Załącznik nr 4  
**Umowa powierzenia przetwarzania danych**

**Umowa powierzenia przetwarzania danych osobowych**

zawarta w dniu ……………………. r. pomiędzy:

………

którego reprezentują:

………

zwaną dalej **Administratorem**

a

………

którego reprezentują:

………

zwaną dalej **Przetwarzającym**

Obie Strony w dalszej części umowy zwane łącznie Stronami oraz każda z osobna Stroną.

1. Przedmiot Umowy
2. Administrator powierza Przetwarzającemu dane osobowe do przetwarzania w trybie art. 28 ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (zwanego dalej RODO), na zasadach, w zakresie i w celu określonych w niniejszej Umowie.
3. Przedmiotem umowy jest realizacja zadań Umowy ……… Nr ……………… z dnia ……………… r. (zwaną dalej Umową Główną) wiążących się z przetwarzaniem danych osobowych.
4. Przetwarzający zobowiązuje się do przetwarzania powierzonych mu danych osobowych:
   1. zgodnie z niniejszą Umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, chroniącymi prawa osób, których dane dotyczą.
   2. wyłącznie na udokumentowane polecenie administratora, które stanowi niniejsza Umowa.
5. Zakres i cel przetwarzania danych
6. Rodzaj danych, kategorie osób, których dane dotyczą oraz czynności przetwarzania zostały określone w załączniku nr 1 do niniejszej Umowy.
7. Dane osobowe powierzone przez Administratora będą przetwarzane przez Przetwarzającego wyłącznie w celu realizacji Umowy Głównej.
8. Przetwarzanie będzie miało charakter ciągły.
9. Sposób przetwarzania danych niezautomatyzowany.
10. Obowiązki Podmiotu przetwarzającego
11. Przetwarzający przy przetwarzaniu powierzonych danych osobowych zobowiązuje się do ich zabezpieczenia przez stosowanie odpowiednich środków technicznych   
    i organizacyjnych, odpowiadających stanowi wiedzy technicznej, zapewniających zgodność z RODO, w tym adekwatny stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą.
12. Przetwarzający:
    1. zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
    2. zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane osobowe, przy czym będą to jedynie osoby, które mają odpowiednie przeszkolenie z zakresu ochrony danych osobowych i są niezbędne do realizacji celu niniejszej Umowy.
    3. zobowiązuje się do podejmowania wszelkich niezbędnych środków określonych   
       w art. 32 RODO.
    4. zapewnia, że osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zobowiążą się do zachowania tajemnicy lub będą podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,   
       o której mowa w art. 28 ust. 3 lit. b) RODO, zarówno w trakcie zatrudnienia ich przez Przetwarzającego, jak i po jego ustaniu. Zapewnia ponadto, że osoby,   
       o których mowa w niniejszym punkcie, będą przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej.
    5. dokonuje okresowej weryfikacji listy osób, którym udzielono dostępu do danych przetwarzanych w imieniu Administratora dla prawidłowej realizacji pkt. e.
    6. biorąc pod uwagę charakter przetwarzania, w miarę możliwości będzie pomagał Administratorowi wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO.
    7. po zakończeniu świadczenia usług związanych z przetwarzaniem niezwłocznie zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych. Poprzez trwałe usunięcie danych należy rozumieć takie zniszczenie tych danych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. Usunięcie danych zostanie potwierdzone przez Przetwarzającego protokołem usunięcia danych, przekazanym na adres Administratora w ciągu  5 dni roboczych  od daty usunięcia danych, lecz nie później niż  14 dni  od zakończenia świadczenia usług w ramach Umowy Głównej.
    8. pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, oraz z obowiązków określonych w art. 32–36 RODO. Przetwarzający – w razie wpływu do niego żądania w zakresie realizacji praw osób, których dotyczą powierzone dane – informuje o tym Administratora w terminie  3 dni roboczych  od otrzymania wiadomości. Udzielając informacji, Przetwarzający przekazuje dane nadawcy   
       i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania. W szczególności zaś:
