Załączniki do Ogólnych Warunków Umów

Załącznik nr 1 do OWU Umowa Powierzenia Przetwarzania Danych Osobowych

Umowa Powierzenia Przetwarzania Danych Osobowych

zwana dalej: "PPDO"

pomiędzy
Klientem, zwanym dalej "**Powierzającym**"
a

Manago AI, zwanym dalej "**Podmiotem przetwarzającym**"

W związku z tym, że Strony zawarły Umowę, Strony niniejszym postanawiają co następuje:

§ 1 Oświadczenia stron

1. Powierzający oświadcza, że w stosunku do powierzanych danych osobowych jest administratorem albo podmiotem przetwarzającym i posiada prawo do ich przetwarzania oraz powierzenia albo dalszego powierzenia ich przetwarzania, a w przypadku gdy Powierzający jest podmiotem przetwarzającym, Powierzający oświadcza również, że wszystkie wymagania względem administratora danych zostały spełnione.
2. Podmiot przetwarzający zapewnia wdrożenie odpowiednich środków technicznych i organizacyjnych w taki sposób, aby przetwarzanie spełniało wymagania Ustawy oraz RODO i zapewniało ochronę praw osoby, której dane dotyczą.
3. Podmiot przetwarzający oświadcza, że stosuje wszelkie wymagane środki techniczne i organizacyjne, tak by przetwarzanie odbywało się zgodnie z art. 32 RODO.
4. Podmiot przetwarzający niniejszym oświadcza, że posiada zasoby, w tym zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany personel, w zakresie umożliwiającym należyte wykonanie PPDO, w zgodzie z obowiązującymi przepisami prawa. W szczególności Podmiot przetwarzający oświadcza, że znane mu są zasady przetwarzania i zabezpieczenia danych osobowych wynikającego z RODO.

§ 2 Przedmiot PPDO

1. Strony postanawiają, że w celu spełnienia obowiązków wynikających z przepisów prawa, a w szczególności przepisów Rozporządzenia 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) z dnia 27 kwietnia 2016 r. (Dz.Urz.UE.L Nr 119, str. 1) zwanego dalej „RODO", ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz. 1781), zwanej dalej „Ustawą", przepisów innych ustaw krajowych dotyczących ochrony danych osobowych, które mają zastosowanie do Umowy oraz w celu właściwej realizacji postanowień Umowy, Powierzający powierza Podmiotowi przetwarzającemu do przetwarzania dane osobowe w zakresie określonym niniejszą PPDO.
2. Strony wspólnie ustalają, że przetwarzanie danych osobowych odbywa się w imieniu Powierzającego, a Podmiot przetwarzający zapewnia wdrożenie odpowiednich środków technicznych i organizacyjnych w taki sposób, aby przetwarzanie spełniało wymagania Ustawy oraz RODO i zapewniało ochronę praw osoby, której dane dotyczą.

3. Jeżeli w niniejszej PPDO użyto terminów zdefiniowanych w RODO, terminy te mają takie samo znaczenie jak w RODO.

§ 3 Opis i zakres przetwarzania

1. PPDO ma zastosowanie do przetwarzania danych osobowych określonego poniżej:
   a. kategorie osób, których dane osobowe są przetwarzane: użytkownicy stron internetowych Powierzającego, będący klientami lub potencjalnymi klientami Powierzającego
   b. kategorie przetwarzanych danych osobowych: imię i nazwisko, adres e-mail, numer telefonu, Contact ID, numer IP, Informacje o lokalizacji, dane behawioralne online osób, których dane dotyczą
   c. charakter i cel przetwarzania: wykonywanie Umowy, z wykorzystaniem zasobów udostępnionych przez Podmiot przetwarzający.
   d. przedmiot przetwarzania: dane osobowe przechowywane w Systemie w okresie obowiązywania Umowy
2. Strony wspólnie przyjmują, że Powierzający powierza Podmiotowi przetwarzającemu wyłącznie dane osobowe w zakresie i w odniesieniu do kategorii osób określonych w § 3 ust. 1 PPDO. W sytuacji powierzenia szerszego zakresu danych osobowych niż wskazany w § 3 ust. 1 PPDO, Powierzający zobowiązuje się do wskazania innego zakresu danych osobowych na dzień zawarcia Umowy w treści Formularza Zamówienia. W przypadku zmiany zakresu przetwarzanych danych osobowych w trakcie realizacji Umowy, Powierzający jest zobowiązany do wskazania nowego zakresu danych osobowych Podmiotowi przetwarzającemu.
3. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celu i zakresie określonym powyżej na podstawie PPDO, lub w oparciu o udokumentowane polecenia Powierzającego(przekazywane w formie pisemnej lub dokumentowej pod rygorem nieważności), które mają również zastosowanie do przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej (chyba że nałożono taki obowiązek zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlega Podmiot przetwarzający, w tym przypadku Podmiot przetwarzający informuje Powierzającego o tym obowiązku prawnym przed rozpoczęciem przetwarzania, chyba że prawo to zabrania przekazywania takich informacji ze względu na ważny interes publiczny). Udokumentowane polecenia Powierzającego mają na celu doprecyzowanie postanowień PPDO i nie mogą rozszerzać zakresu obowiązków Podmiotu przetwarzającego, wynikających z PPDO.

§ 4 Prawa i obowiązki Stron

1. Powierzający powierza Podmiotowi przetwarzającemu dane osobowe gromadzone wyłącznie zgodnie z prawem i potwierdza, że uzyskał wszystkie wymagane zgody na przetwarzanie danych osobowych oraz wszelkie inne zgody, do uzyskania których zastosowanie mają przepisy o ochronie danych.
2. Na pisemny wniosek Powierzającego, Podmiot przetwarzający jest zobowiązany do dostarczenia informacji dotyczących przetwarzania powierzonych mu danych osobowych, w tym szczegółów technicznych i organizacyjnych wykorzystywanych w celu przetwarzania danych, w zakresie objętym wnioskiem Powierzającego, w ciągu 14 dni od otrzymania wniosku zawierającego żądanie udostępnienia takich danych. Przed przesłaniem wniosku, o którym mowa powyżej, Powierzający musi dołożyć starań, aby we własnym zakresie uzyskać wszelkie niezbędne informacje związane z przetwarzaniem danych osobowych, np. korzystając z dokumentów i korespondencji pomiędzy stronami przy negocjowaniu i wykonywaniu PPDO.
3. Podmiot przetwarzający informuje Powierzającego przed rozpoczęciem przetwarzania danych o realizacji ewentualnego obowiązku prawnego polegającego na przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, zgodnie z art. 28 ust. 3 lit. a RODO.
4. Podmiot przetwarzający zapewnia, że osoby uprawnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności lub są objęte odpowiednim ustawowym obowiązkiem zachowania poufności, zgodnie z art. 28 ust. 3 lit. b RODO.

