VIMS — VARILO INTEGRATED MANAGEMENT SYSTEM

Umowa powierzenia przetwarzania danych osobowych

Wersja: 1.0 | Aktualizacja: 2026-09-26

Wzór umowy powierzenia zawieranej na podstawie art. 28 RODO pomiędzy organizacją korzystającą z platformy VIMS (administratorem danych) a dostawcą platformy (podmiotem przetwarzającym). Dokument stanowi załącznik do umowy głównej i jest gotowy do podpisu.

Vesta Usługi i Szkolenia Marcin Makowski, ul. Wrzosowa 33, 84-300 Lębork, Polska · NIP/VAT ID: 841-161-18-09 · kontakt@varilo.eu · v-ims.pl

1. Strony i przedmiot umowy

Podmiot przetwarzający: Vesta Usługi i Szkolenia Marcin Makowski, ul. Wrzosowa 33, 84-300 Lębork, Polska, NIP 841-161-18-09, adres kontaktowy do spraw ochrony danych: kontakt@varilo.eu.

Administrator danych: organizacja korzystająca z platformy VIMS na podstawie umowy głównej, wskazana w treści tej umowy wraz z danymi rejestrowymi i adresem kontaktowym do spraw ochrony danych.

Przedmiotem umowy jest powierzenie przetwarzania danych osobowych w zakresie niezbędnym do świadczenia usługi dostępu do platformy VIMS. Umowa zostaje zawarta na podstawie art. 28 ust. 3 RODO i obowiązuje przez czas trwania umowy głównej.

2. Charakter, cel i czas przetwarzania

Przetwarzanie odbywa się w formie zautomatyzowanej, w systemie informatycznym udostępnianym przez podmiot przetwarzający, i obejmuje takie operacje jak zbieranie, utrwalanie, przechowywanie, porządkowanie, modyfikowanie, przeglądanie, udostępnianie uprawnionym użytkownikom administratora, usuwanie oraz tworzenie kopii zapasowych.

Celem przetwarzania jest umożliwienie administratorowi prowadzenia w systemie procesów z zakresu bezpieczeństwa pracy, ochrony środowiska, ochrony przeciwpożarowej, jakości i zgodności — w szczególności rejestrów zdarzeń, ocen ryzyka, ewidencji szkoleń i uprawnień, rejestru substancji chemicznych, kontroli i audytów oraz działań korygujących.

Przetwarzanie trwa przez okres obowiązywania umowy głównej oraz przez okres niezbędny do zwrotu lub usunięcia danych po jej zakończeniu.

3. Kategorie osób, których dane dotyczą

- Pracownicy i osoby współpracujące z administratorem, posiadający konta użytkowników w systemie.
- Pracownicy administratora objęci prowadzonymi w systemie rejestrami — ewidencją szkoleń i kwalifikacji, badań lekarskich, ocen ryzyka i przydziałów stanowiskowych.
- Osoby uczestniczące w zdarzeniach wypadkowych i potencjalnie wypadkowych: poszkodowani, świadkowie, osoby prowadzące postępowanie.
- Pracownicy podwykonawców i firm zewnętrznych dopuszczanych do prac na terenie administratora.

- Osoby wskazane jako kontakty organizacyjne: przedstawiciele służb, kierownicy, osoby zatwierdzające zezwolenia i wnioski o zmianę.
- W modelu obsługi wielu klientów przez firmę świadczącą usługi bezpieczeństwa pracy — również osoby, których dane dotyczą, po stronie klientów obsługiwanych przez administratora, o ile administrator zapewnił podstawę prawną ich przetwarzania.

