UMOWA POWIERZENIA

przetwarzania danych osobowych

zawarta w dniu …… r. w …… pomiędzy:

…… z siedzibą w ……, adres: ……, NIP ……, reprezentowaną przez ……, zwaną dalej **„Administratorem”**,

a

Rafałem Walaskiem, prowadzącym działalność gospodarczą pod firmą HERNET Rafał Walasek, adres: Korzeniów 170, 08-504 Ułęż, NIP 5060130080, REGON 545507100, zwanym dalej **„Podmiotem przetwarzającym”**, zwanymi dalej łącznie „Stronami”,

w związku z umową nr …… z dnia …… dotyczącą oprogramowania Ewiden (dalej „Umowa Główna”).

§ 1
Powierzenie

1. Na podstawie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (dalej „RODO”) Administrator powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w zakresie i celu określonych w Umowie, a Podmiot przetwarzający zobowiązuje się przetwarzać je zgodnie z Umową i przepisami prawa.
2. Ilekroć w Umowie mowa jest o przetwarzaniu, naruszeniu ochrony danych osobowych lub innych pojęciach zdefiniowanych w RODO, należy je rozumieć zgodnie z RODO.

§ 2
Zakres, charakter i cel przetwarzania

1. Dane osobowe przetwarzane są wyłącznie w celu wykonania Umowy Głównej, w szczególności instalacji, konfiguracji, importu danych, aktualizacji oprogramowania Ewiden, diagnozowania i usuwania błędów oraz udzielania konsultacji.
2. Dane przechowywane są na serwerze Administratora. Przetwarzanie przez Podmiot przetwarzający obejmuje operacje niezbędne do osiągnięcia celu, o którym mowa w ust. 1, w szczególności przeglądanie, wyszukiwanie, kopiowanie w zakresie niezbędnym do diagnozy, modyfikowanie na polecenie Administratora i usuwanie.
3. Podmiot przetwarzający nie przechowuje danych Administratora w swoich systemach. Jeżeli do usunięcia błędu niezbędne jest przekazanie kopii danych, następuje to za zgodą Administratora wyrażoną w postaci elektronicznej. Kopię przekazuje się w postaci zaszyfrowanej i usuwa niezwłocznie po naprawieniu błędu, nie później niż w terminie 14 dni.
4. Rodzaje danych osobowych i kategorie osób, których dane dotyczą, określa Załącznik nr 1.
5. Integracje oprogramowania z usługami zewnętrznymi, w szczególności z Centralnym Rejestrem Umów oraz z serwerem modelu językowego wskazanym i utrzymywanym przez Administratora, konfiguruje i uruchamia Administrator; nie stanowią one przetwarzania danych przez Podmiot przetwarzający.

§ 3
Obowiązki Podmiotu przetwarzającego

Podmiot przetwarzający zobowiązuje się:

1) przetwarzać dane wyłącznie na udokumentowane polecenie Administratora; za udokumentowane polecenie uważa się Umowę, Umowę Główną oraz polecenia przekazane w postaci elektronicznej przez osoby wskazane w Umowie Głównej, chyba że obowiązek przetwarzania nakłada na niego prawo Unii lub prawo państwa członkowskiego; w takim przypadku przed rozpoczęciem przetwarzania informuje Administratora o tym obowiązku, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
2) niezwłocznie poinformować Administratora, jeżeli jego zdaniem wydane polecenie narusza RODO lub inne przepisy o ochronie danych;
3) dopuszczać do przetwarzania danych, oprócz Podmiotu przetwarzającego działającego osobiście, wyłącznie osoby przez niego upoważnione, które zobowiązały się do zachowania tajemnicy albo podlegają ustawowemu obowiązkowi zachowania tajemnicy;
4) stosować środki techniczne i organizacyjne, o których mowa w art. 32 RODO, w tym środki określone w Załączniku nr 2;
5) pomagać Administratorowi, w miarę możliwości, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, oraz z obowiązków określonych w art. 32–36 RODO;
6) prowadzić rejestr kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 RODO;
7) udostępniać Administratorowi informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO;
8) niezwłocznie przekazywać Administratorowi żądania osób, których dane dotyczą, skierowane do Podmiotu przetwarzającego, oraz informować go o kontrolach i postępowaniach organu nadzorczego dotyczących powierzonych danych;
9) nie przekazywać danych do państwa trzeciego ani organizacji międzynarodowej.