5. Podmiot przetwarzający zobowiązuje się zapewnić, by każda osoba fizyczna działająca z upoważnienia Podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie Powierzającego w celach i zakresie przewidzianym w PPDO.
6. Podmiot przetwarzający oświadcza, że podjął środki ochronne wymagane na podstawie art. 32 RODO, zgodnie z art. 28 ust. 3 lit. c RODO. Zapewnienie bezpieczeństwa danych obejmuje ochronę danych przed naruszeniem bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych (naruszenie ochrony danych osobowych). Oceniając odpowiedni poziom bezpieczeństwa, Strony należycie uwzględniają stan wiedzy technicznej, koszty wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz związane z tym ryzyko dla osób, których dane dotyczą.
7. Podmiot przetwarzający oświadcza, że przestrzega warunków, o których mowa w art. 28 ust. 2 i 4 RODO, dotyczących zaangażowania innego podmiotu przetwarzającego dane osobowe, zgodnie z art. 28 ust. 3 lit. d RODO. Powierzający udziela Podmiotowi przetwarzającemu ogólnego upoważnienia do dalszego powierzenia danych osobowych. Podmiot przetwarzający publikuje na swojej stronie internetowej aktualną listę zarówno istniejących, jak i planowanych dalszych podmiotów przetwarzających. Powierzający jest zobowiązany do okresowego przeglądania tej listy, a w przypadku sprzeciwu wobec zaangażowania określonego dalszego podmiotu przetwarzającego, Powierzający może skorzystać ze swojego prawa do sprzeciwu wobec takiego dalszego przetwarzania. Prawo do sprzeciwu może być wykonane wyłącznie przed planowanym dalszym przetwarzaniem danych osobowych.
8. Pełna lista podmiotów przetwarzających jest dostępna tutaj.
9. Podmiot przetwarzający jest w pełni odpowiedzialny przed Powierzającym za spełnienie obowiązków wynikających z umowy powierzenia zawartej pomiędzy Podmiotem przetwarzającym a dalszym podmiotem przetwarzającym. Jeżeli dalszy podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Powierzającego za wypełnienie obowiązków tego dalszego podmiotu przetwarzającego spoczywa na Podmiocie przetwarzającym.
10. Podmiot przetwarzający bierze pod uwagę charakter przetwarzania, pomaga Powierzającemu poprzez odpowiednie środki techniczne i organizacyjne, o ile jest to możliwe, w celu wypełnienia obowiązku Powierzającego w zakresie reagowania na żądania wykonywania praw osób, których dane dotyczą, określonych w rozdziale III RODO, zgodnie z art. 28 ust. 3 lit. e RODO. Podmiot przetwarzający nie jest uprawniony ani zobowiązany do bezpośredniego odpowiadania na żądania osób, których dane dotyczą. Podmiot przetwarzający może poinformować osobę, której dane dotyczą, że jej żądanie zostało przekazane Powierzającemu. Podmiot przetwarzający może ograniczyć przetwarzanie danych osobowych osoby, której dane dotyczą, na czas udzielania odpowiedzi przez Powierzającego na żądanie osoby, której dane dotyczą, w szczególności gdy żądanie dotyczy sprzeciwu wobec przetwarzania danych osobowych do celów marketingu bezpośredniego.
11. Podmiot przetwarzający uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Powierzającemu wywiązać się z obowiązków określonych w art. 32–36 RODO, zgodnie z art. 28 ust. 3 lit. f RODO. W szczególności:
    11.1. **[Naruszenie ochrony danych dotyczące danych przetwarzanych przez Powierzającego]** W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez Powierzającego, Podmiot przetwarzający wspomaga Powierzającego:
        11.1.1. przy zgłaszaniu naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu niezwłocznie po tym, jak Powierzający dowiedział się o naruszeniu;
        11.1.2. przy uzyskiwaniu następujących informacji, które zgodnie z art. 33 ust. 3 RODO powinny być zawarte w zgłoszeniu Powierzającego i obejmować:
            11.1.2.1. charakter danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

11.1.2.2. możliwe konsekwencje naruszenia ochrony danych osobowych;
11.1.2.3. środki zastosowane lub proponowane przez Powierzającego w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki;

11.1.3. przy wypełnianiu, zgodnie z art. 34 RODO, obowiązku zawiadomienia bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

11.2. **[Naruszenie ochrony danych dotyczące danych przetwarzanych przez podmiot przetwarzający]** W przypadku naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych przez Podmiot przetwarzający, Podmiot przetwarzający zgłasza naruszenie Powierzającemu niezwłocznie, lecz nie później niż w ciągu 24 godzin po tym, jak dowiedział się o naruszeniu. Zgłoszenie to powinno zawierać:

11.2.1. opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie);
11.2.2. dane punktu kontaktowego, w którym można uzyskać więcej informacji na temat naruszenia ochrony danych osobowych;
11.2.3. wskazanie prawdopodobnych konsekwencji naruszenia oraz środków, które zostały lub mają zostać wprowadzone w celu zaradzenia naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, pierwotne zgłoszenie zawiera informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.

12. Podmiot przetwarzający udostępnia Powierzającemu wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w artykule 28 RODO oraz umożliwia Powierzającemu lub audytorowi upoważnionemu przez Powierzającego przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich, zgodnie z art. 28 ust. 3 lit. h RODO i na warunkach określonych w §5 poniżej.
13. Jeżeli wymagają tego względy bezpieczeństwa danych osobowych, na czas trwania dochodzenia lub do czasu wyeliminowania przyczyn naruszenia, Podmiot przetwarzający może ograniczyć przetwarzanie danych osobowych, których bezpieczeństwo jest lub potencjalnie może być naruszone (np. tymczasowo wyłączając określoną usługę lub blokując wysyłanie korespondencji do określonych kontaktów).
14. Podmiot przetwarzający niezwłocznie informuje Powierzającego, jeżeli jego zdaniem instrukcja wydana mu przez Powierzającego narusza RODO lub inne przepisy Unii lub państwa członkowskiego w zakresie ochrony danych.