       * bezzwłoczne zgłasza wszelkie naruszenia ochrony danych osobowych oraz sukcesywne uzupełnianie przekazanych informacji;
       * pomaga Administratorowi w poinformowaniu osób, których dane dotyczą o naruszeniu ich danych;
       * w celu realizacji obowiązków, o których mowa powyżej, Przetwarzający w miarę możliwości dokumentuje wszelkie okoliczności i zbiera wszelkie dowody, które pomogą Administratorowi wyjaśnić szczegóły naruszenia, w tym jego charakter, skalę, skutki, czas zdarzenia, osoby odpowiedzialne, osoby poszkodowane.
13. W przypadku stwierdzenia jakiegokolwiek naruszenia ochrony danych osobowych Przetwarzający lub podwykonawca Przetwarzającego zgłasza je Administratorowi w ciągu  24 godzin .
14. Szczegółowe warunki przetwarzania danych Przetwarzający przedstawi w **Ankiecie kontrolnej** stanowiącej załącznik nr 3 do niniejszej umowy.
15. Prawo kontroli
16. Zgodnie z art. 28 ust. 3 lit. h) RODO Administrator ma prawo kontroli, mającej na celu weryfikację, czy Przetwarzający spełnia obowiązki wynikające z niniejszej Umowy.
17. Administrator będzie realizować prawo kontroli w godzinach pracy Przetwarzającego i z minimum  5 dniowym  uprzedzeniem.
18. Prawo do przeprowadzenia kontroli obejmuje: wstęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych; żądanie złożenia pisemnych lub ustnych wyjaśnień od osób upoważnionych do przetwarzania powierzonych danych osobowych; wgląd do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z celem kontroli; przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.
19. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych, nie dłuższym niż  5 dni .
20. Powyżej określone zasady kontroli Przetwarzającego mają zastosowanie również do przeprowadzanych przez Administratora kontroli podwykonawców Przetwarzającego, o których mowa w § 6 ust. 1 Umowy.
21. Raportowanie
22. Na wniosek Administratora Przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z RODO.
23. Informacji, o których mowa w ust. 1, udziela się w terminie  10 dni roboczych  od dnia doręczenia wniosku, z zastrzeżeniem ust. 3.
24. Jeżeli wniosek, o którym mowa w ust. 1, dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Przetwarzający udziela informacji w najbliższym możliwym terminie, nie później niż w ciągu  24 godzin  od doręczenia wniosku.
25. Dalsze powierzenie danych
26. Administrator wyraża zgodę na powierzenie danych osobowych objętych niniejszą Umową do dalszego przetwarzania przez podwykonawców Przetwarzającego, w celu wykonania niniejszej Umowy, przy czym podwykonawcy Przetwarzającego powinni spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Przetwarzającego niniejszą Umową. Lista takich podwykonawców (podprocesorów) Przetwarzający przedstawi w Załączniku nr 2 do niniejszej Umowy.
27. W przypadku zmiany lub dodania innych podwykonawców biorących udział w przetwarzaniu danych powierzonych przez Administratora Przetwarzający informuje o zamierzonych zmianach, dając Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian w terminie  5 dni roboczych  od przekazania informacji o zamierzonych zmianach.
28. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na udokumentowane polecenie Administratora, chyba że taki obowiązek nakłada na Przetwarzającego prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
29. Przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się z obowiązków spoczywających na podwykonawcy, wynikających z niniejszej Umowy.
30. Odpowiedzialność Przetwarzającego
31. Przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie osobom nieupoważnionym powierzonych do przetwarzania danych osobowych.
32. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Przetwarzającego danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub jakimkolwiek orzeczeniu dotyczących przetwarzania tych danych, skierowanych do Przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania u Przetwarzającego tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.
33. Czas obowiązywania Umowy
34. Niniejsza Umowa obowiązuje przez czas określony Umową Główną.
35. Każda ze stron może wypowiedzieć niniejszą Umowę   
    z zachowaniem  jednomiesięcznego  okresu wypowiedzenia.
36. Rozwiązanie Umowy

Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Przetwarzający:

* 1. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie,
  2. przetwarza dane osobowe w sposób niezgodny z Umową,
  3. powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

1. Zasady zachowania poufności
2. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób, a także danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy, w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
3. Przetwarzający oświadcza, że w związku z zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.
4. Postanowienia końcowe
5. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
6. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz RODO.
7. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy Administratora.
8. Integralną częścią niniejszej umowy jest Ankieta kontrolna podmiotu przetwarzającego.

|  |  |
| --- | --- |
| **Administrator** | **Przetwarzający** |

**Załącznik nr 1**

**Rodzaj danych, kategorie osób, których dane dotyczą oraz czynności przetwarzania**

1. Rodzaj danych osobowych będących przedmiotem przetwarzania, w ramach Umowy:
2. imię i nazwisko,
3. miejsce pracy,
4. PESEL,
5. numer telefonu, adres email.
6. Kategorie osób, których dane osobowe będą przetwarzane, w ramach Umowy:
7. Uczestnicy projektu,
8. Czynności przetwarzania, które będą wykonywane na danych osobowych, w ramach Umowy:
9. zbieranie,
10. utrwalanie,
11. organizowanie,
12. porządkowanie,
13. przechowywanie,
14. adaptowanie lub modyfikowanie,
15. pobieranie,
16. przeglądanie,
17. wykorzystywanie,
18. ujawnianie poprzez przesłanie,
19. rozpowszechnianie lub innego rodzaju udostępnianie,
20. dopasowywanie lub łączenie,
21. ograniczanie,
22. usuwanie lub niszczenie.

**Załącznik nr 2**

**Lista dalszych przetwarzających**

|  |  |  |
| --- | --- | --- |
| **Nazwa podmiotu i adres** | **Zakres czynności** | **Zakres powierzonych danych** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Załącznik nr 3**

**Ankieta kontrolna podmiotu przetwarzającego**

Niniejsza ankieta kontrolna ma na celu wykazanie przestrzegania przepisów RODO. Poniższe pytania nie dotyczą zabezpieczeń stosowanych wobec wszystkich danych, będących w posiadaniu podmiotu, ale jedynie wobec danych powierzonych.

Nazwa i siedziba podmiotu przetwarzającego: **…………………………………………**

UWAGA: Odpowiedź „Nie” lub „nie dotyczy” wymaga krótkiego wyjaśnienia.

