Załącznik Nr 7b do SIWZ
Załącznik Nr 4 do umowy

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH UZYTKOWNIKÓW PLATFORMY

zawarta w dniu …… …… 2018 roku w Pabianicach, pomiędzy:

Miastem Pabianice z siedzibą: 95-200 Pabianice, ul. Zamkowa 16, REGON 472057715, NIP 731 196 27 56, które reprezentuje Grzegorz Mackiewicz – Prezydent Miasta Pabianic, zwanym dalej „Zamawiającym”
a
……., z siedzibą: ……, REGON: ……, NIP: ……, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla ……, …… Wydział Gospodarczy Krajowego Rejestru Sądowego, numer KRS: …….., wysokość kapitału zakładowego: …… zł, którą reprezentuje ……. – ……, zwanym dalej „Wykonawcą”,

zwanymi w dalszej części Umowy łącznie Stronami, a każdą z osobna Stroną.

§1.
Definicje

W niniejszej Umowie „Prawo ochrony danych” oznacza „Rozporządzenie nr 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”). W niniejszej Umowie „**dane osobowe**”, „**Administrator danych**”, „**Podmiot przetwarzający**”, „**przetwarzanie**”, „**podmioty, których dotyczą dane osobowe**”, „**szczególne kategorie danych osobowych**”, „**naruszenie ochrony danych osobowych**” i „**organ nadzorczy**” mają znaczenie nadane im w Rozporządzeniu.

§2.
Postanowienia ogólne

1. W trakcie świadczenia usług Wykonawca będzie przetwarzać dane osobowe na rzecz Zamawiającego. W kontekście przetwarzania danych osobowych Zamawiający pełni funkcję Administratora danych, a Wykonawca – Podmiotu przetwarzającego.
2. Przedmiot, okres, charakter i cel przetwarzania danych osobowych oraz rodzaj danych osobowych i kategorie podmiotów, których te dane dotyczą są następujące:
   1) przedmiot przetwarzania danych osobowych obejmuje dane osobowe osób zarejestrowanych na platformie crowdsourcingowej dostępnej pod adresem ....., takie jak imię, nazwisko, pseudonim, adres e- mail;
   2) okres przetwarzania danych osobowych pokrywa się z okresem ważności Umowy zawartej pomiędzy Wykonawcą a Zamawiającym dnia ……....., Nr ....., zwanej dalej „Umową Główną”;
   3) dane osobowe wykorzystywane są wyłacznie w celu wykonania przedmiotu Umowy Głównej;

4) przetwarzane kategorie danych osobowych to dane osobowe, które pochodzą bezpośrednio od osób, które zarejestrowały się na Platformie (lub zostały przekazane w imieniu tych osób) lub dane osobowe, które zostały zebrane ze źródeł publicznie dostępnych, w szczególności wskazane w ust. 1.

3. Wykonawca przyjmuje do wiadomości, iż w zakresie przestrzegania przepisów Rozporządzenia, zgodnie z art. 28 ust. 10 tego Rozporządzenia, w przypadku naruszenia jego przepisów przy określeniu celów i sposobu przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

4. W celu uniknięcia wątpliwości, niniejsza Umowa nie dotyczy przetwarzania danych osobowych przez Wykonawcę w odniesieniu do wybranych procesów wewnętrznych takich jak zapewnienie działania zgodnie z wymogami regulacyjnymi i prawnymi, które mają zastosowanie do Wykonawcy, weryfikacja występowania konfliktu interesów, zarządzanie ryzykiem i przeglądy jakości oraz wewnętrzne usługi Wykonawcy w zakresie rachunkowości, systemów IT oraz innych usług wsparcia administracyjnego.

5. Jeżeli powierzone dane są przetwarzane w formie elektronicznej na serwerach i nośnikach danych Wykonawcy, serwery i nośniki te nie mogą znajdować się poza obszarem Unii Europejskiej i Europejskiego Obszaru Gospodarczego.