§5 Audyty

1. Powierzający jest uprawniony do przeprowadzenia, nie częściej niż raz w ciągu każdego kolejnego roku kalendarzowego, audytu bezpieczeństwa przetwarzania danych osobowych, w zakresie zgodności ich przetwarzania z treścią PPDO oraz obowiązujących przepisów prawa, w szczególności RODO.
2. Podstawową formą przeprowadzania audytu jest audyt prowadzony drogą elektroniczną. Polega on na przesłaniu przez Powierzającego do Podmiotu przetwarzającego pytań dotyczących zgodności przetwarzania przez Podmiot przetwarzający powierzonych danych osobowych z PPDO, RODO lub powszechnie obowiązującymi przepisami z zakresu ochrony danych osobowych, w tym stosowanych

środków bezpieczeństwa. Podmiot przetwarzający jest zobowiązany do udzielenia odpowiedzi na pytania Powierzającego, w miarę możliwości w terminie 30 dni od ich otrzymania.

3. Po przeprowadzeniu audytu, o którym mowa w ust. 2, Powierzający, w razie potrzeby, jest uprawniony do przeprowadzenia audytu w innej formie. Po otrzymaniu żądania przeprowadzenia takiego audytu, Strony ustalą datę jego rozpoczęcia (która nie może nastąpić wcześniej niż na 10 dni roboczych od otrzymania żądania Powierzającego), jego dokładny zakres, sposób realizacji i osoby upoważnione do jego przeprowadzenia.
4. Audyty będą przeprowadzane w godzinach pracy przedsiębiorstwa Podmiotu przetwarzającego, w zakresie i na obszarze niezbędnym dla przetwarzania danych osobowych bez uszczerbku dla normalnego prowadzenia działalności przez Podmiot przetwarzający, tajemnicy przedsiębiorstwa Podmiotu przetwarzającego oraz informacji poufnych należących do osób trzecich. Powierzający zobowiązuje się do zachowania ww. informacji w tajemnicy. Przed przystąpieniem do czynności audytowych, Strony (lub odpowiednio zewnętrzny audytor wyznaczony przez Powierzającego) podpiszą stosowną umowę o zachowaniu poufności.
5. Koszty przeprowadzenia audytu ponosi Powierzający.

§6 Transfer danych poza Europejski Obszar Gospodarczy

1. **Podmiot przetwarzający nie przekazuje danych osobowych powierzonych przez Powierzającego poza Europejski Obszar Gospodarczy.**
2. W sytuacji, gdy Powierzający przetwarza dane osobowe lub posiada siedzibę poza Europejskim Obszarem Gospodarczym (dalej: EOG) i w związku z tym konieczny jest transfer danych osobowych, o którym mowa w §6ust. 1 PPDO, zastosowanie mają standardowe klauzule umowne, o których mowa w Decyzji Wykonawczej Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, o następującej treści:
   a. gdy dane osobowe przekazywane są poza EOG do Powierzającego, który w stosunku do tych danych jest podmiotem przetwarzającym - link,
   b. gdy dane osobowe przekazywane są poza EOG do Powierzającego, który jest administratorem tych danych - link.
3. Zmiana załącznika “Wykaz podwykonawców przetwarzania” nie stanowi zmiany niniejszej Umowy.
4. W przypadku konieczności zawarcia standardowych klauzul umownych, o których mowa w § 6 ust. 2 PPDO w formie pisemnej, Powierzający zobowiązany jest przekazać żądanie ich zawarcia w tej formie Podmiotowi przetwarzającemu na adres: dpo@manago.ai.
5. Standardowe klauzule umowne, o których mowa w § ust. 2 PPDO mają zastosowanie wyłącznie w przypadku braku decyzji, o której mowa w art. 45 ust. 3 RODO.

§ 7 Odpowiedzialność

1. Każda ze Stron odpowiada za szkody wyrządzone drugiej Stronie oraz osobom trzecim w związku z wykonywaniem niniejszej PPDO, zgodnie z przepisami Kodeksu cywilnego, RODO, Ustawy oraz niniejszej PPDO.
2. Podmiot przetwarzający nie ponosi odpowiedzialności za przekazane przez Powierzającego dane osobowe w zakresie wykraczającym poza zakres określony w §3 ust. 1 PPDO, chyba że nowy zakres danych został wskazany przez Powierzającego w Formularzu Zamówienia. W celu uniknięcia wątpliwości, Podmiot przetwarzający odpowiada za dane osobowe określone w Formularzu Zamówienia w takim samym zakresie jak za dane określone w §3 ust. 1 PPDO
3. W przypadku szkody spowodowanej działaniem Podmiotu przetwarzającego, Podmiot przetwarzający odpowiadać będzie na zasadzie winy za szkody rzeczywiste poniesione przez Powierzającego, przy czym całkowita odpowiedzialność Podmiotu przetwarzającego wobec Powierzającego na podstawie lub w związku z Umową ograniczona jest jednocześnie do kwoty uiszczonego przez Powierzającego wynagrodzenia należnego Podmiotowi przetwarzającemu na podstawie Umowy w okresie roku przed datą wystąpienia zdarzenia powodującego szkodę. Podmioty przetwarzający nie będzie również ponosił odpowiedzialności za utracone korzyści oraz jakiekolwiek

szkody pośrednie. Powyższe wyłączenie odpowiedzialności za określone szkody oraz ograniczenie odpowiedzialności mają zastosowanie w maksymalnym zakresie dozwolonym przez obowiązujące prawo.

4. Podmiot przetwarzający jest wyłączony z odpowiedzialności za:
    1. prawidłowe zabezpieczenie danych osobowych zgodnie z Umową w tej części Systemu, która jest zarządzana przez Powierzającego (np. w przypadku niewłaściwego zabezpieczenia konta użytkownika poprzez przypisanie zbyt słabego hasła przez Powierzającego lub ujawnienie tego hasła przez Powierzającego);
    2. przetwarzanie danych osobowych bez wymaganych zgód, które Powierzający powinien był uzyskać, a także z odpowiedzialności za przetwarzanie danych osobowych na podstawie wadliwie uzyskanych zgód;
    3. przetwarzanie danych osobowych z naruszeniem Umowy lub obowiązujących przepisów, jeżeli takie przetwarzanie wynika z niewłaściwej integracji Systemu przez Powierzającego;
    4. niespełnienie szczególnych wymagań wynikających z przepisów sektorowych, którym podlega Powierzający (np. Dyrektywa NIS2, DORA), chyba że Powierzający poinformował Podmiot przetwarzający o tych wymaganiach przed zawarciem Umowy lub w ciągu 14 dni od wejścia w życie tych wymagań, a Podmiot przetwarzający oświadczył, że spełni te wymagania w zakresie, w jakim dotyczą Podmiotu przetwarzającego.