§ 4
Dalsze powierzenie

1. W dniu zawarcia Umowy Podmiot przetwarzający nie korzysta z usług innych podmiotów przetwarzających.
2. Administrator udziela ogólnej zgody na korzystanie przez Podmiot przetwarzający z usług innych podmiotów przetwarzających. Podmiot przetwarzający informuje Administratora o zamiarze dodania lub zastąpienia innego podmiotu przetwarzającego co najmniej 14 dni wcześniej, podając nazwę podmiotu i zakres przetwarzania. Administrator może w tym terminie wyrazić sprzeciw.
3. Na inny podmiot przetwarzający Podmiot przetwarzający nakłada te same obowiązki ochrony danych, które wynikają z Umowy. Za niewywiązanie się z nich przez inny podmiot przetwarzający Podmiot przetwarzający odpowiada wobec Administratora jak za własne działanie.

§ 5
Naruszenie ochrony danych osobowych

1. Podmiot przetwarzający zawiadamia Administratora o stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od jego stwierdzenia, na adres e-mail …… oraz telefonicznie pod numerem …….
2. Zawiadomienie zawiera co najmniej informacje, o których mowa w art. 33 ust. 3 RODO, w zakresie, w jakim są znane Podmiotowi przetwarzającemu. Informacje niedostępne w chwili zawiadomienia Podmiot przetwarzający przekazuje niezwłocznie po ich uzyskaniu.

3. Podmiot przetwarzający współpracuje z Administratorem przy wyjaśnianiu naruszenia i ograniczaniu jego skutków oraz nie zawiadamia o nim organu nadzorczego ani osób, których dane dotyczą, bez uzgodnienia z Administratorem, chyba że obowiązek taki wynika z przepisów prawa.

§ 6
Kontrola

1. Administrator ma prawo kontrolować zgodność przetwarzania danych z Umową, w formie pisemnych pytań albo kontroli w siedzibie Podmiotu przetwarzającego, przeprowadzanej przez Administratora lub upoważnionego przez niego audytora zobowiązanego do zachowania poufności.
2. O zamiarze przeprowadzenia kontroli w siedzibie Administrator zawiadamia Podmiot przetwarzający co najmniej 14 dni wcześniej. Kontrola odbywa się w godzinach pracy Podmiotu przetwarzającego, nie częściej niż raz w roku, chyba że jest związana z naruszeniem ochrony danych osobowych.
3. Każda ze Stron ponosi własne koszty kontroli.

§ 7
Odpowiedzialność

1. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem danych niezgodnym z Umową lub z RODO, na zasadach określonych w art. 82 RODO.
2. W stosunkach między Stronami do odpowiedzialności Podmiotu przetwarzającego stosuje się ograniczenia określone w Umowie Głównej, z wyjątkiem szkody wyrządzonej umyślnie.

§ 8
Czas obowiązywania

1. Umowa obowiązuje przez okres obowiązywania Umowy Głównej.
2. Po zakończeniu Umowy Głównej Podmiot przetwarzający, w terminie 14 dni, zależnie od decyzji Administratora usuwa albo zwraca mu wszystkie dane osobowe, które znajdują się w jego posiadaniu, oraz usuwa ich kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazuje ich dalsze przechowywanie, i potwierdza to Administratorowi w postaci elektronicznej.
3. Administrator może wypowiedzieć Umowę Główną ze skutkiem natychmiastowym, jeżeli Podmiot przetwarzający, mimo pisemnego wezwania, przetwarza dane w sposób rażąco niezgodny z Umową.

