Umowa powierzenia przetwarzania danych osobowych

zawarta w dniu _____2023 r. we Wrześni pomiędzy:

Gminą Września z siedzibą ul. Ratuszowa 1, 62-300 Września, NIP 789–10–01–386 reprezentowaną przez: Tomasza Kałużnego – Burmistrza Miasta i Gminy Września przy kontrasygnacie Jolanty Kościańskiej – Skarbnika Miasta i Gminy Września zwanym w treści umowy **„Administratorem”,**

a

_____

z siedzibą we _____, przy ul. _____, dla której Sąd Rejonowy dla _____ prowadzi akta rejestrowe pod numerem Krajowego Rejestru Sądowego _____, numer NIP: _____ numer Regon _____, reprezentowaną przez: _____
zwaną w dalszej części Umowy **„Przetwarzającym”.**

Projekt pn. ”Rozwój elektronicznych usług publicznych w gminie Września” współfinansowany
w ramach Regionalnego Programu Operacyjnego Województwa Wielkopolskiego na lata 2014-2020

Spis treści:

Projekt pn. "Rozwój elektronicznych usług publicznych w gminie Września" współfinansowany
w ramach Regionalnego Programu Operacyjnego Województwa Wielkopolskiego na lata 2014-2020

§ 1. Definicje mające zastosowanie w Umowie

O ile treść Umowy nie stanowi inaczej, użyte w niniejszej Umowie określenia posiadają następujące znaczenie:

Nazwa	Definicja
Dane Osobowe (DO)	Dane w rozumieniu art. 4 pkt 1) RODO, tj. wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
Inspektor Ochrony Danych (IOD)	Osoba wyznaczana do wypełnienia zadań, o których mowa w art. 39 RODO.
Podpowierzenie	Dalsze powierzenie Przetwarzania Danych Osobowych.
Przetwarzanie Danych Osobowych	Wszelkie operacje lub zestaw operacji wykonywanych na Danych Osobowych lub zestawach Danych Osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie w rozumieniu art. 4 pkt 2) RODO.
RODO	Rozporządzenie 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1).
Umowa	Niniejsza umowa
Umowa Główna	Umowa nr … z dnia … zawarta z Przetwarzającym, jako wykonawcą zamówienia pn. *„Przeprowadzenie niezależnych testów bezpieczeństwa: Infrastruktury Teleinformatycznej, Aplikacji Web oraz Aplikacji Mobilnej Zintegrowanego Systemu Zarządzania Gminą”.*
Zbiór / Zbiory Danych	Uporządkowany ustrukturyzowany zestaw danych dziedzinowych zawierający Dane osobowe mający formę elektroniczną. Zbiór Danych może mieć postać jednorodnego zestawu danych w formie pliku (np. logi systemowe) lub zbioru plików tekstowych / binarnych, w tym zbiorów stanowiących struktury danych (tabel, rekordów) systemu zarządzania relacyjnej bazą danych (PostgreSQL, Firebird).

Projekt pn. ”Rozwój elektronicznych usług publicznych w gminie Września” współfinansowany w ramach Regionalnego Programu Operacyjnego Województwa Wielkopolskiego na lata 2014-2020

