Warunki powierzenia przetwarzania danych osobowych - Pidgey

Kandydat po opracowaniu: nie wszedł w życie. Warunki publikacji wskazano w raporcie przeglądu.

Wersja 1.1 z 1 listopada 2026 r. Załącznik do umowy o Pidgey; wymaga przyjęcia przez strony i spełnienia warunków dopuszczenia podwykonawców.

1. Strony i zawarcie

Podmiotem przetwarzającym jest ELECTRO-VIBE sp. z o.o., ul. Piastowska 108, 80-358 Gdańsk, KRS 0001245544, NIP 5842885852, kapitał zakładowy 5 000 zł, kontakt biuro@electro-vibe.pl, tel. +48 692 348 335. Powierzającym jest klient zidentyfikowany w zamówieniu i potwierdzeniu umowy, który określa cele i sposoby przetwarzania danych swojej organizacji. Jeżeli sam działa jako procesor, zapewnia umocowanie do dalszego powierzenia.

Załącznik jest zawierany w formie pisemnej, w tym elektronicznej, przez udokumentowane przyjęcie zidentyfikowanej wersji przez uprawnione strony. Samo otwarcie strony, dodanie pracownika lub publikacja dokumentu nie dowodzi zawarcia powierzenia. Warunki nie są zgodą osób na dowolne przetwarzanie ich danych.

2. Przedmiot, cel i czas

Przedmiotem jest obsługa danych w wyodrębnionej organizacji Pidgey w celu świadczenia zamówionych funkcji zarządzania pracą, projektami, zadaniami, czasem, raportami, komunikacją i rozliczeniami. Operacje obejmują zbieranie na polecenie, zapisywanie, porządkowanie, przechowywanie, udostępnianie uprawnionym osobom, eksport, odtwarzanie i usuwanie.

Powierzenie trwa przez wykonywanie usługi, a następnie wyłącznie w zakresie niezbędnym do uzgodnionego zwrotu, ograniczonego archiwum, usunięcia i ochrony kopii. Na udokumentowane polecenie klienta archiwum może trwać do 12 miesięcy od zakończenia aktywnej umowy; klient może wcześniej wybrać zwrot lub usunięcie. Nie daje to operatorowi prawa dalszego używania dokumentacji do własnych celów.

3. Osoby i rodzaje danych

Kategorie osób: właściciele i przedstawiciele klienta, pracownicy, współpracownicy, osoby wykonujące prace, osoby kontaktowe kontrahentów oraz osoby, których dane klient zasadnie zamieszcza w dokumentacji projektów.

Kategorie danych: imiona i nazwiska, służbowe dane kontaktowe, identyfikatory i role, uprawnienia, przypisania do projektów i zadań, ewidencja czasu, raporty, zatwierdzenia, dane zawodowe i rozliczeniowe oraz treść przekazanych wiadomości, zdjęć i dokumentów. Szczególne kategorie z art. 9 RODO i dane z art. 10 nie są objęte domyślnym zakresem; wymagają odrębnego uzgodnienia legalności, funkcji i zabezpieczeń przed przekazaniem.

4. Instrukcje i poufność

Przetwarzamy dane wyłącznie na udokumentowane polecenie klienta, także w sprawie przekazywania poza EOG, chyba że obowiązek wynika z prawa; wówczas informujemy przed przetwarzaniem, o ile prawo tego nie zabrania. Instrukcjami są uzgodniony zakres umowy, działania upoważnionych osób w organizacji oraz zweryfikowane polecenia przekazane ustalonym kanałem.

Jeżeli polecenie narusza przepisy ochrony danych, niezwłocznie informujemy klienta i wyjaśniamy możliwość zgodnego wykonania. Zapewniamy, że osoby z dostępem są upoważnione, podlegają

obowiązkowi poufności i otrzymują zakres dostępu odpowiadający zadaniom. Obowiązek poufności pozostaje po zakończeniu współpracy.

5. Bezpieczeństwo

Stosujemy środki odpowiednie do ryzyka, zgodnie z art. 32 RODO: uwierzytelnianie i zarządzanie uprawnieniami w kontekście organizacji, szyfrowanie transmisji, ochronę haseł, rejestrację istotnych operacji, aktualizacje bezpieczeństwa, ograniczenie dostępu administracyjnego, kopie bezpieczeństwa i sprawdzanie możliwości odtworzenia. Zakres i skuteczność środków podlegają okresowej ocenie, uwzględniającej poufność, integralność, dostępność i odporność.

Nie deklarujemy bezwarunkowej odporności na każdą awarię ani nie utożsamiamy zaszyfrowanej kopii z gwarantowaną kompletnością danych źródłowych. O znanym ograniczeniu istotnym dla powierzonych danych informujemy klienta. Zmiana środka technicznego nie może obniżyć uzgodnionego poziomu ochrony.

6. Dalsi przetwarzający i transfery

Przed rozpoczęciem dalszego powierzenia dostawca przedstawia tożsamość podwykonawcy, czynności, lokalizacje i podstawy ewentualnych transferów oraz zapewnia umowę nakładającą obowiązki wymagane art. 28 ust. 4 RODO. Zgoda klienta na podwykonawcę nie zastępuje brakującej umowy z tym podwykonawcą.