4. Rodzaje powierzonych danych osobowych

- Dane identyfikacyjne i kontaktowe: imię i nazwisko, stanowisko, jednostka organizacyjna, służbowy adres e-mail i numer telefonu.
- Dane zatrudnienia i kompetencji: przydział do stanowiska i strefy, zakres uprawnień, szkolenia, kwalifikacje, terminy ich odnowienia.
- Dane dotyczące zdarzeń: opis okoliczności zdarzenia, rola osoby w zdarzeniu, ustalenia postępowania, załączniki w tym dokumentacja fotograficzna.
- Dane związane z profilaktyczną opieką zdrowotną w zakresie prowadzonym przez administratora: rodzaj badania, data wykonania, data następnego badania, informacja o orzeczeniu o zdolności do pracy. Administrator zobowiązuje się nie wprowadzać do systemu danych o stanie zdrowia w zakresie szerszym niż wymagany przepisami prawa pracy.
- Dane techniczne kont i logowań: identyfikator konta, adres e-mail, informacje o urządzeniach zaufanych, znaczniki czasu zdarzeń bezpieczeństwa.
- Strony zgodnie ustalają, że administrator nie wprowadza do systemu danych szczególnych kategorii innych niż wskazane powyżej ani danych dotyczących wyroków skazujących, chyba że uzgodni to odrębnie na piśmie z podmiotem przetwarzającym.

5. Obowiązki podmiotu przetwarzającego

- Przetwarzanie danych wyłącznie na udokumentowane polecenie administratora, którym jest również konfiguracja i sposób korzystania z systemu przez administratora, oraz zgodnie z niniejszą umową.
- Zapewnienie, że osoby upoważnione do przetwarzania danych zobowiązały się do zachowania poufności, również po zakończeniu współpracy.
- Wdrożenie i utrzymywanie środków technicznych i organizacyjnych, o których mowa w art. 32 RODO, opisanych w punkcie 6 tej umowy.
- Wspieranie administratora w realizacji żądań osób, których dane dotyczą, w tym niezwłoczne przekazywanie administratorowi wniosków skierowanych omyłkowo do podmiotu przetwarzającego.
- Wspieranie administratora w wypełnianiu obowiązków z art. 32–36 RODO, w szczególności w zakresie oceny skutków dla ochrony danych i obsługi naruszeń.
- Udostępnianie administratorowi informacji niezbędnych do wykazania zgodności oraz umożliwienie audytu na zasadach opisanych w punkcie 8.
- Informowanie administratora, jeżeli w ocenie podmiotu przetwarzającego wydane polecenie narusza przepisy o ochronie danych osobowych.

6. Środki techniczne i organizacyjne

- Szyfrowanie transmisji danych między przeglądarką użytkownika a systemem.
- Obowiązkowe uwierzytelnianie dwuetapowe kont: hasło oraz jednorazowy kod przesyłany na adres e-mail konta, z ograniczoną ważnością i limitem prób.

- Przechowywanie haseł i jednorazowych kodów wyłącznie w postaci skrótów kryptograficznych.
- Izolacja danych poszczególnych organizacji wymuszana na poziomie bazy danych, na poziomie pojedynczego wiersza, niezależnie od filtrów interfejsu.
- Kontrola uprawnień oparta na rolach, z zatwierdzaniem członkostwa w organizacji przez właściciela lub administratora organizacji oraz przechowywaniem uprawnień poza profilem użytkownika.
- Ochrona załączników, w tym dokumentacji fotograficznej zdarzeń, przed dostępem z pominięciem kontroli uprawnień — pliki nie są dostępne pod publicznym adresem.
- Rejestr zdarzeń bezpieczeństwa obejmujący logowania, zmiany uprawnień, eksporty danych i odsłonięcia danych szczególnie chronionych.
- Automatyczne kopie zapasowe warstwy danych wykonywane w infrastrukturze dostawcy chmurowego oraz procedura odtworzenia środowiska z kopii.
- Przetwarzanie danych w infrastrukturze zlokalizowanej na terenie Europejskiego Obszaru Gospodarczego.
- Rozdzielenie uprawnień administracyjnych platformy od uprawnień w obrębie organizacji klienta oraz zasada minimalnego dostępu dla personelu wsparcia.

7. Dalsze powierzenie (podprocesorzy)

Administrator udziela podmiotowi przetwarzającemu ogólnej zgody na korzystanie z podprocesorów niezbędnych do świadczenia usługi, pod warunkiem nałożenia na nich obowiązków ochrony danych nie mniej rygorystycznych niż wynikające z tej umowy.