|  |  |
| --- | --- |
| Środki organizacyjne | |
|  | Czy wyznaczono Inspektora Ochrony Danych lub pracownika do pełnienia zadań związanych z ochroną danych osobowych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy opracowano i wdrożono dokumentację ochrony danych opisującą zasady przetwarzania i zabezpieczania danych osobowych (np. polityka ochrony danych)?  *- należy przesłać skan dokumentu wdrażającego – Zarządzenie, oficjalna informacja itp.*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy prowadzony jest rejestr kategorii czynności przetwarzania zwierający wszystkie informacje wskazane w art. 30 ust. 2 RODO?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy osoby biorące udział w przetwarzaniu powierzonych danych osobowych zostały upoważnione do przetwarzania danych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy pracownicy dopuszczeni do pracy z danymi powierzonymi zostali zobowiązani do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy pracownicy dopuszczeni do pracy z danymi powierzonymi zostali przeszkoleni z zakresu ochrony danych powierzonych i uświadomieni w zakresie ochrony danych osobowych dotyczących danych powierzonych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy stworzono procedurę przechowywania/archiwizowania dokumentacji, która zawiera powierzone dane osobowe?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy organizacja posiada procedury szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy zostały wdrożone procedury, umożliwiające skuteczne zgłoszenie naruszenia bezpieczeństwa powierzonych danych osobowych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
| Realizacja praw osób fizycznych | |
|  | Czy w ostatnich 24 miesiącach do podmiotu przetwarzającego trafiły jakieś żądania osób fizycznych z art. 12-22 RODO? *- jeżeli tak, to czy Administrator został o tym poinformowany i w jaki sposób?*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
| Podpowierzenie | |
|  | Czy w procesie przetwarzania powierzonych danych wykorzystywane są usługi innych podwykonawców (tzw. podpowierzenie przetwarzania danych)?  *- jeżeli tak, należy uzupełnić załącznik nr 2 do niniejszej Umowy i odpowiedzieć na pytania 11-13.*  *- jeżeli nie, w pkt od 11 do 13 należy zaznaczyć: NIE DOTYCZY.*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy z podmiotami, o których mowa w pkt 10 zostały podpisane umowy/porozumienia/inny instrument prawny regulujący podpowierzenie zgodne z art. 28 ust. 3 RODO?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy podmioty zewnętrzne, o których mowa w załączniku nr 2 do niniejszej umowy zostały sprawdzone pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych, o których mowa w art. 32 RODO w związku z art. 28 ust. 4 RODO?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy przed podpisaniem umowy z podmiotami, o których mowa w pkt 10, uzyskano zgodę Administratora?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
| Zabezpieczenia fizyczne | |
|  | Czy zastosowano środki kontroli dostępu fizycznego do budynku/budynków tylko dla autoryzowanego personelu w miejscu przechowywania powierzonych danych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy dostęp do pomieszczeń pozostających w dyspozycji podmiotu przetwarzającego po godzinach pracy jest możliwy dla osób trzecich (m.in. firma sprzątająca, ochrona)?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy powierzone dane osobowe gromadzone w formie papierowej, po godzinach pracy organizacji, przechowywane są w zamykanych szafach/szafkach/szufladach bez możliwości dostępu do nich osób nieupoważnionych (tzw. zasada „czystego biurka”)?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy pracownicy zostali zobowiązani do niszczenia dokumentów zawierających dane osobowe przy użyciu niszczarek, które nie pozwalają na odtworzenie dokumentu w łatwy sposób?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Proszę zaznaczyć **zastosowane** elementy zabezpieczenia fizycznego:  pomieszczenia zamykane na klucz;  klucze do pomieszczeń zdawane na portierni, recepcji itp.;  dokumentacja zawierająca dane osobowe przechowywana w zamykanych meblach;  dostęp do dokumentów tylko dla osób upoważnionych;  kontrola dostępu do budynku (ochrona, portiernia, system kontroli dostępu itp.);  kontrola dostępu do pomieszczeń (czytnik kart magnetycznych, kod do drzwi itp.);  monitoring wizyjny budynku;  monitoring wizyjny piętra, na którym przechowywane są powierzone dane;  system sygnalizacji włamania i napadu;  system sygnalizacji pożaru; |
| Zabezpieczenia teleinformatyczne | |
|  | Czy każdy użytkownik dostaje imienny identyfikator do systemów informatycznych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy uprawnienia do przetwarzania danych osobowych są odbierane, gdy kończy się stosunek pracy (lub inna forma współpracy)?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy systemy informatyczne zapewniają wymuszanie na użytkownikach okresowe zmiany haseł oraz zmiany w razie zaistniałej potrzeby?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy wprowadzono ochronę systemów poprzez blokadę komputera, gdy nie jest on używany?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy zapewniono oprogramowanie antywirusowe na stacjach używanych do przetwarzania powierzonych danych oraz na urządzeniach mobilnych (np. telefonach)?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy wykorzystywane oprogramowanie posiada licencję i jest na bieżąco aktualizowane?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy stosuje się szyfrowanie urządzeń przenośnych (np. dysków komputerów przenośnych, zewnętrznych pamięci), na których przetwarzane są dane powierzone?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy pracownicy zostali zobowiązani do szyfrowania powierzonych danych osobowych przesyłanych drogą elektroniczną (np. raportowanie)?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy urządzenia mobilne (np. telefony), na których przetwarzane są dane powierzone posiadają skonfigurowaną kontrolę dostępu?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy wykonywane są kopie zapasowe powierzonych danych osobowych zapewniające szybkie przywrócenie dostępu do nich w razie incydentu fizycznego lub technicznego?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy kopie zapasowe są przechowywane w sposób zapewniający bezpieczeństwo powierzonych danych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
| Analiza ryzyka | |
|  | Czy dokonywana jest okresowa ocena ryzyka dotycząca bezpieczeństwa przetwarzania powierzonych danych osobowych, w szczególności w zakresie zagrożeń:   1. przypadkowego lub niezgodnego z prawem zniszczenia, 2. utraty, modyfikacji, nieuprawnionego ujawnienia, 3. lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.   TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy organizacja wprowadziła, na podstawie oszacowanego ryzyka bezpieczeństwa powierzonych danych, inne środki techniczne i organizacyjne, które nie zostały wymienione powyżej?  *- jeżeli tak, należy wymienić jakie.*  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
| Naruszenia ochrony danych | |
|  | Czy podmiot przetwarzający wdrożył procedury dotyczące zarzadzania incydentami bezpieczeństwa?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |
|  | Czy w ostatnim roku wystąpiły incydenty/naruszenia ochrony danych osobowych?  TAK  NIE  NIE DOTYCZY  WYJAŚNIENIA: |