§ 2. Przedmiot Umowy

1. Na podstawie art. 28 ust.3 RODO Administrator powierza Przetwarzającemu (zwanemu w Umowie Głównej – Wykonawcą lub Pentesterem) Przetwarzanie Danych Osobowych w zakresie Zbiorów Danych w Infrastrukturze Technicznej Zamawiającego, jaka została wskazana w Umowie Głównej (OPZ Załącznik nr 1-3) – do przeprowadzenia czynności, o których mowa w ust. 4
2. Dane zawarte w Zbiorach Danych, o których mowa w ust. 1 nie zaliczają się do zamkniętego katalogu danych szczególnej kategorii, a co za tym idzie nie podlegają szczególnej ochronie. Dane te stanowią kategorie danych zwykłych, takich jak: imię / imiona, nazwisko / nazwiska, adres / adresy (ulica, nr budynku, nr lokalu, kod pocztowy, miejscowość/poczta), numer PESEL, numer NIP, dane kontaktowe, a także powiązane z nimi lub zależne takie dane, jak numer telefonu, adres e-mail, czy adres IP.
3. Rodzajowo dane zawarte w Zbiorach Danych odnoszą się do interesantów Gminy Września (Urzędu Miasta i Gminy Września) takich grup osób, jak: podatnicy i płatnicy Miasta i Gminy Września, osoby pełniące rolę pełnomocników osób fizycznych lub osób prawnych, mieszkańcy gminy Września oraz osoby fizyczne, które zainicjowały czynności formalno – prawne w zakresie kompetencji i zadań prowadzonych przez Gminę i Miasto Września – a także, dane pracowników, współpracowników Administratora.
4. Celem Przetwarzania Danych Osobowych jest wykonanie Umowy Głównej w zakresie czynności związanych z realizacją zamówienia pn. *„Przeprowadzenie niezależnych testów bezpieczeństwa: Infrastruktury Teleinformatycznej, Aplikacji Web oraz Aplikacji Mobilnej Zintegrowanego Systemu Zarządzania Gminą”,* którego celem zgodnie z Umową Główną jest m.in.:

1) ocena zastosowanych przez Wykonawcę Systemu RATUSZ mechanizmów bezpieczeństwa danych, w tym ich integralności, spójności i rozliczalności;
2) ocena aspektu ciągłości i dostępności danych oraz funkcji przedmiotowego systemu – służącego do gromadzenia i przetwarzania danych, w tym danych DO;
3) przeprowadzenie testów bezpieczeństwa, w tym testów inwazyjnych.

5. Przetwarzanie Danych Osobowych jest nieodpłatne i obejmuje wyłącznie dane w formie elektronicznych Zbiorów Danych.
6. Niniejsza Umowa stanowi udokumentowane polecenie Administratora w zakresie Przetwarzania Danych Osobowych przez Przetwarzającego.
7. Administrator upoważnia Przetwarzającego do udzielenia poleceń Przetwarzania Danych Osobowych w zakresie niezbędnym do wykonania Umowy Głównej i niniejszej Umowy. Powyższe upoważnienie nie obejmuje upoważnienia do powierzenia Przetwarzania Danych Osobowych innemu podmiotowi, o czym mowa w §6.
8. Niniejsza Umowa oraz Umowa Główna stanowią realizację wydzielonego zadania realizowanego w ramach prowadzonego przez Gminę i Miasta Września projektu pn. *„Rozwój elektronicznych usług publicznych w Gminie Września”* w ramach Wielkopolskiego Regionalnego Programu Operacyjnego (WRPO) na lata 2014-2020: Oś Priorytetowa 2: „Społeczeństwo informacyjne” Działanie 2.1 „Rozwój elektronicznych usług publicznych”, Poddziałanie 2.1.1.

Projekt pn. ”Rozwój elektronicznych usług publicznych w gminie Września” współfinansowany
w ramach Regionalnego Programu Operacyjnego Województwa Wielkopolskiego na lata 2014-2020

§ 3. Szczegółowe zasady powierzenia przetwarzania danych

1. Przed rozpoczęciem Przetwarzania Danych Osobowych Przetwarzający musi podjąć środki, które zabezpieczą Dane Osobowe, o których mowa w art. 32 RODO, a w szczególności musi:

1) zastosować środki techniczne i organizacyjne zapewniające bezpieczeństwo Przetwarzanych Danych Osobowych, o których mowa w art. 32 RODO, uwzględniając w tych działaniach stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia;
2) udokumentować odpowiednio zastosowanie środków, o których mowa stanowi pkt. 1);
3) umożliwiać Administratorowi, na każde żądanie, dokonania oceny i przeglądu stosowanych środków technicznych i organizacyjnych i dokumentacji dotyczącej tych środków, aby przetwarzanie toczyło się zgodnie z prawem, a także wprowadzić zalecenia dot. zmiany lub uaktualnienia tych środków, o ile w opinii Administratora są one niewystarczające do tego, aby zapewnić zgodne z prawem Przetwarzanie Danych Osobowych powierzonych Przetwarzającemu;
4) zapewnić by każda osoba fizyczna działająca z upoważnienia Przetwarzającego, która ma dostęp do Danych Osobowych, przetwarzała je wyłącznie na polecenie Przetwarzającego;
5) prowadzić ewidencję osób upoważnionych do Przetwarzania Danych Osobowych przetwarzanych w związku z wykonywaniem Umowy Głównej;