Ogólna zgoda na korzystanie z należycie umocowanych podwykonawców wymaga wcześniejszego przekazania ich wykazu. O planowanym dodaniu lub zastąpieniu informujemy co najmniej 30 dni przed zmianą, umożliwiając uzasadniony sprzeciw dotyczący ochrony danych i uzgodnienie rozwiązania. Dostawca odpowiada wobec klienta za wykonanie obowiązków podwykonawcy zgodnie z RODO.

Obecna infrastruktura obejmuje hosting OVHcloud, pocztę Interia.pl i zaszyfrowane kopie w konsumenckim Dysku Google. Ten opis nie jest zatwierdzonym wykazem dalszych przetwarzających. Google nie oferuje umowy powierzenia dla wersji konsumenckiej. Zanim ten załącznik będzie mógł być stosowany jako kompletne umocowanie przetwarzania danych klienta, należy zapewnić zgodną konfigurację i przekazać wykaz rzeczywiście prawidłowo umocowanych dostawców. Nie ustanawiamy fikcyjnej umowy ani transferu samym postanowieniem niniejszego dokumentu.

Transfer wymagający rozdziału V RODO może następować tylko po zapewnieniu właściwego mechanizmu i ocenie jego warunków, z niezbędnymi środkami uzupełniającymi. Szyfrowanie, ogólna zgoda na usługę ani akceptacja tej umowy nie zastępują tych wymagań.

7. Prawa osób, naruszenia i pomoc

Uwzględniając charakter przetwarzania, pomagamy klientowi wykonywać żądania osób i obowiązki z art. 32-36 RODO. Żądanie dotyczące danych powierzonych przekazujemy bez zbędnej zwłoki i nie odpowiadamy merytorycznie w miejsce administratora bez jego polecenia, chyba że przepis stanowi inaczej.

O naruszeniu ochrony danych powierzonych zawiadamiamy klienta bez zbędnej zwłoki po jego stwierdzeniu. Zgłoszenie obejmuje dostępne informacje o charakterze naruszenia, kategoriach i przybliżonej liczbie osób i zapisów, możliwych skutkach, podjętych środkach i kontakcie; informacje można uzupełniać etapami. Nie odkładamy pierwszej informacji do zakończenia pełnego dochodzenia. Zabezpieczamy dowody i pomagamy w zgłoszeniu organowi, poinformowaniu osób oraz ograniczeniu skutków.

Administrator podejmuje własne decyzje o podstawach, zawiadomieniach i ocenie skutków. Powierzenie nie przenosi na operatora wszystkich obowiązków pracodawcy ani administratora. Nie ograniczamy pomocy do niezweryfikowanego zapewnienia o zgodności.

8. Informacje i audyty

Udostępniamy informacje niezbędne do wykazania wykonania obowiązków oraz umożliwiamy i wspieramy audyty, w tym inspekcje, prowadzone przez klienta lub upoważnionego audytora. Uzgadniamy sposób chroniący inne organizacje, poufne informacje i bezpieczeństwo oraz odpowiadający zakresowi kontroli. Warunki organizacyjne nie mogą faktycznie wyłączać uprawnienia z art. 28 RODO ani uprawnień organu nadzorczego.

9. Zwrot, usunięcie i kopie

Po zakończeniu świadczenia klient wybiera zwrot albo usunięcie powierzonych danych, chyba że prawo wymaga ich dalszego przechowywania. Po zwrocie usuwamy pozostające kopie zgodnie z uzgodnionym zakresem; ograniczone archiwum wymaga udokumentowanego polecenia klienta. Potwierdzamy wykonanie, wskazując rzeczywisty zakres, termin i prawnie uzasadnione wyjątki.

Dane w kopiach są odseparowane od zwykłego użycia i dostępne wyłącznie upoważnionym osobom w celach bezpieczeństwa i odtworzenia. Harmonogram usuwania musi obejmować również kopie; nie wolno pozostawić ich bezterminowo po upływie uzgodnionego okresu. Przy odtwarzaniu ponownie wykonuje się obowiązujące polecenia usunięcia, aby dane nie wróciły do bieżącej pracy.

Przyjęty harmonogram kopii przewiduje ich codzienne wykonywanie i zachowanie do siedmiu punktów dziennych, czterech tygodniowych oraz trzech miesięcznych, przy maksymalnym wieku każdego punktu 90 dni. Ten sam punkt może spełniać kilka kategorii, więc nie oznacza to 14 niezależnych pełnych kopii. Harmonogram nie przedłuża automatycznie okresu przetwarzania danych po żądaniu usunięcia, zakończeniu właściwego powierzenia lub upływie ustawowego terminu. Takie przypadki wymagają odrębnego wykonania i potwierdzenia właściwej instrukcji, również wobec kopii.

Nie kasuje się ręcznie pojedynczych obiektów zaszyfrowanego repozytorium restic. Usuwanie migawek wymaga kontrolowanej operacji retencji z oceną zależności, potwierdzeniem zakresu i weryfikacją odtworzenia. Obecny brak automatycznej rotacji kopii Google jest ograniczeniem wymagającym operacyjnego zamknięcia, nie uzgodnioną bezterminową retencją.

Zatwierdzenie harmonogramu nie oznacza samo przez się jego działania w każdym używanym środowisku. Przed zastosowaniem tej umowy jako kompletnego umocowania operator musi wykazać wdrożenie i kontrolę terminów oraz rzeczywisty zwrot i usuwanie danych. Test jednorazowego repozytorium jest dowodem mechanizmu, a nie potwierdzeniem usunięcia danych konkretnego klienta.