§ 9
Postanowienia końcowe

1. W sprawach dotyczących ochrony danych osobowych postanowienia Umowy mają pierwszeństwo przed postanowieniami Umowy Głównej.
2. Z tytułu wykonywania Umowy Podmiotowi przetwarzającemu nie przysługuje wynagrodzenie odrębne od określonego w Umowie Głównej.
3. Zmiana Umowy wymaga formy pisemnej albo formy elektronicznej z kwalifikowanymi podpisami elektronicznymi, pod rygorem nieważności.

4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron, albo w postaci elektronicznej opatrzonej kwalifikowanymi podpisami elektronicznymi Stron.

……	……
ADMINISTRATOR	**PODMIOT PRZETWARZAJĄCY**

Załącznik nr 1 do Umowy powierzenia

RODZAJE DANYCH I KATEGORIE OSÓB

Kategoria osób	**Rodzaje danych**	**Moduł**	**Dotyczy**
Pracownicy, współpracownicy i kandydaci do pracy Administratora	imię i nazwisko, stanowisko, komórka organizacyjna, dane kontaktowe, dane dotyczące zatrudnienia i kwalifikacji, szkolenia, upoważnienia i uprawnienia	Kadry, SZBI, KSC, RODO	TAK / NIE
Pracownicy i kandydaci do pracy, wobec których przepisy wymagają informacji o niekaralności	informacja o przedłożeniu zaświadczenia z Krajowego Rejestru Karnego lub oświadczenia o niekaralności, jego data i podstawa prawna wymogu, bez kopii zaświadczenia (dane, o których mowa w art. 10 RODO)	Kadry, KSC	TAK / NIE
Kontrahenci Administratora i ich przedstawiciele	imię i nazwisko, firma, NIP, adres, dane kontaktowe, dane dotyczące zawartych umów	Umowy i CRU	TAK / NIE
Osoby, których dotyczą wnioski, naruszenia i incydenty	dane identyfikacyjne i kontaktowe, opis sprawy; w zależności od treści sprawy także szczególne kategorie danych	RODO, KSC	TAK / NIE
Użytkownicy oprogramowania	imię i nazwisko, adres e-mail, login, rola, zapisy w dzienniku zdarzeń, adres IP	wszystkie	TAK
Inne: ……	……	……	TAK / NIE

Załącznik nr 2 do Umowy powierzenia

ŚRODKI TECHNICZNE I ORGANIZACYJNE

Podmiot przetwarzający stosuje w szczególności następujące środki:

1) dostęp do Środowiska Administratora wyłącznie przez połączenie wskazane przez Administratora i wyłącznie na czas wykonywania prac;
2) uwierzytelnianie wieloskładnikowe do kont służbowych Podmiotu przetwarzającego, w tym do repozytorium kodu i poczty elektronicznej;
3) szyfrowanie dysków komputerów używanych do pracy oraz nośników zawierających kopie danych;
4) hasła przechowywane w menedżerze haseł, unikalne dla każdego systemu;
5) bieżące aktualizacje systemów operacyjnych i oprogramowania na urządzeniach Podmiotu przetwarzającego;
6) rejestr dostępów do Środowiska Administratora;
7) usuwanie kopii danych przekazanych do diagnozy niezwłocznie po zakończeniu prac;
8) podpisywanie pakietów instalacyjnych oprogramowania kluczem przechowywanym bez połączenia z siecią oraz weryfikacja podpisu przed instalacją;
9) skanowanie wydań oprogramowania pod kątem znanych podatności i dołączanie zestawienia komponentów (SBOM);
10) szyfrowanie połączeń z oprogramowaniem (HTTPS), uruchamianie aplikacji bez uprawnień administratora systemu, kontrola dostępu oparta na rolach.