§3.
Obowiązki Podmiotu Przetwarzającego

1. Wykonawca zachowa w tajemnicy dane osobowe, które przetwarza w imieniu Zamawiającego oraz zapewni, by każda osoba działająca z upoważnienia Wykonawcy zapewniła poufność danych osobowych, chyba że jest ona zobowiązana do ich ujawnienia w świetle przepisów prawa lub regulacji dotyczących wykonywania zawodu. Wykonawca zobowiązuje się przetwarzać dane osobowe wyłącznie na podstawie przepisów prawa.

2. Z uwzględnieniem aktualnego stanu, kosztów implementacji oraz charakteru, zakresu, kontekstu i celów przetwarzania danych osobowych oraz ryzyka - o zmiennym prawdopodobieństwie wystąpienia i różnym stopniu - w odniesieniu do praw i obowiązków osób fizycznych, Wykonawca zobowiązuje się wdrożyć odpowiednie środki techniczne i organizacyjne, o których mowa w załączniku do umowy w celu zapewnienia poziomu bezpieczeństwa adekwatnego do ryzyka. Celem tych środków musi być również niedopuszczenie do bezpodstawnego gromadzenia i dalszego przetwarzania danych osobowych.

3. Wykonawca będzie okresowo oceniać i utrwalać, uzupełniać oraz udoskonalać środki wdrożone dotychczas w zakresie, w jakim wymagają tego obowiązujące wymogi lub postęp technologiczny.

4. Wykonawca zapewni Zamawiającemu możliwość okresowej weryfikacji wypełnienia wymogów określonych w niniejszej Umowie oraz przepisów regulujących przetwarzanie danych osobowych. Weryfikacja może być przeprowadzana w imieniu Zamawiającego przez (zewnętrznego) niezależnego audytora, chyba że audytor jest bezpośrednią spółką konkurencyjną Wykonawcy. Okresowa weryfikacja będzie ograniczona do udzielania przez Wykonawcę odpowiedzi na pytania zadane przez Zamawiającego (maksymalnie raz w roku) dotyczące działania Wykonawcy zgodnie ze stosownymi przepisami Prawa ochrony danych osobowych oraz w razie konieczności, zezwolenia Zamawiającemu na przeprowadzenie rozmowy z pracownikiem lub pracownikami działu IT Wykonawcy w siedzibie Wykonawcy.

5. Raz w roku Wykonawca zleci niezależnemu audytorowi przeprowadzenie audytu SOC 1 i SOC 2 w zakresie środków bezpieczeństwa wdrożonych przez Wykonawcę. Na pisemną

prośbę Zamawiającego Wykonawca udostępni najnowsze sprawozdania SOC 1 i SOC 2 lub jakiekolwiek inne sprawozdanie przygotowane zgodnie z porównywalnymi lub bardziej rygorystycznymi standardami.

6. Z uwzględnieniem obowiązku zachowania poufności przez Wykonawcę wobec innych klientów, Zamawiający przyjmuje i uznaje, że Wykonawca nie zezwoli Zamawiającemu ani audytorowi upoważnionemu przez Zamawiającego na uzyskanie dostępu do swoich systemów IT i/ lub infrastruktury IT.

7. Wykonawca zobowiązuje się informować Zamawiającego:
   1) o każdym przypadku naruszenia ochrony danych osobowych, który podlega zgłoszeniu zgodnie z art. 33 i 34 Rozporządzenia. Wykonawca zobowiązuje się informować Zamawiającego bez zbędnej zwłoki oraz w uzasadnionym zakresie nie później niż w ciągu 24 godzin od uzyskania informacji o naruszeniu ochrony danych osobowych.
   2) o skargach od podmiotów, których dotyczą dane osobowe i których dane osobowe są przetwarzane przez Wykonawcę.
   3) o wnioskach od podmiotów, których dotyczą dane osobowe i których dane osobowe są przetwarzane przez Wykonawcę w odniesieniu do realizacji praw w zakresie ochrony danych osobowych przysługujących im na podstawie Rozporządzenia.
   4) o audycie prowadzonym przez organ nadzoru lub inny właściwy organ, jeśli jest to dopuszczalne na podstawie stosownych przepisów prawa lub rozporządzeń.

