzanie danych obejmuje wykonywanie na danych takich czynności jak odczytywanie, zapisywanie, przechowywanie, przesyłanie i sporządzanie kopii serwisowych.**

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

**na podstawie Umowy nr ………………………. z dnia ………………………….. r. o realizację budowy przydomowych oczyszczalni ścieków**

Czas trwania przetwarzania:

**Przez okres związany z realizacją inwestycji oraz w obowiązkowym okresie przechowywania, ustalanym zgodnie z odrębnymi przepisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.**

W przypadku przetwarzania przez podmioty przetwarzające lub podprzetwarzające należy również określić przedmiot, charakter i czas trwania przetwarzania.

ZAŁĄCZNIK III

**Środki techniczne i organizacyjne, w tym środki techniczne i organizacyjne w celu zapewnienia**

**bezpieczeństwa danych**

1. 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:

***(środki bezpieczeństwa, jakimi dysponuje Wykonawca, zostaną wskazane z poniższego katalogu, zgodnie z częścią A. ankiety wg Załącznika V do niniejszego projektu umowy)***

1. Zapewnienie poufności
* Kontrola dostępu – zakaz nieuprawnionego dostępu do pomieszczeń, w których przetwarzane są dane osobowe, np.: karty magnetyczne lub chipowe, klucze, pracownicy ochrony, systemy alarmowe, systemy monitoringu.
* Kontrola dostępu – zakaz nieuprawnionego korzystania z systemu, np.: bezpieczne hasła, automatyczne mechanizmy blokujące, uwierzytelnianie dwuskładnikowe, szyfrowanie nośników danych.
* Kontrola dostępu – zakaz nieuprawnionego odczytywania, kopiowania, zmieniania lub usuwania danych w systemie, np.: określenie sposobów autoryzacji i prawa dostępu, logowanie dostępu.
* Kontrola oddzielenia danych poprzez separację przetwarzania danych zebranych w różnych celach.
1. Kontrola bezpieczeństwa sieci
* Do kontroli bezpieczeństwa sieci wykorzystywana jest zapora sieciowa (firewall);
* Do wdrożenia kontroli dostępu do sieci, system wykrywania włamań/system system zapobiegania włamaniom (Intrusion Detection System / Intrusion Prevention System – IDS/IPS) do ochrony przez znanymi, nieznanymi i nieujawnionymi lukami;
* Zastosowano bezpieczną bramkę internetową do kontroli aplikacji z funkcją wykrywania exploitów zero-day, zaawansowane skanowanie pod katem złośliwego oprogramowania, reputację sieci w czasie rzeczywistym oraz elastyczne filtrowanie adresów URL, w celu zapewnienia najwyższej jakości ochrony przed zagrożeniami internetowymi.
1. Kontrola punktu końcowego
* Stosowane są rozwiązania z zakresu bezpieczeństwa punktów końcowych, w tym szyfrowanie i pseudonimizacja wraz z automatycznym uczeniem się o wysokiej dokładności, analiza behawioralna, ochrona przed exploitami i zaawansowana ochrona przed wariantami złośliwego oprogramowania, ochrona przed exploitami sieciowymi, reputacja sieci itp. w celu ochrony przed zagrożeniami i złośliwym oprogramowaniem.
1. Polityki kopii zapasowych nośników danych
* Serwerownia backupów znajduje się w innej lokalizacji niż serwery organizacji;
* Zostały zawarte umowy z podmiotem świadczącym usługę utrzymania systemów informatycznych z określonym SLA;
* Zostały zawarte umowy powierzenia przetwarzania danych z dostawcą;
1. Kontrola transferu danych
* Zakaz nieuprawnionego odczytywania, kopiowania, zmiany lub usuwania danych podczas transferu danych, np. szyfrowanie, wirtualne sieci prywatne (VPN), podpis elektroniczny;
* Rodzaj szyfrowania używany do wymiany danych między administratorem a podmiotem przetwarzającym: SFTP;
* Przesyłane dane są zaszyfrowane;
* Dane administratora transportowane są w zamkniętych kontenerach;
* Nośniki danych wysyłane są tylko za obopólną zgodą i jeśli jest to absolutnie konieczne;
* Przy przekazywaniu danych administratora w formie papierowej lub w porównywalnej formie osobom trzecim lub administratorowi zapewnia się, że dane nie będą dostępne w trakcie procesu przenoszenia;
* Zostały opracowane procedury określające szczegóły procesu powiadamiania administratora po otrzymaniu nośnika danych lub w przypadku podejrzenia utraty nośnika danych;
* Opracowane zostały szczegóły dotyczące dysponowania nośnikiem danych otrzymanym od administratora, w tym dokumentacji: niszczenie na miejscu natychmiast po użyciu (niszczarka);
* Dane administratora zapisywane są dodatkowo w postaci zaszyfrowanej.
1. Usuwanie danych po rozwiązaniu umowy
* Dane administratora usuwane są w ciągu 7 dni po ustaniu umowy (elektroniczne nośniki danych/dokumenty papierowe);
* Z usunięcia danych sporządzany jest protokół usunięcia danych, przekazywany do administratora.
1. Kontrola wprowadzania danych
* Pliki dziennika logów tworzone są dla każdego pracownika, aby zapewnić przejrzystość zmian/usunięć danych;
* Istnieje restrykcyjna koncepcja dostępu do wyżej wymienionych plików dziennika logów.
1. Zagadnienia organizacyjne
* Wyznaczono osobę za utrzymanie systemu, jego systematyczną weryfikację;
* Określono sposób wdrażania nowych wersji oprogramowania i jego testowania;
* Stosowane są testy bezpieczeństwa, testy penetracyjne systemów służących do przetwarzania danych osobowych;
* Nośniki danych, na których przetwarzane są dane osobowe są szyfrowane i odpowiednio zabezpieczone;
* Niszczenie nośników danych zawierających dane osobowe odbywa się w sposób uniemożliwiający ich odczytanie;
* Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
* Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika;
* Stosuje się uwierzytelnianie wieloskładnikowe (MFA) podczas dostępu do systemu informatycznego służącego do przetwarzania danych osobowych.
* Stosowane są mechanizmy zabezpieczające przed nieautoryzowanym dostępem osób trzecich do przetwarzania danych osobowych;
* Stosowana jest polityka czystego biurka, polityka czystego ekranu oraz polityka kluczy;
* Została opracowana i wdrożona polityka bezpieczeństwa;
* Została opracowana i wdrożona instrukcja zarządzania systemami informatycznymi;
* Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie ochrony danych osobowych, w tym zabezpieczeń systemu informatycznego.
1. Inne

