Załącznik nr 4

Umowa powierzenia przetwarzania danych osobowych (dalej: UPD)

zawarte w dniu ……. …… 2022 roku w Warszawie pomiędzy:
Ośrodkiem Przetwarzania Informacji – Państwowym Instytutem Badawczym, z siedzibą w Warszawie (00-608), przy al. Niepodległości 188 b, wpisanym do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy Sąd Gospodarczy XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000127372, NIP: 525-000-91-40, REGON: 006746090,
reprezentowanym przez dr inż. Jarosława Protasiewicza – Dyrektora Instytutu,
zwanym dalej "**Administratorem**",
a
……
zwanymi dalej "**Podmiotem przetwarzającym**".

§ 1

Powierzenie przetwarzania danych osobowych

1. W związku z realizacją Umowy nr …….. z dnia …….. dotyczącej świadczenia usług serwisowych urządzeń wielofunkcyjnych (dalej: Umowa), Podmiot przetwarzający będzie przetwarzał w imieniu Administratora dane osobowe , znajdujące się w serwisowanych urządzeniach.
2. Przedmiotem przetwarzania są dane wskazane w ust. 1.
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:
   1) postanowień UPD,
   2) 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***).
2. Administrator oświadcza, że jest Administratorem danych oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Podmiotowi przetwarzającemu.
3. 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.
4. 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.
5. Przetwarzanie danych osobowych wskazanych w ust. 1 odbywa się w miejscu serwisowanych urządzeń na co Administrator wyraża zgodę.
6. 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.

§ 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 prawidłowej realizacji Umowy, obejmującym takie operacje jak podgląd danych znajdujących się w serwisowanych urządzeniach wielofunkcyjnych.
2. Charakter przetwarzania danych wynika z Umowy i określony jest rolą Podmiotu przetwarzającego jako podmiotu realizującego na rzecz Administratora stałą usługę serwisu urządzeń wielofunkcyjnych, dokonywania przeglądów oraz aktualizacji i usuwania błędów oprogramowania.
3. Przetwarzanie danych osobowych będzie dotyczyć następujących kategorii osób: użytkownicy urządzeń. .

§ 3

Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się:
   1) dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych,
   2) przy przetwarzaniu powierzonych danych osobowych na podstawie Umowy, zabezpieczyć je poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, zapewniających 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 1,
   3) nadać upoważnienia do przetwarzania danych osobowych wskazanych w § 1 ust. 1 wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji Umowy,
   4) prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych,
   5) zapewnić zachowanie w tajemnicy przetwarzanych danych oraz sposobów ich zabezpieczenia przez osoby, które posiadają upoważnia do przetwarzania danych osobowych w celu realizacji Umowy, zarówno w trakcie zatrudnienia lub współpracy z Podmiotem przetwarzającym jak i po ustaniu zatrudnienia lub współpracy,
   6) stosować się do wewnętrznych procedur bezpieczeństwa informacji obowiązujących u Administratora w trakcie realizacji przeglądów,
   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 § 9.

2. Podmiot przetwarzający pomaga Administratorowi:
   1) uwzględniając charakter przetwarzania, kontekst usługi oraz 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. 32-33 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 § 9 ust. 2 UPD niezwłocznie, jednak nie później niż w terminie 24 godzin od chwili stwierdzenia naruszenia, z uwzględnieniem postanowień ust. 1 pkt 8 i § 9).

3. Podmiot przetwarzający nie jest uprawniony do przetwarzania danych poza siedzibą Zamawiającego. Po zakończeniu przeglądu w danym dniu zobowiązany do usunięcia lub zwrotu Administratorowi na jego żądanie powierzonych danych osobowych, w tym istniejących kopii danych.

§ 4

Prawo do kontroli

1. Administrator ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu danych spełniają postanowienia UPD i Rozporządzenia.
2. Podmiot przetwarzający na każde żądanie Administratora zobowiązany jest do udzielenia informacji dotyczących przetwarzania powierzonych mu danych osobowych.
3. Administrator ma prawo do weryfikacji sposobu przetwarzania danych osobowych wskazanych w § 1 ust. 1 .
4. Podmiot przetwarzający udostępni Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązku określonego w art. 28 Rozporządzenia.
5. Po stwierdzeniu przez Administratora naruszeń UPD Podmiot przetwarzający jest zobowiązany do ich niezwłocznego usunięcia.