8. Wykonawca zobowiązuje się do udzielania Zamawiającemu uzasadnionej pomocy, jakiej Zamawiający zażąda w związku z żądaniem ze strony organu nadzorczego lub innego właściwego organu lub audytem organu nadzorczego lub innego właściwego organu, lub w związku z żądaniem bądź skargą ze strony podmiotów, których dotyczą dane osobowe i których dane osobowe są przetwarzane przez Wykonawcę. Wykonawca będzie również udzielać Zamawiającemu pomocy w zakresie zapewnienia działania zgodnie ze stosownymi przepisami Prawa ochrony danych osobowych, zgodnie z którymi Zamawiający może mieć obowiązek przeprowadzania oceny skutków dla ochrony danych oraz konsultacji z organami nadzorczymi.

9. Wykonawca zobowiązuje się nie zlecać przetwarzania danych osobowych w całości ani w części do podwykonawcy bez uprzedniej pisemnej zgody Zamawiającego. Zamawiający ma prawo do odmowy udzielenia tego rodzaju zgody bez podania przyczyny lub do uzależnienia udzielenia zgody od spełnienia dodatkowych warunków. Podwykonawca Wykonawcy musi również, w ramach wymaganego minimum, wypełniać postanowienia umowy zbliżone do niniejszej umowy. W przypadku naruszenia przez podwykonawcę obowiązków w zakresie ochrony danych osobowych na podstawie tego rodzaju umowy z Wykonawcą, Wykonawca ponosi pełną odpowiedzialność wobec Zamawiającego w zakresie wypełniania obowiązków podwykonawcy na podstawie umowy podwykonawczej. Poprzez podpisanie niniejszej umowy, Zamawiający upoważnia Wykonawcę do zlecania przetwarzania danych osobowych innym Firmom z grupy Wykonawcy, udziałowcom, członkom zarządu, przedstawicielom, partnerom, dyrektorom lub pracownikom Wykonawcy oraz podmiotom trzecim udzielającym Wykonawcy wsparcia administracyjnego oraz IT.

§4.
Okres świadczenia usług przetwarzania

1. Okres świadczenia usług przetwarzania danych jest tożsamy z okresem udzielonej licencji, o której mowa w Umowie Głównej. Po wykonaniu usług przez Wykonawcę, Zamawiający wyraża zgodę na przetwarzanie danych osobowych przekazanych Wykonawcy i/lub zebranych przez niego, przez okres 3 lat od dnia zakończenia współpracy, a Wykonawca zobowiązuje się do ich zgodnego z prawem i niniejszą Umową przetwarzania:

1) w celu i zakresie niezbędnym do udowodnienia podjętej pomiędzy stronami współpracy,
2) w celu i zakresie niezbędnym do obrony przed potencjalnymi roszczeniami podmiotów, których dane osobowe dotyczą na podstawie niniejszej Umowy,
3) w celu i w zakresie niezbędnym do udowodnienia przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa.

2. Po zakończeniu wskazanego wyżej okresu w zakresie przetwarzania danych osobowych, na żądanie Zamawiającego Wykonawca zwróci Zamawiającemu wszystkie dane osobowe, a w przypadku braku takiego żądania – usunie je oraz usunie wszystkie kopie, chyba że Wykonawca podlega obowiązkowi przechowywania danych osobowych przez okres dłuższy niż okres trwania Umowy Głównej na podstawie przepisów prawa lub regulacji zawodowych.

3. Strony uznają, że Wykonawca może przechowywać dane mające status kopii zapasowych, które to dane Wykonawca może przechowywać zgodnie z obowiązującymi u Wykonawcy regulaminami przechowywania dokumentów i zapewnienia kontynuacji działalności, o ile postanowienia niniejszej Umowy dotyczące bezpieczeństwa i zachowania tajemnicy w dalszym ciągu mają do nich zastosowanie.

§ 5.
Naruszenie ochrony danych osobowych

1. Wykonawca jest odpowiedzialny za udostępnianie lub wykorzystanie danych osobowych niezgodnie z niniejsza umową, a w szczególności za bezpodstawne udostępnianie lub przekazywanie danych osobowych nieuprawnionym podmiotom lub osobom.