§8 Przedstawiciele Stron

Dla potrzeb realizacji niniejszej PPDO, Powierzający i Podmiot przetwarzający wyznaczają osobę uprawnioną do kontaktów:

a. Powierzający: osoba kontaktowa wskazana w Formularzu Zamówienia
b. Podmiot przetwarzający: dpo@manago.ai
    - wskazana osoba może być w każdej chwili zmieniona poprzez zawiadomienie drugiej Strony drogą elektroniczną. Zmiana taka nie stanowi zmiany PPDO.

§9 Postanowienia końcowe

1. Podmiot przetwarzający nie pobiera dodatkowych opłat z tytułu realizacji postanowień niniejszej PPDO.
2. Bez uszczerbku dla pozostałych postanowień PPDO, PPDO pozostaje w mocy przez cały okres przetwarzania Danych Osobowych powierzonych przez Powierzającego, niezależnie od rozwiązania lub wygaśnięcia Umowy.
3. W przypadku rozwiązania Umowy, Powierzający indywidualnie, w terminie 7 dni od daty wygaśnięcia niniejszej PPDO, zabezpieczy wszelkie dane osobowe powierzone Podmiotowi przetwarzającemu do przetwarzania. W terminie 14 dni po dacie wygaśnięcia PPDO, Podmiot przetwarzający trwale usunie wszelkie zapisy zawierające dane osobowe powierzone mu do przetwarzania, przekazane mu w związku lub podczas wykonywania Umowy, z wyjątkiem Danych Osobowych przetwarzanych w ramach kopii zapasowych. Kopie zapasowe będą tworzone w szczególności w celu zabezpieczenia danych i zapewnienia ich dostępności podczas realizacji Umowy Głównej. Kopie zapasowe będą przechowywane maksymalnie przez okres 12 miesięcy od ich utworzenia i automatycznie usuwane po tym okresie. Dane osobowe przechowywane w kopiach zapasowych są „wyłączone z przetwarzania", co oznacza, że ich przetwarzanie jest ograniczone do przechowywania wyłącznie w formie zaszyfrowanej, z wyjątkiem sytuacji, gdy konieczne stanie się wykorzystanie kopii zapasowej w związku z realizacją Umowy, zgodnie z celem kopii zapasowej, na przykład w wyniku awarii systemu, w którym dane są przetwarzane podczas realizacji Umowy. Dostęp do takich danych będą miały wyłącznie osoby upoważnione działające w imieniu Podmiotu przetwarzającego. W odniesieniu do kopii zapasowych, niniejsza Umowa ulega rozwiązaniu po upływie okresu przechowywania kopii zapasowych, o którym mowa powyżej.
4. Strony oświadczają, że wszelkie wcześniej zawarte umowy dotyczące przetwarzania danych osobowych zostają uchylone i zastąpione niniejszą PPDO.

5. Wszelkie kwestie nieobjęte zakresem niniejszej Umowy podlegają przepisom prawa właściwego, w tym w szczególności przepisom Ustawy i RODO.

Załącznik nr 2 do OWU Informacja o przetwarzaniu danych osobowych dla Klienta, osoby reprezentującej Klienta, Użytkownika oraz osoby kontaktowej po stronie Klienta

Administrator danych osobowych: Administratorem danych osobowych jest Benhauer sp. z o.o. z siedzibą w Krakowie przy ul. Stanisława Klimeckiego 4, zarejestrowana w rejestrze przedsiębiorców KRS prowadzonym przez XI Wydział Gospodarczy Krajowego Rejestru Sądowego Sądu Rejonowego dla Krakowa – Śródmieścia w Krakowie pod numerem 0000523346, REGON 122334666, NIP 6762447754 (dalej: Benhauer lub Administrator).

Cele i podstawy przetwarzania danych: Dane osobowe kontrahentów, którzy są osobami fizycznymi będą przetwarzane:

- w celu realizacji umowy zawartej pomiędzy kontrahentem, a Administratorem lub w celu podjęcia działań na żądanie kontrahenta przed zawarciem umowy (art. 6 ust. 1 lit. b RODO),
- w celu wypełnienia obowiązków nałożonych na Administratora na podstawie obowiązujących przepisów prawa, w szczególności w zakresie wystawiania i przechowywania faktur VAT, wynikających z przepisów podatkowych i o rachunkowości,
- w celu ewentualnego ustalenia, dochodzenia jak i obrony roszczeń, co stanowi uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO).

Cele i podstawy przetwarzania danych: dane przedstawicieli kontrahentów, osób wykonujących umowę i osób wyznaczonych do kontaktu będą przetwarzane:

- dla celów kontaktowych, w tym w celu nawiązania i prowadzenia kontaktów biznesowych, co stanowi uzasadniony interes Administratora (art. 6 ust. 1 lit. f RODO),
- dla celów wypełnienia obowiązków nałożonych na Administratora na podstawie obowiązujących przepisów prawa (art. 6 ust. 1 lit. c RODO),
- w celu ewentualnego dochodzenia jak i obrony roszczeń, co stanowi uzasadniony interes Administratora (6 ust. 1 lit. f RODO).

Odbiorcy danych: Dane osobowe mogą być udostępniane podmiotom upoważnionym na podstawie przepisów prawa. Dostęp do danych na podstawie stosownych umów mogą posiadać także podmioty wspierające Administratora m.in. w zakresie usług IT.

Okres przechowywania: Dane osobowe kontrahentów będą przechowywane przez okres wymagany na podstawie obowiązujących przepisów prawa lub przez okres przedawnienia ewentualnych roszczeń w zależności, które z tych zdarzeń nastąpi później. Dane przetwarzane w celach kontaktowych będą przechowane przez okres trwania relacji biznesowych.

Dobrowolność/obowiązek podania danych: Podanie danych osobowych jest dobrowolne, jednakże niezbędne do zawarcia lub realizacji umowy łączącej strony.

Przekazanie danych do Państwa trzeciego: Dane osobowe będą przetwarzane również z użyciem narzędzi/systemów dostarczanych przez podmioty wspierające Administratora, które mają siedzibę lub przetwarzają dane poza Europejskim Obszarem Gospodarczym. W takim wypadku, dane osobowe są przekazywane na podstawie standardowych klauzul umownych zatwierdzonych przez Komisję Europejską lub decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony w danym kraju, np. na podstawie Ram ochrony danych UE-USA.