W przypadku przekazywania danych podmiotom przetwarzającym lub podprzetwarzającym należy również opisać konkretne środki techniczne i organizacyjne, jakie powinien zastosować podmiot przetwarzający lub podprzetwarzający, aby móc udzielić pomocy administratorowi.

* 1. Opis konkretnych środków technicznych i organizacyjnych, jakie powinien zastosować podmiot przetwarzający, aby móc udzielić pomocy administratorowi.
1. Podmiot przetwarzający pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązków wynikających z RODO, w tym:
* z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO;
* z obowiązków określonych w art. 32–36 RODO.
1. W razie potrzeby Administrator przekaże Podmiotowi przetwarzającemu zakres czynności, których wykonania oczekuje.
2. Podmiot przetwarzający pomaga ustosunkować się do prośby Administratora niezwłocznie po otrzymaniu żądania.
3. Administrator może zwrócić się o przekazanie mu następujących informacji:
* opisu systemów informatycznych używanych do przetwarzania danych osobowych;
* listy osób upoważnionych do przetwarzania danych osobowych;
* zaktualizowanego opisu stosowanych środków technicznych i organizacyjnych.
1. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków w RODO.
2. W przypadku, gdyby to Podmiot przetwarzający otrzymał od osoby, której dane dotyczą (a której dane przetwarza administrator) żądanie w zakresie wykonywania przez nią praw przysługujących jej na mocy rozdziału III RODO, niezwłocznie przekaże treść tego żądania Administratorowi. Strony ustalą wówczas sposób i treść odpowiedzi, która zostanie udzielona osobie, której dane dotyczą.

ZAŁĄCZNIK IV

**Wykaz podmiotów podprzetwarzających**

***(wykaz podmiotów podprzetwarzających zostanie uzupełniony zgodnie z częścią B. ankiety
wg Załącznika V do niniejszego projektu umowy)***

*UWAGA WYJAŚNIAJĄCA: Niniejszy załącznik należy wypełnić w razie udzielenia szczegółowej zgody na korzystanie z usług podmiotów podprzetwarzających (klauzula 7.7 lit. a), opcja 1).*

Administrator zezwolił na korzystanie z usług następujących podmiotów podprzetwarzających:

1. Imię i nazwisko lub nazwa: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Adres: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: . . . . . . . . . .

Opis przetwarzania (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających):

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

2) Imię i nazwisko lub nazwa: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Adres: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Imię i nazwisko, stanowisko i dane kontaktowe osoby wyznaczonej do kontaktów: . . . . . . . . . .