2. Jeżeli w związku z powierzeniem przetwarzania danych osobowych Zamawiający zostanie prawomocnym orzeczeniem sądowym zobowiązany do wypłaty odszkodowania, zadośćuczynienia lub zostanie ukarany grzywną, Wykonawca zobowiązuje się zrekompensować Zamawiającemu udokumentowane straty z tego tytułu w wysokości poniesionego odszkodowania, zadośćuczynienia lub grzywny wraz z kosztami postępowania, o ile nastąpiło to wskutek okoliczności leżących po stronie Wykonawcy.

3. Zamawiający powiadomi Wykonawcę o każdym przypadku wystąpienia z roszczeniem wobec Zamawiającego i jego podstawach prawnych i faktycznych, w celu umożliwienia Wykonawcy zajęcia stanowiska, odniesienia się do podstaw takiej odpowiedzialności i ewentualnego wystąpienia do sprawy na etapie sądowym. Wykonawca zobowiązuje się do udzielenia Zamawiającemu wszelkich wyjaśnień i pomocy w celu obrony przed roszczeniami.

4. Nie uchybiając powyższemu, Wykonawca ponosi odpowiedzialność odszkodowawczą względem Zamawiającego na zasadach ogólnych.

§ 7.
Postanowienia końcowe

1. W sprawach nieuregulowanych niniejszą umową zastosowanie będą miały przepisy ogólnie obowiązujące, w szczególności przepisy ustawy Kodeks cywilny, Ustawy o ochronie danych osobowych oraz RODO.

2. Zmiany niniejszej umowy wymagają zachowania formy pisemnego aneksu, pod rygorem nieważności.

3. Wszelkie spory związane z wykonaniem niniejszej umowy oraz wynikłe na jej tle, rozstrzygane będą przez sąd właściwy dla siedziby Zamawiającego.

4. Niniejsza umowa wchodzi w życie z dniem podpisania.

5. Niniejszą umowę powierzenia danych osobowych sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Załącznik:
Załącznik do Umowy – Bezpieczeństwo IT

…… ……

Zamawiający **Wykonawca**

Załącznik nr 1 do Umowy – Bezpieczeństwo IT

W ramach świadczenia usług, Wykonawca zobowiązuje się podejmować wszelkie niezbędne kroki oraz środki bezpieczeństwa zgodnie z uzasadnionymi biznesowo standardami sektora w celu zminimalizowania ryzyka uzyskania nieuprawnionego dostępu lub sabotowania informacji Zamawiającego i danych osobowych przekazanych Wykonawcy w celu wykonania usług.

Wykonawca zobowiązuje się utrzymać w mocy i dokonywać aktualizacji „Globalnej polityki bezpieczeństwa IT" zgodnej z normą ISO 27001/2, która określa procedury mające na celu zapewnienie bezpieczeństwa informacji Zamawiającego i danych osobowych w formie elektronicznej znajdujących się w posiadaniu Wykonawcy, przechowywanych przez Wykonawcę lub pod kontrolą Wykonawcę, w obszarach wymienionych niżej.

1. Polityka bezpieczeństwa informacji.

1.1. Wykonawca zobowiązuje się do opracowania, administrowania i utrzymania w mocy odpowiednich polityk, których celem jest ochrona systemów informacji przed utratą danych osobowych, szkodą, nieuprawnionym ujawnieniem lub przerwą w działalności, obejmujących fizyczną ochronę oraz logiczną segmentację systemów informacji, w tym informacji Zamawiającego i danych osobowych do przetwarzania lub przekazania Wykonawcy w celu wykonania usług.

2. Organizacja bezpieczeństwa informacji.

2.1. Wykonawca będzie posiadać odpowiednio wyszkolony personel z jasnym podziałem ról i obowiązków w ramach organizacji bezpieczeństwa informacji, w celu zapewnienia koordynowania wdrażania środków bezpieczeństwa u Wykonawcy.

2.2. Wykonawca określi wymogi w zakresie wrażliwości, ochrony i ujawniania informacji oraz zobowiązuje się przeprowadzać coroczną weryfikację tych wymogów.

2.3. Wykonawca zobowiązuje się przeprowadzać efektywny podział zadań, ról i obowiązków w celu niedopuszczenia do nieuprawnionego wykorzystania kluczowych aktywów Wykonawcy w zakresie informacji.

