

Załącznik nr 4 do umowy

Umowa
dot. powierzenia przetwarzania danych osobowych (dalej: UPD)

zawarte dnia w Warszawie pomiędzy:

Ośrodek Przetwarzania Informacji – Państwowy Instytut Badawczy z siedzibą w Warszawie, al. Niepodległości 188b, wpisany do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XVI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000127372, posiadający nr NIP 525 – 000 – 91 – 40 oraz nr REGON 006746090, reprezentowany przez: dr Jarosława Protasiewicza - Dyrektora Instytutu zwaną w dalszej części Umowy „Administratorem”
oraz

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

reprezentowanym przez:

zwaną w dalszej części Umowy „Podmiotem przetwarzającym”

§ 1

Powierzenie przetwarzania danych osobowych

1. W związku z zawarciem i realizacją umowy nr z dnia dotyczącej świadczenia usługi przechowywania i udostępniania plików w chmurze (Object Storage), dostarczonej jako rozwiązanie chmurowe w modelu SaaS (dalej: **Umowa**), Administrator powierza Podmiotowi przetwarzającemu dane osobowe przetwarzane w ramach tej usługi.
2. Przedmiotem przetwarzania są dane osobowe wskazane w ust. 1 znajdujące się w ramach przechowywanych plików, które obejmują dane kontaktowe oraz dane identyfikacyjne, a także dane związane z kursami e-learningowymi. Zakres danych osobowych wymienionych w ust. 1 może być w każdym czasie zmieniony, rozszerzony lub ograniczony przez Administratora, w zależności od tego co aktualnie przechowuje Administrator w ramach usługi.
3. Z tytułu wykonywania świadczeń określonych w UPD Podmiotowi przetwarzającemu nie przysługuje dodatkowe wynagrodzenie ponad to, które zostało określone w Umowie.
4. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone dane osobowe zgodnie z poleceniem Administratora, przestrzegając postanowień UPD, Umowy oraz obowiązujących przepisów regulujących kwestię ochrony danych osobowych; w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: **Rozporządzenie**).
5. Administrator oświadcza, że jest uprawniony do przetwarzania w zakresie, w jakim powierzył je Podmiotowi przetwarzającemu.
6. Podmiot przetwarzający oświadcza, że w ramach prowadzonej działalności profesjonalnie zajmuje się przetwarzaniem danych osobowych objętych Umową, posiada w tym zakresie niezbędną

- wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania postanowień UPD.
7. Poprzez zawarcie UPD Administrator poleca przetwarzanie danych osobowych Podmiotowi 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 zw. z art. 29 RODO.
 8. Przetwarzanie danych osobowych wskazanych w ust. 1 odbywa się w miejscu określonym w **załączniku nr 1**, na co Administrator udziela wyraźnej zgody.
 9. Jeżeli przetwarzanie danych osobowych będzie odbywać się poza Unią Europejską („UE”), takie przetwarzanie nastąpi wyłącznie w przypadku, gdy Administrator wyrazi uprzednią pisemną zgodę i pod warunkiem, że przetwarzanie będzie się odbywać w oparciu o odpowiednie środki bezpieczeństwa, które zapewnią odpowiedni poziom ochrony danych osobowych, które Podmiot przetwarzający zobowiązany jest przedstawić, w szczególności Podmiot przetwarzający zobowiązany jest wykazać TIA (Transfer Impact Assesment) oraz odpowiednie regulacje na podstawie których dokonuje dalszego powierzenia przetwarzania danych .