2. Przetwarzający zobowiązuje się do zachowania w tajemnicy Danych Osobowych oraz sposobów ich zabezpieczenia, w tym także po rozwiązaniu Umowy oraz zobowiązuje się zapewnić, aby przedmiotowe zobowiązania były również w mocy prawa wobec osób Przetwarzających Dane Osobowe na jego polecenie.
3. Przetwarzający zobowiązuje się, iż dopuści do Przetwarzania Danych Osobowych wyłącznie i tylko te osoby, które zostały przez niego upoważnione do Przetwarzania Danych Osobowych w ramach niniejszej Umowy oraz podpisały zobowiązanie do zachowaniu w tajemnicy Danych Osobowych, w tym sposobów ich zabezpieczenia.
4. Przetwarzający nie może kopiować, przekazywać, wykorzystywać, ujawniać, powielać, a tym bardziej rozpowszechniać uzyskanych od Administratora Dane Osobowe. Powyższe zobowiązanie jest wyłączone w sytuacji, gdy określone czynności następują w celu wykonania niniejszej Umowy lub Umowy Głównej na polecenie Administratora.

§ 4. Obowiązki Przetwarzającego

1. Przetwarzający oświadcza, iż dysponuje odpowiednimi środkami technicznymi i organizacyjnymi spełniającymi wymogi RODO, doświadczeniem, wiedzą i wykwalifikowanym personelem, umożliwiającymi prawidłowe wykonanie niniejszej Umowy i Projektu.
2. Przetwarzający zobowiązuje się dopuszczać do przetwarzania danych osoby poinformowane oraz przeszkolone z obowiązujących przepisów o ochronie danych osobowych oraz zasad z nich wynikających, posiadające stosowne upoważnienia do przetwarzania danych osobowych.
3. Przetwarzający ponosi pełną, prawną odpowiedzialność za nieuprawnione udostępnienie lub wykorzystanie danych osobowych niezgodnie z niniejszą Umową.

Projekt pn. "Rozwój elektronicznych usług publicznych w gminie Września" współfinansowany
w ramach Regionalnego Programu Operacyjnego Województwa Wielkopolskiego na lata 2014-2020

4. W przypadku rozwiązania niniejszej Umowy lub ustania celu powierzenia Przetwarzania Danych Osobowych, Przetwarzający zobowiązany jest, odpowiednio do decyzji Administratora do usunięcia wszelkich Danych Osobowych oraz usunięcia ich istniejących kopii.
5. Przetwarzający zobowiązuje się pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO. W szczególności, Przetwarzający zobowiązuje się przekazywać Administratorowi informacje oraz wykonywać jego polecenia dotyczące stosowanych środków zabezpieczania Danych Osobowych oraz przypadków naruszenia ochrony Danych Osobowych. Przetwarzający w szczególności ma obowiązek:

1) przekazania Administratorowi informacji dotyczących naruszenia ochrony Danych Osobowych w ciągu 24 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych;
2) przygotowania w ciągu 24 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony Danych Osobowych informacji wymaganych w zgłoszeniu naruszenia ochrony danych do organu nadzorczego, o których mowa w art. 33 ust. 3 RODO;
3) prowadzenia rejestru naruszeń ochrony danych, w którym dokumentowane są wszelkie naruszenia ochrony Danych Osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze;
4) przeprowadzenia wstępnej analizy ryzyka naruszenia praw i wolności podmiotów danych i przekazania wyników tej analizy do Administratorowi w ciągu 36 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony Danych Osobowych;
5) podania wszystkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, o których mowa w art. 33 ust. 3 RODO w ciągu 24 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony Danych Osobowych;
6) wyznaczenia osób odpowiedzialnych za podjęcie kroków w celu zaradzenia naruszeniu i podjęcia działań naprawczych w uzgodnieniu z Powierzającym;
7) szacowania ryzyka naruszenia praw lub wolności pomiotów danych / oceny analizy ryzyka przeprowadzonej przez Administratora;
8) dokonanie analizy, czy zachodzi obowiązek przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych,
9) udzielania Administratorowi informacji potrzebnych do przeprowadzenia sporządzenia oceny skutków planowanych operacji przetwarzania dla ochrony Danych Osobowych, o których mowa w art. 35 RODO;
10) udzielania Administratorowi informacji potrzebnych do konsultacji z organem nadzorczym w zakresie oceny skutków dla ochrony danych, o których mowa w art. 35 ust. 2 oraz art. 36 RODO.