Zautomatyzowane podejmowanie decyzji / profilowanie: Administrator nie podejmuje decyzji opierających się na zautomatyzowanym przetwarzaniu, w tym profilowaniu (w odniesieniu do wyżej opisanych celów przetwarzania danych).

Prawa osób, których dane dotyczą: Posiadają Państwo stosownie do sytuacji prawo do:

- żądania dostępu do swoich danych osobowych, ich sprostowania, usunięcia oraz ograniczenia przetwarzania, a jeżeli dane osobowe są przetwarzane w sposób zautomatyzowany na podstawie umowy, posiadają Państwo również prawo do przenoszenia swoich danych osobowych;
- wycofania udzielonej zgody w dowolnym momencie, o ile dane przetwarzane były na podstawie tej zgody. Wycofanie zgody, nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem;
- wniesienia sprzeciwu wobec przetwarzania danych osobowych – gdy dane przetwarzane są na podstawie uzasadnionego interesu Administratora;
- wniesienia skargi do organu nadzorczego (PUODO – Prezes Urzędu Ochrony Danych Osobowych ul. Stawki 2, 00-193 Warszawa, email: kancelaria@uodo.gov.pl

Administrator danych osobowych:
Benhauer sp. z o.o. z siedzibą w Krakowie
ul. Stanisława Klimeckiego 4
30-705 Kraków
e-mail: rodo@manago.ai

Inspektor ochrony danych:
e-mail: dpo@manago.ai

Załącznik nr 3 do OWU Warunki dla Usług Wdrożeniowych

Niniejsze Warunki dla Usług Wdrożeniowych („Warunki") regulują nabywanie przez Klienta Usług Wdrożeniowych Manago AI. Terminy pisane wielką literą mają definicje określone w OWU, chyba że poniżej wyraźnie określono inaczej.

§ 1 Przedmiot Warunków

1. Manago AI zobowiązuje się świadczyć na rzecz Klienta Usługi Wdrożeniowe zgodnie z pakietem wdrożeniowym wybranym przez Klienta, wskazanym w Formularzu Zamówienia. Zakres Usług Wdrożeniowych wynika z pakietu licencji wybranego przez Klienta, chyba że Strony uzgodnią inaczej
2. *usunięto*
3. OWU ma zastosowanie do niniejszych Warunków w zakresie nieuregulowanym w niniejszych Warunkach, chyba że wyraźnie wskazano inaczej.
4. W przypadku jakichkolwiek rozbieżności między postanowieniami OWU a niniejszymi Warunkami, pierwszeństwo mają niniejsze Warunki.
5. Usługi wdrożeniowe rozliczane są w oparciu o Jednostki Usługowe (SU), których liczba podana jest w Formularzu Zamówienia.

§ 2 Zakres i cele projektu

1. Niezależnie od odmiennych postanowień, Strony przyjmują do wiadomości i uzgadniają, że Usługi Wdrożeniowe świadczone na podstawie niniejszych Warunków ograniczają się do wymienionych niżej elementów. Manago Ali Klient wspólnie uzgadniają, że nie będą dokonywane żadne dostosowania standardowych cech i funkcjonalności Systemu.
2. Manago AI i Klient będą współpracować, aby osiągnąć uzgodnione poniżej cele, zgodnie z wybranym pakietem Usług Wdrożeniowych. W zależności od pakietu licencji wybranego przez Klienta, Usługi Wdrożeniowe będą obejmować podstawowe przypadki użycia opisane tutaj[1].

[1] https://manago.ai/use-cases

3. Za obopólną zgodą Stron Klient może wykorzystać zakupione Jednostki Usługowe do realizacji częściowo zamiast podstawowych przypadków użycia, innych przypadków użycia wskazanych w tabelach powyżej.
4. Koszty poszczególnych działań Usług Wdrożeniowych wyrażone w SU oraz zakres wdrożenia opisano poniżej. W przypadku niestandardowych lub złożonych wdrożeń liczba wymaganych Jednostek Usługowych może różnić się od szacunków podanych tutaj.

§ 3 Założenia i uwarunkowania projektu

1. Strony przyjmują, że wybrane Usługi Wdrożeniowe zostaną zrealizowane w terminie wskazanym w Formularzu Zamówienia, począwszy od daty rozpoczęcia obowiązywania Umowy zgodnie z Formularzem Zamówienia. Jeżeli świadczone Usługi Wdrożeniowe (lub jakakolwiek ich część) nie zostaną ukończone na koniec ww. okresu z powodu nieudostępnienia Manago AI przez Klienta niezbędnych zasobów (np. danych, które powinny zostać zaimportowane do Systemu) lub nieterminowego wykonania innych zobowiązań Klienta (np. niedostępności osób kontaktowych, niewdrożenia integracji Systemu), takie Usługi Wdrożeniowe zostaną uznane za ukończone i kompletne na koniec ww. okresu.
2. Wszystkie usługi będą świadczone zdalnie. Podróż i związane z nią wydatki nie są wymagane przez Klienta i nie są uwzględnione w stałej opłacie. Żadne inne opłaty i/lub wydatki nie są dopuszczalne bez uprzedniej pisemnej zgody Klienta i Manago AI.
3. Manago AI może zdecydować o zmianie personelu przypisanego do Usług Wdrożeniowych w dowolnym momencie z dowolnego powodu.
4. Klient zapewni:
    a. odpowiednio wykwalifikowany personel, posiadający wiedzę na temat istniejącego środowiska Klienta w celu wsparcia działań Manago AI w zakresie Usług Wdrożeniowych. Personel ten będzie dostępny bez zbędnej zwłoki w celu wyjaśnienia wymagań biznesowych i walidacji wyników, w razie potrzeby;
    b. bieżący dostęp do oprogramowania wymaganego do prowadzenia prac (np. wtyczek, jeśli dotyczy);
    c. szybkie i sprawne rozwiązywanie kwestii biznesowych lub technicznych wynikających z podjętych działań
    d. że wszelkie dane przesyłane do Manago AI będą chronione hasłem, a rozmiar żadnego przesyłanego pliku nie przekroczy 20 MB;
    e. integrację strony internetowej, plik produktowy (lub kanał produktowy), baza danych, projekt graficzny i materiały, treść, wytyczne strategiczne.
5. Klient zobowiązuje się do wykonania pełnej integracji Systemu (kod monitorujący, przesyłanie zdarzeń transakcyjnych, monitorowanie zgłoszeń i kontaktów, zarządzanie zgodami i subskrypcjami kontaktów, konfiguracja XML lub API produktu).
6. Klient zobowiązuje się do poinformowania o ewentualnej zmianie osób, o których mowa w pkt 5a, z odpowiednim wyprzedzeniem.
7. Usługi Wdrożeniowe są ograniczone wyłącznie do usług związanych z Systemem. Manago AI nie będzie dostarczać treści i nie będzie konfigurować platform zewnętrznych.