§5

Podpowierzenie

Administrator nie wyraża zgody na dalsze podpowierzenie przetwarzania danych.

§ 6

Odpowiedzialność

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy lub UPD, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym lub nieuprawnionym.
2. 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 jakiejkolwiek 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 i przepisów Rozporządzenia.
3. 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 posiadł informację na temat wystąpienia roszczenia strony trzeciej.
4. W celu uniknięcia wątpliwości, Podmiot przetwarzający ponosi odpowiedzialność za działania swoich pracowników i innych osób oraz podmiotów, przy pomocy których przetwarza powierzone dane osobowe, czy też umożliwia im dostęp do powierzonych danych, w tym podwykonawców jak za własne działanie i zaniechanie.
5. Za szkody wyrządzone Administratorowi z tytułu przetwarzania danych osobowych w sposób naruszający przepisy o ochronie danych osobowych lub UPD Administrator może dochodzić od Podmiotu przetwarzającego odszkodowania na zasadach ogólnych, z zastrzeżeniem postanowień poniżej.
6. Za każde naruszenie postanowień UPD, zasad dotyczących przetwarzania i ochrony danych osobowych w niej określonych lub w powszechnie obowiązujących przepisach prawa, w tym RODO, Administrator może żądać od Podmiotu przetwarzającego kary umownej w wysokości 5 000 zł (słownie złotych: pięć tysięcy zł) za każdy przypadek naruszenia. Za przypadek naruszenia rozumie się w szczególności każde jednorazowe, niezgodne z prawem lub UPD przetwarzanie danych osobowych osoby fizycznej, której

dane dotyczą. Administrator może dochodzić odszkodowania przewyższającego wysokość kar umownych.

7. Karę umowną Podmiot przetwarzający zobowiązany będzie zapłacić na wskazany przez Administratora rachunek bankowy przelewem, w terminie 7 dni od dnia doręczenia mu przez Administratora żądania zapłaty takiej kary umownej.

§ 7

Czas obowiązywania umowy

1. UPD obowiązuje przez okres obowiązywania Umowy.

§ 8

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.
2. Podmiot przetwarzający oświadcza, że z zastrzeżeniem § 5 UPD, w związku ze zobowiązaniem do zachowania w tajemnicy danych osobowych 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.

§ 9

Naruszenie bezpieczeństwa danych

1. Podmiot przetwarzający musi niezwłocznie powiadomić Administratora 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.

§10

Postanowienia końcowe

1. 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 - Inspektor Ochrony Danych e-mail: iod@opi.org.pl

b) ze strony Podmiotu przetwarzającego – ……., e-mail: ……

2. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
3. Sądem właściwym dla rozpatrywania sporów jest sąd właściwy dla siedziby Administratora.
4. W sprawach nieuregulowanych zastosowanie mają przepisy Kodeksu cywilnego oraz Rozporządzenia.

_____	_____
Administrator	Podmiot przetwarzający

Załącznik nr 1 – wykaz stosowanych środków technicznych i organizacyjnych

L.p.	Środek techniczny i organizacyjny	Tak	Nie/ Nie dotyczy	Uwagi

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			
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			

L.p.	Środek techniczny i organizacyjny	Tak	Nie/ Nie dotyczy	Uwagi
23.	Kopie bezpieczeństwa			
24.	Kontrola dostępu i zarządzanie przywilejami w systemach teleinformatycznych			
25.	Lokalizacja infrastruktury informatycznej w lokalizacjach bezpiecznych			
26.	Umowy serwisowe			
27.	Umowy powierzenia przetwarzania danych			
28.	Kary umowne z dostawcami usług			
29.	Zapasowe centrum danych			
30.	Zabezpieczenie dostępu do systemów			