Opis przetwarzania (w tym jasne określenie zakresu odpowiedzialności w przypadku upoważnienia kilku podmiotów podprzetwarzających):

 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

ZAŁĄCZNIK V – wzór ankiety

1. Wykaz środków organizacyjnych i technicznych stosowanych przez Podmiot przetwarzający

|  |  |
| --- | --- |
| PYTANIE | ODPOWIEDŹ |
| Czy podmiot przetwarzający posiada opracowaną i zatwierdzoną politykę ochrony danych osobowych? |  |
| Czy podmiot przetwarzający jest w stanie wykazać przestrzeganie ochrony danych osobowych, m.in. przez przedstawienie obowiązujących w jego organizacji procedur i dokumentacji ochrony danych osobowych? |  |
| Czy podmiot przetwarzający zapewnia, że nowo zatrudniony pracownik przed podjęciem czynności związanych z przetwarzaniem danych osobowych zostanie odpowiednio przeszkolony w tym zakresie i zapoznany z obowiązującymi przepisami prawa? |  |
| Czy podmiot przetwarzający dba o bieżące doskonalenie wiedzy swoich pracowników dzięki cyklicznym szkoleniom oraz innym działaniom mającym na celu uświadamianie pracowników w zakresie zagadnień dotyczących ochrony danych osobowych? |  |
| Czy pracownicy podmiotu przetwarzającego, którzy uczestniczą w operacjach przetwarzania danych osobowych, zostali zobowiązani do zachowania ich w tajemnicy? |  |
| Czy podmiot przetwarzający stosuje zatwierdzony kodeks postępowania, o którym mowa w art. 40 Rozporządzenia, lub zatwierdzony mechanizm certyfikacji, o którym mowa w art. 42 Rozporządzenia? |  |
| Czy w ciągu dwóch ostatnich lat podmiot przetwarzający poddawał zewnętrznej kontroli niezależnych audytorów funkcjonujący w jego organizacji system ochrony danych osobowych? |  |
| Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych / podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? |  |
| Czy podmiot przetwarzający zastosował środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu? |  |
| Czy podmiot przetwarzający zapewnił fizyczne oddzielenie środków przetwarzania informacji zarządzanych przez jego organizację od tych, które należą do innych organizacji? |  |
| Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy nie jest możliwy dla osób trzecich (firma sprzątająca, ochrona) bądź dostęp ten jest szczegółowo nadzorowany? |  |
| Czy każdy pracownik podmiotu przetwarzającego otrzymuje imienny identyfikator do systemów informatycznych? |  |
| Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowych zmian haseł oraz zmian w razie zaistniałej potrzeby? |  |
| Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do zabezpieczania nieużywanych w danym momencie systemów przez blokadę ekranu lub w inny równoważny sposób? |  |
| Czy pracownicy podmiotu przetwarzającego zostali zobowiązani do niezwłocznego odbierania z drukarek wydruków zawierających dane osobowe lub inne poufne informacje? Czy wskazana zasada jest przestrzegana przez pracowników? |  |
| Czy w organizacji podmiotu przetwarzającego jest stosowana polityka czystego biurka? |  |
| Czy dane osobowe gromadzone w formie papierowej są przechowywane, po godzinach pracy organizacji podmiotu przetwarzającego, w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych? |  |
| Czy podmiot przetwarzający zapewnił oprogramowanie antywirusowe na wszystkich stacjach? |  |
| Czy podmiot przetwarzający stosuje szyfrowanie dysków komputerów przenośnych? |  |
| Czy urządzenia mobilne mają skonfigurowaną kontrolę dostępu? |  |
| Czy podmiot przetwarzający stosuje techniki kryptograficzne wobec urządzeń mobilnych? |  |
| Czy na urządzeniach mobilnych zainstalowano oprogramowanie antywirusowe? |  |
| Czy zapewniono zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego? |  |
| Jaki przyjęto zakres oraz jaką częstotliwość tworzenia kopii zapasowych? |  |
| Gdzie są przechowywane kopie zapasowe? |  |
| Czy podmiot przetwarzający posiada procedury odtwarzania systemu po awarii oraz ich testowania? |  |
| Czy podmiot przetwarzający wdraża nowe rozwiązania zgodnie z zasadą privacy by design? |  |
| Czy podmiot przetwarzający działa zgodnie z zasadą privacy by default? |  |
| Czy podmiot przetwarzający prowadzi ocenę skutków dla ochrony danych? |  |
| Czy podmiot przetwarzający gwarantuje realizację praw osób, których dane dotyczą, tj. m.in. prawo do przenoszenia danych, prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym? |  |

1. Wykaz podwykonawców Podmiotu przetwarzającego (podprocesorów)

Przy wykonaniu Umowy Procesor korzysta z usług następujących podprocesorów:

|  |  |
| --- | --- |
| Podprocesor | Adres siedziby |
|  |  |
|  |  |
|  |  |