3. Zarządzanie aktywami.

3.1. Wykonawca zobowiązuje się utrzymywać procedury, których celem jest identyfikowanie, kontrolowanie i utrzymanie własności oraz kategoryzacji kluczowych aktywów pod względem bezpieczeństwa Wykonawcy oraz informacji Zamawiającego i danych osobowych przechowywanych w infrastrukturze należącej do Wykonawcy.

3.2. Wykonawca opracuje polityki określające dopuszczalne wykorzystanie informacji i aktywów oraz przekaże je do wszystkich zainteresowanych użytkowników aktywów i informacji Wykonawcy.

4. Bezpieczeństwo zasobów ludzkich.

4.1. Wykonawca opracuje oraz wdroży polityki i procedury gwarantujące odpowiedni dobór personelu Wykonawcy i stron trzecich z punktu widzenia pełnionych ról i obowiązków.

4.2. Wykonawca zapewni odpowiednie szkolenie w zakresie dostępu do informacji, tak by zwiększyć świadomość użytkowników Wykonawcy i stron trzecich w zakresie bezpieczeństwa IT w odniesieniu do informacji Zamawiającego i danych osobowych.

4.3. Wykonawca zapewni przestrzeganie wszystkich niezbędnych procedur dotyczących pracowników Wykonawcy w związku ze zmianą roli, zakończeniem zlecenia, rozwiązaniem stosunku pracy, kontraktu lub umowy.

5. Bezpieczeństwo fizyczne oraz bezpieczeństwo środowiska IT.

5.1. Wykonawca wdroży efektywne środki procedury kontroli fizycznej i środowiska IT w celu zachowania integralności oraz dostępności systemów informacji Wykonawcy oraz zawartych w nich informacji Wykonawcy / danych osobowych, niezależnie od tego, czy są one wykorzystywane w siedzibie Wykonawcy, siedzibie Zamawiającego czy siedzibie stron trzecich.

5.2. Wykonawca wdroży środki w celu zapewnienia oraz zagwarantuje funkcjonowanie infrastruktury wsparcia informacji i systemów informacji, w tym w zakresie fizycznej ochrony wszelkich urządzeń związanych z jakimkolwiek zleceniem wykonywanym na rzecz Zamawiającego.

6. Bezpieczeństwo komunikacji i operacji.

6.1. Wykonawca opracuje odpowiedni zbiór procesów i procedur do efektywnego zarządzania systemami sieci komunikacji oraz systemami przetwarzania informacji, które zawierają informacje Zamawiającego i dane osobowe, w tym w następującym zakresie:

a) zarządzanie zmianą,
b) zarządzanie wykonywaniem usług stron trzecich,
c) planowanie i zatwierdzanie systemu,
d) ochrona przed złośliwymi kodami,
e) regularne tworzenie kopii zapasowych informacji i oprogramowania,
f) zarządzanie bezpieczeństwem sieci, w tym zapewnienie bezpiecznego dostępu zdalnego, wykrywanie intruza, ochrona protokołu sieci i perymetru, środki zaradcze w celu wykrywania działań nieuprawnionych, przechowywanie i obsługa nośników cyfrowych,
g) wymiana informacji przy zastosowaniu uzgodnionych metod oraz właściwym wykorzystaniu szyfrowania,
h) monitoring oraz prowadzenie dziennika kontroli,
i) wycofanie systemów informacji z eksploatacji,
j) zarządzanie przepustowością systemów i komponentów o kluczowym znaczeniu dla działalności,
k) opracowywanie programów oraz środowisko przedprodukcyjne,
l) procedury regulujące zarządzanie, obsługę i przechowywanie nośników.

7. Kontrola dostępu.

7.1. Wykonawca wdroży procedury kontroli dostępu do systemów informacji i informacji Zamawiającego/ danych osobowych, w tym procedury kontroli identyfikacji użytkownika i kontroli dostępu.

7.2. Wykonawca będzie podejmować starania w celu ograniczenia dostępu do poufnych informacji Zamawiającego / danych osobowych do uprawnionych użytkowników, dla których konieczność uzyskania dostępu uwarunkowana jest wymogami związanymi z prowadzoną działalnością.