§ 4 Opłaty i płatności

1. Klient zostanie obciążony stałą opłatą za Usługi Wdrożeniowe zgodnie z cennikiem opisanym w Formularzu Zamówienia.
2. Warunki płatności za Usługi opisane są w Formularzu Zamówienia. Faktura za Usługi Wdrożeniowe zostanie wystawiona w dniu rozpoczęcia obowiązywania Umowy, zgodnie z Formularzem Zamówienia (płatność z góry).
3. Niedokonanie płatności w terminie może skutkować wszczęciem postępowania windykacyjnego, naliczeniem odsetek za opóźnienie lub wstrzymaniem świadczenia Usług Wdrożeniowych.

4. Nieznane okoliczności mogą spowodować, że rzeczywiste koszty i nakłady pracy będą różnić się od opłat i terminów określonych w niniejszych Warunkach i Formularzu Zamówienia. Wszelkie usługi wykraczające poza opisane powyżej będą podlegać odrębnej wycenie.
5. Zamówienia Usług Wdrożeniowych nie można anulować, a opłaty za Usługi Wdrożeniowe nie podlegają zwrotowi.

§ 5 Odpowiedzialność

1. W żadnym wypadku łączna odpowiedzialność Manago AI wynikająca lub związana z Usługami Wdrożeniowymi nie przekroczy łącznej kwoty zapłaconej przez Klienta za Usługi Wdrożeniowe. W żadnym wypadku Manago AI nie będzie ponosić odpowiedzialności wynikającej lub związanej z Usługami Wdrożeniowymi za utracone korzyści oraz jakiekolwiek szkody pośrednie. Powyższe wyłączenie odpowiedzialności za określone szkody oraz ograniczenie odpowiedzialności mają zastosowanie w maksymalnym zakresie dozwolonym przez obowiązujące prawo.
2. Wszelkie ograniczenia lub modyfikacje, do których Manago AI jest uprawnione na mocy niniejszych Warunków, nie wpływają na ocenę należytego wykonania przez Manago AI niniejszych Warunków i nie wpływają na wynagrodzenie należne Manago AI na mocy niniejszych Warunków.
3. Usługi świadczone na mocy niniejszych Warunków stanowią odrębne zobowiązanie od pozostałych postanowień Umowy. W związku z tym, wykonanie przez Manago AI niniejszych Warunków nie wpływa na: (i) ocenę należytego wykonania przez Manago AI pozostałych zobowiązań Umowy, ani nie wpływa na ważność Umowy ani nie stanowi jej naruszenia w jakimkolwiek innym aspekcie; (ii) wynagrodzenie należne Manago AI na mocy pozostałej części Umowy.

§ 6 Pozostałe postanowienia

1. Warunki mają zastosowanie wyłącznie do usług w nich wskazanych i nie regulują wsparcia Klienta po zakończeniu ich świadczenia przez Manago AI w rozumieniu niniejszych Warunków.
2. Zakończenie świadczenia usług na podstawie niniejszych Warunków nie wpływa na ważność i zakres umowy dotyczącej korzystania z Systemu.

Załącznik nr 4 do OWU
Informacja o jurysdykcji

Informacja o jurysdykcji

Zgodnie z art. 28 ust. 1 lit. a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych), infrastruktura ICT używana do przetwarzania danych w ramach poszczególnych usług Manago AI, podlega jurysdykcji sądów powszechnych w Rzeczypospolitej Polskiej. W zakresie, w jakim infrastruktura ICT używana do przetwarzania danych w ramach poszczególnych usług Manago AI wykonywana jest przez Google Cloud Poland sp. z o.o., podlega ona jurysdykcji sądu arbitrażowego London Court of International Arbitration z siedzibą w Londynie (Wielka Brytania) z wyłączeniem wszelkich niezbędnych sądowych środków tymczasowych, w tym w szczególności pilnych środków tymczasowych oraz zabezpieczenia roszczeń, mających na celu ochronę praw i interesów strony, które podlegają ogólnym zasadom jurysdykcji.

Załącznik nr 5 do OWU
Szczegółowa specyfikacja wszystkich kategorii danych i aktywów cyfrowych, które można przenieść w trakcie procesu zmiany dostawcy, w tym co najmniej wszystkich danych eksportowalnych.

Manago AI zapewnia kompleksową możliwość eksportu danych osobowych i nieosobowych klientów, obejmujących następujące kategorie: dane użytkowników końcowych, marketingowe, operacyjne oraz analityczne. Dane te są przechowywane w infrastrukturze DC Play oraz Google Cloud Platform (GCP). Firma udostępnia szeroki wybór standardowych formatów eksportowych: CSV (domyślny format eksportu z poziomu interfejsu użytkownika), JSON (domyślny format API) oraz XLSX (alternatywny format eksportowy dostępny z poziomu interfejsu aplikacji).

Dane osobowe są przetwarzane zgodnie z umową powierzenia przetwarzania danych osobowych. Są to m.in. imię i nazwisko, e-mail, telefon, Contact ID, adres IP, lokalizacja, dane behawioralne online, które można zakwalifikować jako: podstawowe dane kontaktowe, dane lokalizacyjne, preferencje zakupowe, dane behawioralne.

Eksportowalne są także aktywa cyfrowe, takie jak raporty standardowe i niestandardowe, skrypty integracyjne używane do automatyzacji procesów marketingowych oraz integracji z systemami zewnętrznymi (np. CRM, ERP, e-commerce), jak również pliki konfiguracyjne dotyczące segmentacji klientów, kampanii i automatyzacji.

Dodatkowo, Manago AI oferuje możliwość eksportu danych i zasobów o zakresie wykraczającym poza standardowy, dostępny z poziomu aplikacji. Takie rozszerzone lub niestandardowe eksporty realizowane są na podstawie indywidualnej wyceny, dostosowanej do specyficznych wymagań klienta i zakresu danych.