6. Przetwarzający jest zobowiązany w ciągu 48 godzin powiadomić Administratora o każdym przypadku naruszenia ochrony danych, które mogłoby stanowić podstawę zgłoszenia roszczeń, w związku z naruszeniem zasad przetwarzania danych osobowych, gdy okoliczności zdarzenia wskazują na jego odpowiedzialność lub współodpowiedzialność w powstaniu takich roszczeń. Niniejszy ustęp dotyczy wyłącznie Danych Osobowych powierzonych Przetwarzającemu przez Administratora.
7. Przetwarzający zobowiązuje się udostępnić Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, o których mowa w art. 28 RODO.

Projekt pn. ”Rozwój elektronicznych usług publicznych w gminie Września” współfinansowany
w ramach Regionalnego Programu Operacyjnego Województwa Wielkopolskiego na lata 2014-2020

8. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym Przetwarzania Danych Osobowych przez Przetwarzającego, a także, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym Przetwarzania Danych Osobowych, skierowanej do Przetwarzającego, w tym o wszelkich kontrolach i inspekcjach dotyczących Przetwarzania Danych Osobowych przez Przetwarzającego, w szczególności prowadzonych przez organ nadzorczy.

§ 5. Prawo kontroli i audytu

1. Zgodnie z art. 28 ust. 3 lit. h) RODO Administrator ma prawo przeprowadzenia kontroli przestrzegania przez Przetwarzającego postanowień niniejszej Umowy.
2. Czynności kontroli mogą mieć formę inspekcji odnoszącej się do określonego zakresu Przetwarzania Danych Osobowych zgodnie z Umową.
3. Podczas czynności kontroli Przetwarzający jest zobowiązany udostępnić Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
4. Na wniosek Administratora przywołujący wyniki kontroli – inspekcji lub audytu - Przetwarzający jest zobowiązany do niezwłocznego zastosowania się do poleceń Administratora w zakresie związanym z realizacją Umowy, w tym w szczególności do wskazanych uchybień oraz – o ile zostało to podniesione we wnioskach z audytu – zaleceń dotyczących sposobu Przetwarzania Danych Osobowych i zapewnienia bezpieczeństwem danych.

§ 6. Powierzenie przetwarzania danych innemu podmiotowi

1. Przetwarzający zgodnie z art 28 RODO może korzystać z usług innego podmiotu przetwarzającego dane, zgłoszonego Administratorowi, co do którego Administrator nie zgłosił sprzeciwu zgodnie z ust. 2 poniżej.
2. Administrator może zgłosić uzasadniony sprzeciw względem dalszego powierzenia przetwarzania danych konkretnemu podmiotowi trzeciemu w ciągu 3 dni od dnia otrzymania informacji w tym zakresie.
3. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć Przetwarzania Danych Osobowych podmiotowi objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego podpowierzenia, to wówczas Przetwarzający musi wycofać wyrażoną zgodę i polecenie powierzenia przetwarzania danych udzielone temu podmiotowi w możliwie, jak najkrótszym terminie – nie później niż w ciągu 2 dni od dnia otrzymania sprzeciwu.
4. Jeżeli nie będzie to możliwe bez uszczerbku na świadczeniu usług w ramach Umowy lub Umowy Głównej, Przetwarzający poinformuje o tym Administratora oraz o skutkach wniesienia takiego sprzeciwu.
5. W przypadku potwierdzenia wniesienia sprzeciwu przez Administratora, czynność ta następuje na ryzyko i z woli Administratora, a tym samym tenże zrzeka się wszelkich roszczeń z tytułu problemów, jakie mogą wyniknąć w świadczeniu usług zgodnie z Umową, spowodowanych wniesieniem sprzeciwu.