8. Zakup, opracowanie i zapewnienie funkcjonowania systemów informacji.

8.1. W zakresie wskazania, zakupu, opracowania i zapewnienia funkcjonowania systemów informacji, w tym systemów zakupionych od dostawców zewnętrznych oraz tych wytworzonych przy wykorzystaniu zasobów wewnętrznych, Wykonawca określi niezbędne wymogi dotyczące poufności, integralności i dostępności oraz zobowiązuje się przeprowadzać ich weryfikację z uwzględnieniem stałego profilu ryzyka przez okres ich użytkowania.

8.2. Wykonawca określi i zapewni obowiązywanie zasad dotyczących odpowiednich aspektów bezpieczeństwa w ramach procesu projektowania oprogramowania.

8.3. Wykonawca wskaże i oceni zgłoszone potencjalne usterki techniczne i istniejące zagrożenia oraz wdroży efektywną ścieżkę oraz politykę zarządzania podatnością na zagrożenia w celu zapewnienia, w razie konieczności, naprawy systemów informacji Wykonawcy.

9. Zarządzanie zdarzeniami związanymi z bezpieczeństwem informacji.

9.1. Wykonawca opracuje i utrzyma w mocy plan reagowania na zdarzenia oraz program zawierający procedury i instrukcje postępowania w razie wystąpienia zdarzenia związanego z bezpieczeństwem infrastruktury komputerowej Wykonawcy wraz z dokumentacją niezbędnych kroków oraz kanałów komunikacji do wykorzystania.

9.2. Wykonawca zapewni, by instrukcje postępowania zawierały odpowiednie procedury niezwłocznego powiadamiania Zamawiajacego oraz innych kluczowych interesariuszy o każdym zdarzeniu związanym z bezpieczeństwem w przypadku stwierdzenia, że skutkuje ono naruszeniem zasad bezpieczeństwa danych osobowych.

10. Aspekty zarządzania kontynuacją działalności związane z bezpieczeństwem informacji.

10.1. Wykonawca przeprowadzi i utrzyma w mocy analizy wpływu zdarzeń na kontynuację działalności oraz planów działania na wypadek utraty danych, których celem jest zagwarantowanie wykonywania usług Wykonawcy przy minimalnych możliwych przerwach. Każdy plan będzie zawierać szczegółowy opis środków służących do skutecznego przywrócenia świadczenia usług w celu wznowienia działalności po wystąpieniu zdarzenia nadzwyczajnego w najkrótszym możliwym terminie.

10.2. Wykonawca będzie przeprowadzać okresowe testy najważniejszych aplikacji biznesowych firmy w celu zagwarantowania ich natychmiastowej dostępności w przypadku zgłoszonej awarii. Wykonawca zapewni przeniesienie kopii zapasowych poza siedzibę, którego celem jest wsparcie przywrócenia funkcjonowania systemów Wykonawcy w przypadku awarii.

11. Spełnienie wymogów.

11.1. Wykonawca gwarantuje, że systemy informacyjne Wykonawcy spełniają wymogi i są zgodne z politykami bezpieczeństwa, odpowiednimi wymogami ustawowymi i przepisami rozporządzeń.

11.2. Wykonawca wdroży odpowiednie procedury kontrolne ograniczające dostęp do narzędzi i systemów w celu uniemożliwienia nieuprawnionego korzystania lub naruszenia integralności systemów oraz gwarantujące zgodność przeprowadzanych kontroli z „Globalną polityką bezpieczeństwa IT u Wykonawcy – kodeks obligatoryjnych wymogów warunkujących korzystanie z systemu”.

12. Kryptograficzne procedury kontrolne.

12.1. Wykonawca opracuje i wdroży politykę w zakresie stosowania kryptograficznych procedur kontrolnych w zakresie zapewnienia stałej ochrony, poufności i zachowania integralności wrażliwych informacji i aktywów.

13. Relacje z dostawcami.

13.1. Wykonawca podpisze i utrzyma w mocy formalne umowy ze stronami trzecimi uczestniczącymi w zarządzaniu świadczeniem usług w zakresie systemów informacji Wykonawcy, włączając w stosownym zakresie niezbędne procedury i polityki bezpieczeństwa oraz umowy w sprawie świadczenia usług.