W dniu zawarcia umowy podmiot przetwarzający korzysta z następujących kategorii podprocesorów: dostawca infrastruktury chmurowej i zarządzanej bazy danych wraz z przestrzenią na załączniki, dostawca usług wysyłki wiadomości transakcyjnych i powiadomień e-mail, dostawca hostingu i dostarczania warstwy aplikacyjnej.

O planowanej zmianie lub dodaniu podprocesora podmiot przetwarzający informuje administratora z wyprzedzeniem co najmniej trzydziestu dni. Administrator może wnieść uzasadniony sprzeciw; jeżeli strony nie uzgodnią rozwiązania, administrator może wypowiedzieć umowę główną w trybie w niej przewidzianym.

8. Audyt i wykazanie zgodności

Administrator ma prawo weryfikować sposób wykonywania umowy, w tym przeprowadzić audyt, po uprzednim zawiadomieniu z wyprzedzeniem co najmniej czternastu dni, w godzinach pracy i w sposób nieprzerywający ciągłości usługi.

Audyt nie może obejmować dostępu do danych innych organizacji korzystających z platformy ani do informacji stanowiących tajemnicę przedsiębiorstwa podmiotu przetwarzającego lub jego podprocesorów.

Podmiot przetwarzający może wykazać zgodność przez udostępnienie opisu środków bezpieczeństwa, odpowiedzi na kwestionariusz bezpieczeństwa oraz dokumentacji uzyskanej od podprocesorów infrastruktury.

9. Naruszenia ochrony danych

Podmiot przetwarzający zgłasza administratorowi każde naruszenie ochrony powierzonych danych osobowych bez zbędnej zwłoki, nie później niż w ciągu czterdziestu ośmiu godzin od jego stwierdzenia, na adres kontaktowy administratora wskazany w umowie.

Zgłoszenie zawiera dostępne informacje o charakterze naruszenia, kategoriach i przybliżonej liczbie osób oraz rekordów, prawdopodobnych konsekwencjach i podjętych lub proponowanych środkach zaradczych. Informacje niedostępne w chwili zgłoszenia przekazywane są sukcesywnie.

Zgłoszenia do organu nadzorczego oraz zawiadomienia osób, których dane dotyczą, dokonuje administrator. Podmiot przetwarzający udziela mu w tym zakresie niezbędnej pomocy.

10. Zwrot i usunięcie danych po zakończeniu umowy

Administrator może w dowolnym momencie trwania umowy, a także przed jej zakończeniem, samodzielnie pobrać z systemu archiwum danych swojej organizacji. Uprawnienie to przysługuje właścicielowi oraz administratorowi organizacji, a wykonanie eksportu jest odnotowywane w rejestrze zdarzeń.

Po zakończeniu umowy głównej podmiot przetwarzający usuwa powierzone dane w terminie trzydziestu dni od zakończenia umowy albo zwraca je administratorowi, zgodnie z jego pisemnym żądaniem złożonym najpóźniej w dniu zakończenia umowy.

Usunięcie obejmuje również kopie danych, z zastrzeżeniem kopii zapasowych, które są usuwane wraz z wygaśnięciem ich cyklu retencji, oraz danych, których przechowywanie jest wymagane przepisami prawa.

11. Odpowiedzialność i postanowienia końcowe

Każda ze stron odpowiada za skutki naruszenia przepisów o ochronie danych osobowych w zakresie własnych obowiązków. Administrator odpowiada w szczególności za podstawę prawną przetwarzania, zakres wprowadzanych do systemu danych oraz realizację obowiązku informacyjnego wobec osób, których dane dotyczą.

Zmiany umowy wymagają formy pisemnej lub równorzędnej formy elektronicznej z podpisem kwalifikowanym, z wyjątkiem aktualizacji wykazu podprocesorów dokonywanej w trybie opisanym w punkcie 7.

W sprawach nieuregulowanych stosuje się RODO, przepisy prawa polskiego oraz postanowienia umowy głównej i Regulaminu platformy VIMS.

Wzór w wersji 1.0 obowiązuje od 2026-09-26 i jest publikowany pod adresem v-ims.pl/umowa-powierzenia-dpa.