Projekt pn. "Rozwój elektronicznych usług publicznych w gminie Września" współfinansowany
w ramach Regionalnego Programu Operacyjnego Województwa Wielkopolskiego na lata 2014-2020

6. W przypadku brak sprzeciwu, Przetwarzający zobowiązuje się zawrzeć umowę na powierzenie Przetwarzania Danych Osobowych z innym podmiotem zapewniającą, co najmniej taki sam standard ochrony, jaki został uregulowany w Umowie. W wyjątkowych okolicznościach dopuszcza się zawarcie umowy podpowierzenia opartej o zwyczajowo używane klauzule umowne.
7. Zaakceptowane przez Administratora na dzień zawarcia Umowy inne podmioty Przetwarzające Dane Osobowe wskazano w Załączniku nr 2 do Umowy.
8. Zmiana Załącznika nr 2 przez wprowadzenie lub wykreślenie innego podmiotu upoważnionego do przetwarzania danych wymaga zmiany Umowy.

§ 7. Czas obowiązywania umowy

1. Niniejsza Umowa wchodzi w życie z dniem jej zawarcia i obowiązuje przez okres obowiązywania Umowy Głównej.
2. Umowa może zostać rozwiązana w następujących przypadkach:

1) na podstawie porozumienia Stron;
2) w przypadku wystąpienia okoliczności uniemożliwiających dalsze wykonywanie obowiązków wynikających z Umowy;
3) w sytuacji kiedy Przetwarzający przetwarza dane osobowe niezgodnie z obowiązującymi przepisami prawa.

§ 8. Koordynacja realizacji Umowy

1. Strony wyznaczą, każdy ze swojej strony, po jednej osobie, która będzie odpowiedzialna za koordynację współpracy.
2. Zmiana osób, o których mowa w ust. 1 nie stanowi zmiany Umowy i wymaga jedynie pisemnego poinformowania drugiej Strony. Do czasu otrzymania informacji o zmianie danych, za prawidłowe dane do kontaktu uznaje się dane dotychczasowe.

§ 9. Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. Spory mogące wyniknąć w związku z realizacją Umowy, Strony będą starały się rozwiązywać polubownie.
3. W sprawach nieuregulowanych zastosowanie będą miały obowiązujące przepisy, w szczególności RODO, ustawy z 10 maja 2018 r. o ochronie danych osobowych oraz ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny.
4. Umowa została sporządzona w formie elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym osoby uprawnionej do reprezentowania każdej ze Stron.
5. Integralną część Umowy stanowi Załącznik:

Projekt pn. "Rozwój elektronicznych usług publicznych w gminie Września" współfinansowany
w ramach Regionalnego Programu Operacyjnego Województwa Wielkopolskiego na lata 2014-2020

6. Załącznik nr 1 – Wykaz Zbiorów Danych
7. Załącznik nr 2 – Wykaz innych podmiotów upoważnionych do Przetwarzania Danych Osobowych

Załącznik nr 1 do Umowy – Wykaz Zbiorów Danych

Zidentyfikowane przez Przetwarzającego zbiory danych w toku czynności obejmujących rozeznanie Infrastruktury Technicznej, systemowej i aplikacyjnej do przeprowadzenia testów bezpieczeństwa, w tym w szczególności bazy danych systemów zarządzania relacyjną bazą danych – PostgreSQL i FirBird, o których mowa w Załączniku nr 1 do Opisu Przedmiotu Zamówienia do Umowy Głównej.

Załącznik nr 2 do Umowy – Wykaz innych podmiotów upoważnionych do przetwarzania danych osobowych

Zgodnie z wykazem podwykonawców, jaki został wskazany w Ofercie Przetwarzającego.

Projekt pn. ”Rozwój elektronicznych usług publicznych w gminie Września” współfinansowany
w ramach Regionalnego Programu Operacyjnego Województwa Wielkopolskiego na lata 2014-2020