§ 2

Charakter i cel przetwarzania danych

1. Administrator upoważnia Podmiot przetwarzający do przetwarzania w jego imieniu danych osobowych w celu i zakresie niezbędnym i koniecznym do realizacji Umowy, obejmującym takie operacje jak przechowywanie danych, kopiowanie danych w ramach kopii bezpieczeństwa i dostęp do danych wyłącznie na potrzeby utrzymania środowiska informatycznego w którym dane te będą przechowywane, a następnie usunięcia tych danych.
2. Charakter przetwarzania danych osobowych wynika z Umowy i określony jest rolą Podmiotu przetwarzającego jako podmiotu realizującego w imieniu i na rzecz Administratora stałą usługę hostingu przechowywanych plików przez okres obowiązywania Umowy, dostarczonej jako rozwiązanie chmurowe w modelu SaaS, w ramach której Administrator przechowuje swoje dane osobowe, a Podmiot przetwarzający zapewnia dla nich bezpieczne środowisko informatyczne, przechowywanie, utrzymanie dostarczonego rozwiązania i jego ciągłość działania. Przetwarzanie jest realizowane przez pracowników lub osoby stale współpracujące z Podmiotem przetwarzającym i prowadzone w sposób automatyczny, tj. z wykorzystaniem technologii informatycznych.
3. Przetwarzanie danych osobowych będzie dotyczyć następujących kategorii osób: pracownicy administratora których dane osobowe przetwarzane są w ramach panelu administracyjnego do zarządzania usługami w ramach dostarczonego rozwiązania informatycznego, uczestnicy kursów, administratorzy kursów.

§ 3

Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się:
 - 1) przy przetwarzaniu powierzonych danych osobowych na podstawie Umowy, zabezpieczyć je poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, zapewniający adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia, wykaz stosowanych środków technicznych i organizacyjnych na dzień zawarcia UPD stanowi **załącznik nr 2**. Podmiot przetwarzający przedstawi Administratorowi informacje i dokumenty potwierdzające, że zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i

organizacyjnych wskazanych w załączniku, przed przekazaniem danych osobowych. Podmiot przetwarzający zobowiązany jest do niezwłocznego przedstawiania Administratorowi wszelkich aktualizacji informacji i dokumentów, o których mowa w zdaniu poprzednim.

- 2) nadać upoważnienia do przetwarzania danych osobowych wskazanych w § 1 ust. 1 UPD wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy i UPD,
 - 3) prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych,
 - 4) zapewnić zachowanie w tajemnicy przetwarzanych danych oraz sposobów ich zabezpieczenia przez osoby, które posiadają upoważnienia do przetwarzania danych osobowych w celu realizacji Umowy lub UPD, zarówno w trakcie zatrudnienia lub współpracy z Podmiotem przetwarzającym jak i po ustaniu zatrudnienia lub współpracy,
 - 5) udostępniać Administratorowi na jego żądanie wszelkie informacje niezbędne do wykazania spełnienia obowiązków wskazanych w przepisach RODO, innych powszechnie obowiązujących przepisach oraz w UPD,
 - 6) stosować środki w celu zaradzenia naruszeniom ochrony danych osobowych oraz w stosownych przypadkach środki w celu zminimalizowania ich ewentualnych negatywnych skutków,
 - 7) stosować się do pisemnych instrukcji wydanych przez Administratora w zakresie przetwarzania powierzonych danych osobowych, chyba że co innego wynika z wiążących Podmiot przetwarzający obowiązujących przepisów prawa. W tym drugim przypadku Podmiot przetwarzający informuje Administratora o przepisach prawnych i wynikających z nich obowiązkach,
 - 8) dokumentować wszelkie naruszenia ochrony danych w tym ich okoliczności, skutki oraz podjęte działania zaradcze w sposób określony w § 7.
2. Podmiot przetwarzający pomaga Administratorowi:
- 1) w miarę swoich możliwości, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia (Prawa osoby, której dane dotyczą),
 - 2) w wywiązywaniu się z obowiązków określonych w art. 32-36 Rozporządzenia, w szczególności w przypadku stwierdzenia naruszenia zasad ochrony i przetwarzania powierzonych danych osobowych na podstawie Umowy, zgłasza je Administratorowi za pośrednictwem osób wskazanych w § 10 ust. 5 UPD niezwłocznie, jednak nie później niż w terminie 24 godzin od chwili stwierdzenia naruszenia, z uwzględnieniem postanowień ust. 1 pkt 8 i § 7).
3. Podmiot przetwarzający nie jest uprawniony do przekazywania informacji o naruszeniu ochrony powierzonych danych jakimkolwiek podmiotom bez uprzedniej konsultacji z Administratorem.
 4. Podmiot przetwarzający jest zobowiązany do niezwłocznego poinformowania o wszelkich zgłoszeniach praw osób których dane dotyczą, jeżeli zgłoszenia te dotyczą powierzonych danych.
 5. Podmiot przetwarzający po zakończeniu Umowy, nie później niż w ciągu 30 dni od jej zakończenia, jest zobowiązany na żądanie Administratora do usunięcia lub zwrotu Administratorowi powierzonych danych osobowych, o ile przepis prawa powszechnie obowiązującego nie stanowi inaczej.
-