Kategoria danych / aktywów	Lokalizacja	Format eksportowy	Metoda eksportu	Komentarz
Dane kontaktowe klientów	DC Play	CSV, JSON, XLSX	UI/API	Dane personalne i kontaktowe klientów.
Dane kampanii marketingowych	DC Play	CSV, JSON	UI/API	Szczegóły kampanii, segmenty odbiorców.
Raporty analityczne	DC Play	CSV, JSON, XLSX	UI/API	Raporty standardowe i customowe.
Skrypty integracyjne	DC Play/GCP	JSON, kod źródłowy	UI/Repozytorium klienta	Integracje zewnętrzne (CRM, ERP, itp.)
Pliki konfiguracyjne (segmenty, automatyzacje, kampanie)	DC Play/GCP	JSON/CSV	UI/API	Definicje segmentów, automatyzacji oraz kampanii.

Załącznik nr 6 do OWU
Szczegółowa specyfikacja kategorii danych specyficznych dla wewnętrznego funkcjonowania dostawcy usługi przetwarzania danych, które są wyłączone spośród danych eksportowalnych przewidzianych w Załączniku nr 5, w przypadku gdy istnieje ryzyko naruszenia tajemnic przedsiębiorstwa dostawcy, o ile wyłączenia te nie utrudniają ani nie opóźniają procesu zmiany dostawcy.

Manago AI, jako dostawca kompleksowej platformy Marketing Automation i Customer Data Platform (CDP), rozumie kluczowe znaczenie zapewnienia naszym klientom pełnej kontroli nad ich danymi oraz swobodnego wyboru dostawcy usług. Zgodnie z wymogami Data Act, dokładamy wszelkich starań, aby proces eksportu danych był transparentny, efektywny i niezakłócony. Jednocześnie, w trosce o ochronę naszych innowacji i przewagi konkurencyjnej, niezbędne jest precyzyjne określenie tych kategorii danych, które, stanowiąc wyłączną własność intelektualną i tajemnicę przedsiębiorstwa Manago AI są wyłączone z mechanizmu eksportu. Poniżej przedstawiamy szczegółową specyfikację tych kategorii, gwarantując jednocześnie, że ich wyłączenie w żaden sposób nie utrudni ani nie opóźni procesu zmiany dostawcy przez naszych klientów, a wszystkie dane niezbędne do kontynuowania ich działalności pozostaną w pełni eksportowalne.

Szczegółową specyfikację kategorii danych specyficznych dla wewnętrznego funkcjonowania dostawcy usługi przetwarzania danych, które są wyłączone spośród danych eksportowanych przewidzianych w pkt 1 powyżej, przedstawia poniższa tabela:

Phone
+48 533 600 808

Email
support@manago.ai

Address
Stanisława Klimeckiego 4, 30-705
Cracow

Kategoria danych / aktywów	Przykład danych / aktywów	Uzasadnienie
Dane dotyczące wewnętrznej architektury systemu i infrastruktury	Szczegółowe schematy baz danych, diagramy sieciowe, konfiguracje serwerów, algorytmy routingu danych, specyfikacje sprzętowe i programowe wykorzystywane wewnętrznie do świadczenia usługi, w tym kod aplikacji.	Ujawnienie tych informacji mogłoby dać konkurencji rynkowej i Manago AI dostęp do kluczowego know-how dotyczącego optymalizacji, skalowalności i bezpieczeństwa platformy, stanowiąc przewagę konkurencyjną. Dodatkowo, mogłoby to również stworzyć potencjalne luki bezpieczeństwa.
Unikalne algorytmy i modele danych (w tym autorskie implementacje istniejących)	Wszelkie algorytmy AI/ML, modele predykcyjne, algorytmy kompresji danych, algorytmy przesyłu danych, algorytmy optymalizacji zasobów (np. alokacji maszyn wirtualnych), które zostały stworzone i są własnością intelektualną dostawcy. Dotyczy to również schematów baz danych zaprojektowanych wewnętrznie do przechowywania i przetwarzania danych w unikalny, zoptymalizowany sposób.	Algorytmy i modele danych opracowane przez Manago AI wynikają z lat badań i rozwoju, które stanowią o przewadze technologicznej i efektywności usług. Ujawnienie tych informacji mogłoby pozwolić konkurencji rynkowej Manago AI na kopiowanie tych rozwiązań bez ponoszenia kosztów ich opracowania.
Wewnętrzne narzędzia monitorowania i zarządzania wydajnością	Specyficzne narzędzia i metodologie wykorzystywane do wewnętrznego monitorowania wydajności Waszych systemów, wykrywania anomalii, zarządzania obciążeniem, rozwiązywania problemów i optymalizacji zasobów.	Narzędzia te są integralną częścią zdolności organizacji do utrzymania wysokiej dostępności i wydajności usług. Ich specyfika i sposób działania stanowią cenną wiedzę operacyjną.
Dane dotyczące wewnętrznych procesów operacyjnych i bezpieczeństwa	Szczegółowe procedury reagowania na incydenty, wewnętrzne audyty bezpieczeństwa, specyficzne protokoły uwierzytelniania i autoryzacji stosowane wewnętrznie, plany ciągłości działania i odtwarzania po awarii (o ile nie dotyczą bezpośrednio danych klienta).	Dane w tej kategorii kategoryzowane są jako krytyczne dla utrzymania bezpieczeństwa i niezawodności świadczonych usług. Ujawnienie tych informacji mogłoby stworzyć luki bezpieczeństwa lub umożliwić działania sabotażowe.

Załącznik nr 7 do OWU
Informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych.

Manago AI umożliwia swobodną migrację danych klientów do innych dostawców usług poprzez proste i efektywne mechanizmy eksportu. Użytkownicy mają dostęp do eksportu danych i zasobów zarówno przez interfejs aplikacji (UI), jak i przez API, w popularnych formatach takich jak CSV, JSON oraz XLSX.

Manago AI wdraża monitoring technicznych limitów eksportu, takich jak ograniczenia wielkości pojedynczego pliku eksportu oraz limit zapytań API na poziomie 500 zapytań na minutę, co zapewnia optymalną wydajność infrastruktury.

Procedura / metoda migracji	Dostępność	Ograniczenia techniczne	Komentarze / uwagi
Eksport danych przez UI	TAK	Maksymalny rozmiar pliku eksportu	Eksport CSV/XLSX
Eksport danych przez API (JSON)	TAK	Limit zapytań API/minuta	Wymagana integracja klienta
Migracja między innymi dostawcami	NIE	-	Brak możliwości ze względu na koszty

Załącznik nr 8 do OWU
Aktualny rejestr internetowy prowadzony przez Manago AI ze szczegółowymi informacjami o wszelkich strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne, o których mowa w Załączniku nr 5.