6. Podmiot przetwarzający nie ma prawa do wykorzystywania powierzonych danych w jakimkolwiek celu po wygaśnięciu, rozwiązaniu lub odstąpieniu od Umowy, z wyjątkiem usunięcia lub zwrotu Administratorowi; dane te stanowią tajemnicę przedsiębiorstwa Administratora.
7. Podmiot przetwarzający będzie przetwarzał dane osobowe wyłącznie w celach dla których otrzymał instrukcje oraz w celu wypełnienia zobowiązań wynikających z UPD. Podmiot przetwarzający nie będzie wykorzystywał danych osobowych do innych celów.
8. Podmiot przetwarzający nie będzie przekazywał danych osobowych stronom trzecim, chyba że przekazanie to odbywa się zgodnie z instrukcjami Administratora w związku z realizacją Umowy lub gdy jest to konieczne w celu wywiązania się z obowiązku prawnego.
9. Podmiot przetwarzający nie będzie modyfikował danych osobowych bez instrukcji Administratora.
10. Podmiot przetwarzający powinien prowadzić rejestr kategorii czynności przetwarzania dokonywanych w imieniu Administratora, zgodnie z wymogami wynikającymi z RODO.

§ 4

Prawo do kontroli

1. Administrator ma prawo kontroli (audytu), czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu danych spełniają postanowienia UPD i RODO. W tym celu Podmiot przetwarzający umożliwi Administratorowi lub upoważnionemu przez Administratora audytorowi przeprowadzenie audytów, w tym inspekcji i przyczynia się do nich.
2. Administrator poinformuje Podmiot przetwarzający o zamiarze przeprowadzenia audytu. Podmiot przetwarzający wyznaczy terminy możliwych audytów w ciągu 14 dni roboczych od otrzymania powiadomienia. Prawo audytu dotyczy wyłącznie danych powierzonych przez Administratora oraz miejsca ich przetwarzania. Audyt może odbyć się w wyznaczonym przez Podmiot przetwarzający czasie i pod kontrolą wyznaczonej przez niego osoby. Jeżeli w ciągu 14 dni Podmiot przetwarzający nie wyznaczy terminów Administrator jest uprawniony do wskazania terminów audytów.
3. Niezależnie od postanowień ust. 2 Podmiot przetwarzający na każdy pisemny wniosek Administratora zobowiązany jest do udzielenia informacji dotyczących przetwarzania powierzonych mu danych osobowych w terminie 14 dni od dnia otrzymania takiego wniosku.
4. Podmiot przetwarzający udostępni Administratorowi informacje niezbędne do wykazania spełnienia obowiązku określonego w art. 28 Rozporządzenia.
5. Po stwierdzeniu przez Administratora naruszeń Umowy Podmiot przetwarzający jest zobowiązany do ich usunięcia w terminie i w sposób ustalony pomiędzy Stronami.

§5

Podpowierzenie

1. Podmiot przetwarzający jest uprawniony do dalszego powierzania wskazanych w § 1 ust. 1 UPD danych osobowych w celu niezbędnym do wykonania Umowy, podmiotom będącym podwykonawcami Podmiotu przetwarzającego, po uprzednim każdorazowym uzyskaniu zgody Administratora i przekazaniu informacji o tych podmiotach i miejscu przetwarzania przez nich danych. Podmiot przetwarzający zobowiązany jest przekazać Administratorowi informacje w zakresie wskazanym w **załączniku nr 1** dotyczących podwykonawcy lub dalszych podwykonawców.
2. Podmiot przetwarzający poinformuje Administratora na piśmie o wszelkich zmianach polegających na zastąpieniu lub dodaniu podwykonawców celem wyrażenia zgody.

3. Podmiot przetwarzający jest zobowiązany do zapewnienia, że podmioty wskazane w ust. 1 spełniają takie same wymagania i obowiązki ochrony danych osobowych, jak Podmiot przetwarzający, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków organizacyjnych i technicznych, aby przetwarzanie odpowiadało wymogom aktualnie obowiązujących przepisów prawa w zakresie ochrony danych osobowych.
4. Zaangażowanie podwykonawcy nie wpływa na obowiązki Podmiotu przetwarzającego względem Administratora. Za działania i zaniechania podwykonawców Podmiot przetwarzający odpowiada jak za działania i zaniechania własne. Dostęp do danych osobowych może zostać udzielony tylko wtedy, gdy podwykonawca przestrzega (lub zapewnia przestrzeganie) obowiązków wynikających z UPD. Podmiot przetwarzający zawrze pisemną umowę z podwykonawcą, która będzie zgodna z prawem, odpowiednimi przepisami oraz UPD.

§ 6

Odpowiedzialność

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy oraz UPD, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot powierzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania danych osobowych przez Podmiot przetwarzający, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania danych, a także o wszelkich kontrolach i inspekcjach dotyczących przetwarzania danych osobowych przez Podmiot przetwarzający, w szczególności prowadzonych przez organ nadzoru ochrony danych.
3. Podmiot przetwarzający będzie chronił, zabezpieczał i zwolni Administratora z odpowiedzialności za wszelkie roszczenia, działania, szkody, straty, koszty i wydatki (w tym między innymi uzasadnione koszty obsługi prawnej, consultingowej i audytowej), wynikające z lub będące następstwem roszczeń jakiegokolwiek strony trzeciej wobec Administratora, wynikających z lub będących następstwem niespełnienia przez Podmiot przetwarzający jakichkolwiek obowiązków dotyczących ochrony powierzonych danych osobowych oraz wszelkich innych obowiązków nałożonych na niego na mocy UPD.
4. W przypadku jakichkolwiek roszczeń strony trzeciej Podmiot przetwarzający ma obowiązek poinformowania Administratora o wystąpieniu takiego roszczenia niezwłocznie nie później niż w ciągu 3 dni od momentu, w którym posiadał informację na temat wystąpienia roszczenia strony trzeciej.

§ 7

Naruszenie bezpieczeństwa danych

1. Podmiot przetwarzający powinien powiadomić Administratora niezwłocznie o naruszeniu danych nie później niż w ciągu 24 godzin od stwierdzenia naruszenia.
2. Powiadomienie, o którym mowa w ust. 1 powinno zawierać co najmniej:
 - a) charakter naruszenia danych, w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą oraz kategorie i przybliżoną liczbę danych osobowych, których to dotyczy,
 - b) nazwisko i dane kontaktowe Inspektora Ochrony Danych lub innej osoby wyznaczonej do kontaktu, od której można uzyskać więcej informacji,
 - c) prawdopodobne konsekwencje naruszenia danych osobowych,

- d) środki zastosowane lub proponowane przez Podmiot przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środki mające na celu złagodzenie jego ewentualnych negatywnych skutków.
3. Podmiot przetwarzający wspiera Administratora w wypełnianiu ciążącego na nim ustawowego obowiązku informacyjnego wobec organów nadzoru i/ lub osób, których dane dotyczą w przypadku naruszenia danych.
4. Podmiot przetwarzający powinien niezwłocznie poinformować Administratora w każdym przypadku, kiedy uzna, że przetwarzanie jest niezgodne z prawem.

§ 8

Czas obowiązywania umowy

1. UPD obowiązuje przez okres obowiązywania Umowy oraz przez okres do 30 dni od jej zakończenia.
2. Administrator jest uprawniony do rozwiązania UPD w trybie natychmiastowym, jeżeli zaistnieje chociażby jedna z poniższych przesłanek:
 - 1) Podmiot przetwarzający nie wypełnia obowiązków wskazanych w RODO lub innych powszechnie obowiązujących przepisach dotyczących ochrony danych osobowych,
 - 2) Podmiot przetwarzający nie wypełnia obowiązków wskazanych w UPD.
3. Zaistnienie podstaw do rozwiązania UPD bez wypowiedzenia stanowi podstawę do rozwiązania Umowy bez wypowiedzenia.

§ 9

Poufność

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że z zastrzeżeniem § 5 UPD, w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonanie Umowy lub UPD, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub UPD.
3. Strony zobowiązują się do dołożenia wszelkich starań w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania danych poufnych gwarantowały zabezpieczenie danych poufnych, w tym w szczególności danych osobowych powierzonych do przetwarzania, przed dostępem osób trzecich nieupoważnionych do zapoznania się z ich treścią.
4. W zakresie nieuregulowanym postanowienia Umowy dotyczące poufności stosuje się odpowiednio.