Zgodnie z wymaganiami interoperacyjności, Manago AI udostępnia publiczny rejestr informacji technicznych dla danych eksportowalnych, które można przenieść w ramach zmiany dostawcy usług przetwarzania danych.

Rejestr zawiera szczegółowe informacje o:

- strukturach danych stosowanych przy eksporcie (np. contact, email, campaign),
- dostępnych formatach (CSV, JSON, XLSX, kod źródłowy),
- otwartych normach i specyfikacjach technicznych stosowanych do zapewnienia interoperacyjności,
- standardach walidacyjnych wykorzystywanych w API Manago AI (zgodnie z dokumentacją v3/v2).

Dzięki zastosowaniu powszechnie przyjętych formatów (RFC, ISO, JSON Schema, OpenAPI), dane mogą być ponownie wykorzystywane w systemach CRM, ERP, marketing automation czy BI.

Kategoria danych / aktywów	Format eksportowy	Normy i specyfikacje interoperacyjności
Dane kontaktowe klientów	CSV, JSON, XLSX	- RFC 882 (Email) - ietf.org - RFC 4122 (UUID) - ietf.org - ISO 8601 (daty) - iso.org - ISO 3166-1 (kraje) - iso.org - RFC 4180 (CSV) - ietf.org
Dane kampanii marketingowych	JSON, CSV	- JSON Schema → json-schema.org

		- ISO 8601, UUID
Raporty analityczne	JSON, CSV, XLSX	- CSVW (CSV on the Web) → w3.org - ISO 8601, UUID
Skrypty integracyjne	JSON, kod źródłowy	- OpenAPI 3.0 - JSON Schema
Pliki konfiguracyjne (segmenty, automatyzacje, kampanie)	JSON, CSV	- JSON Schema - ISO 8601, UUID

Załącznik nr 9 do OWU

Ogólny opis środków technicznych, organizacyjnych i umownych przyjętych przez dostawcę usług przetwarzania danych w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie Unii lub ich przekazania administracji rządowej, w przypadku gdy taki dostęp lub takie przekazanie skutkowałyby naruszeniem prawa Unii lub prawa krajowego danego państwa członkowskiego

1. ogólna polityka bezpieczeństwa danych osobowych oraz systemów informatycznych,
2. procedury dot. zgłaszania naruszeń,
3. okresowe przeglądy wewnętrznych procedur,
4. procedura postępowania w przypadku nadużyć,
5. Inspektor ochrony danych,
6. wydawane upoważnienia do przetwarzania danych osobowych,
7. szkolenia z zakresu ochrony danych osobowych,
8. oświadczenia o zachowaniu w poufności danych osobowych,
9. ograniczenie dostępu do obszaru przetwarzania danych osobowych (fizycznych miejsc przetwarzania) poprzez w szczególności stosowanie kart dostępu oraz kodów dostępu, szaf i pomieszczeń zamykanych na klucz, monitoringu wizyjnego (w zakresie Data Center oraz monitoringu stosowanego przez administratora biura, w którym mieści się siedzibą Benhauer), systemu alarmowego (w zakresie Data Center), korzystanie z usług firmy ochroniarskiej oraz ograniczenie dostępu do systemów informatycznych, w których przetwarzane są dane osobowe oraz sieci (stosowanie loginu i haseł, wyodrębnienie sieci dla osób trzecich, stosowanie automatycznego wygaszania i blokowania ekranu),
10. procedura nadawania i odbierania uprawnień dostępu do systemów informatycznych,
11. polityka haseł,
12. stosowanie bezpiecznych połączeń sieciowych, np. VPN,
13. High Availability Cluster,
14. środki mające na celu zapewnienie ewidencji zdarzeń, np. Microsoft Clarity, Wewnętrzny system logowania],
15. system anty ddos, np. WanGuard,
16. przeprowadzanie kwartalnych testów podatności systemów informatycznych,
17. przeprowadzanie testów penetracyjnych systemów informatycznych,
18. oprogramowanie antywirusowe,
19. szkolenia z zakresu cyberbezpieczeństwa,
20. procedura weryfikacji usługodawców w zakresie zgodności z przepisami oraz stosowania adekwatnych środków bezpieczeństwa,
21. cyklicznie przeprowadzana analiza ryzyka naruszenia praw i wolności osób, których dane przetwarzane są w procesie przetwarzania,
22. analiza ryzyka związanego z bezpieczeństwem i prywatnością realizowana co najmniej raz w roku,
23. procedury dot. stosowania zasady ochrony prywatności w fazie projektowania oprogramowania,

24. standard dotyczący zachowania zasady ochrony prywatności w ustawieniach domyślnych w fazie projektowania,
25. stosowanie kryptograficznych środków ochrony danych osobowych, np. [protokół SSL [TLS 1.2 - 1.3 + SHA256}],
26. zabezpieczenie przesyłu danych protokołem HTTPS,
27. stosowanie wieloskładnikowego uwierzytelniania użytkownika w systemie teleinformatycznym,
28. środki identyfikacji i autoryzacji użytkowników np. panel logowania typu Basic Auth,
29. logi audytowe informujące o masowych akcjach modyfikujących dane w platformie,
30. indywidualne wskaźniki logowania,
31. Umowa powierzenia danych osobowych, w tym umowny zakaz przekazywania danych osobowych poza Europejski Obszar Gospodarczy bez zgody administratora
32. Umowa o zachowaniu poufności

Załącznik nr 10 do OWU
Informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi

Obecna architektura systemu Manago AI nie posiada znaczących ograniczeń technicznych ani organizacyjnych, które utrudniałyby migrację do innego dostawcy usług. Wszystkie dane klientów są w pełni możliwe do eksportu przez dostępne mechanizmy UI oraz API. Brak jest także złożonych zależności technologicznych mogących uniemożliwić lub istotnie utrudnić taką migrację. Firma stosuje otwarte standardy oraz popularne formaty eksportowe, dzięki czemu minimalizuje ryzyko wystąpienia sytuacji vendor lock-in.

Komponent / usługa	Trudność migracji	Możliwości eksportowe	Uwagi
Dane klientów	Łatwa	CSV, JSON, XLSX	Eksport dostępny UI/API
Raporty i konfiguracje kampanii	Łatwa	CSV, JSON	Dostępny eksport przez UI/API
Integracje zewnętrzne	Średnia	JSON, kod źródłowy	Wymagana rekonfiguracja integracji po stronie nowego dostawcy
Specyficzne zależności technologiczne	Brak	-	Brak znanych ograniczeń technologicznych