§ 10

Postanowienia końcowe

1. Zmiana UPD wymaga formy pisemnej pod rygorem nieważności, z zastrzeżeniem zmian osób o których mowa w ust. 4.
2. Załączniki stanowią integralną część UPD.
3. Obowiązki informacyjne wynikające z UPD mogą być realizowane w formie elektronicznej.

-
4. Strony postanawiają, że osobami odpowiedzialnymi za realizację postanowień UPD, w tym uprawnionymi do kontaktu w zakresie realizacji praw osób których dane dotyczą oraz obowiązków wynikających z UPD jest:
 - a) ze strony Administratora – Tomasz Tołpa, e-mail ttolpa@opi.org.pl lub iod@opi.org.pl
 - b) ze strony Podmiotu przetwarzającego – e-mail:
.....
 5. UPD sporządzono w dwóch jednobrzmiących egzemplarzach.
 6. Sądem właściwym dla rozpatrywania sporów jest sąd właściwy dla siedziby Administratora.

Administrator

Podmiot przetwarzający

Załącznik nr 1 – Podmiot przetwarzający, Dalsze podmioty przetwarzające i kolejne dalsze podmioty przetwarzające

Podmiot przetwarzający

Firma i adres	Lokalizacja przetwarzania	Świadczone usługi/cel

Dalsze Podmioty Przetwarzające

Firma i adres	Lokalizacja przetwarzania	Świadczone usługi/cel

Kolejne dalsze podmioty przetwarzające

Firma i adres	Lokalizacja przetwarzania	Świadczone usługi/cel

Załącznik nr 2 – wykaz stosowanych środków technicznych i organizacyjnych

L.p.	Środek techniczny i organizacyjny	Tak	Nie/ Nie dotyczy	Uwagi
1.	Powołano Inspektora Ochrony Danych lub wyznaczono pracownika do pełnienia zadań związanych z ochroną danych osobowych			
2.	Osoby biorące udział w przetwarzaniu danych osobowych posiadają stosowne upoważnienia i zostały zobowiązane do zachowania tych danych w tajemnicy.			
3.	Rejestr Kategorii Czynności Przetwarzania			
4.	Ustanowiono i wdrożono Politykę bezpieczeństwa danych osobowych			
5.	Szkolenia pracowników			
6.	Audyt bezpieczeństwa w okresie ostatnich 2 lat			
7.	Testy penetracyjne			
8.	Testy socjotechniczne			
9.	Procedura postępowania w przypadku naruszenia ochrony danych osobowych			
10.	Wdrożono SZBI w oparciu o ISO 27001			
11.	Wykonano analizę ryzyka w zakresie zagrożeń: a) przypadkowego lub niezgodnego z prawem zniszczenia danych, b) utraty, modyfikacji, nieuprawnionego ujawnienia danych, c) nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych			
12.	Zapewniono: b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, c) zdolność do szybkiego przywracania dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,			
13.	fizyczne zabezpieczenia pomieszczeń/obszarów przetwarzania danych osobowych przed dostępem osób nieuprawnionych			
14.	Zabezpieczenie dostępu do sprzętu			
15.	Zabezpieczenie dostępu do serwerowni			
16.	Systemy alarmowe/ antywłamaniowe			
17.	Monitoring wizyjny			
18.	Klimatyzacja serwerowni			
19.	Systemy antywirusowe			
20.	Serwery proxy i bramki filtrujące			
21.	Ochrona fizyczna obiektu			
22.	Zarządzanie pojemnością systemów			
23.	Kopie bezpieczeństwa oraz polityka realizacji kopii			
24.	Kontrola dostępu i zarządzanie przywilejami w systemach teleinformatycznych			

L.p.	Środek techniczny i organizacyjny	Tak	Nie/ Nie dotyczy	Uwagi
25.	Lokalizacja infrastruktury informatycznej w lokalizacjach bezpiecznych			
26.	Umowy serwisowe			
27.	Umowy powierzenia przetwarzania danych			
28.	Kary umowne z dostawcami usług			
29.	Zapasoowe centrum danych			
30.	Zabezpieczenie dostępu do systemów			
