Polityka prywatności ClockIt

Wersja 2026-10-26-B2B-04.

1 Operator i role w przetwarzaniu danych

Operatorem ClockIt jest Patryk Pławski, NIP 5842854283, ul. Hołdu Pruskiego 4/1, 80-321 Gdańsk, e-mail: kontakt@clockit.pl. Serwis jest dostępny pod adresem https://clockit.pl, a panel pod adresem https://panel.clockit.pl. W sprawach danych osobowych kontaktuj się na kontakt@clockit.pl lub listownie na adres Operatora.

ClockIt obsługuje organizację pracy w firmach. Administratorem danych dotyczących pracy, wynagrodzeń, nieobecności, komunikacji i lokalizacji jest pracodawca albo inna organizacja udostępniająca konto. Jej tożsamość wynika z zaproszenia i przypisania konta do organizacji. Organizacja przekazuje użytkownikowi własną informację o przetwarzaniu danych, w tym swój kontakt w sprawach prywatności. Operator obsługuje te dane na jej udokumentowane polecenie, zgodnie z umową powierzenia. Rola administratora konta w interfejsie nie oznacza automatycznie roli administratora danych w rozumieniu RODO.

Operator jest odrębnym administratorem danych niezbędnych do nawiązania i rozliczenia własnej współpracy, obsługi pytań i reklamacji, ochrony swoich roszczeń oraz bezpieczeństwa własnej infrastruktury. Dane z treści dokumentacji pracowniczej nie stają się z tego powodu danymi wykorzystywanymi we własnych celach Operatora. Niniejsza polityka nie zastępuje informacji pracodawcy.

2 Zakres i źródła danych

W zależności od używanych modułów dane obejmują:

- konto: imię, nazwisko, e-mail, identyfikator, rolę, organizację i oddział, stanowisko, opcjonalny telefon i zdjęcie, skrót hasła, dane aktywacji, sesji i uwierzytelniania dwuskładnikowego;
- organizację i współpracę: nazwę firmy, NIP, adres, dane przedstawicieli i osób kontaktowych, zamówienia, akceptacje dokumentów, faktury i historię obsługi;
- pracę: rozpoczęcie i zakończenie, przerwy, grafiki, dostępność, korekty, miejsca pracy, nieobecności i statusy wniosków;
- rozliczenia i dokumenty: stawki, wymiar i rodzaj współpracy, informacje płacowe oraz skany umów i dokumenty nieobecności wprowadzone przez organizację;
- GPS: współrzędne, czas i dokładność pomiaru, adres miejsca, a w GPS Pro także kolejne punkty, odcinki i postoje aktywnej zmiany;
- współpracę zespołu: treści komunikatów i zadań, odbiorców, potwierdzenia odczytu i wykonania, wiadomości czatu i ich metadane, zdjęcia, nagrania, filmy i inne załączniki;
- dane techniczne: adres IP, wersję aplikacji i platformę, tokeny powiadomień, zdarzenia logowania, błędy i informacje niezbędne do działania oraz ochrony usługi;
- treść zgłoszeń pomocy i korespondencji.

Dane pochodzą od użytkownika, jego urządzenia, organizacji i osób upoważnionych przez organizację. Firma może utworzyć konto i wprowadzić dane przed pierwszym logowaniem. W takich sytuacjach własną informację o źródle i celu przekazuje organizacja.

Nieobecność chorobowa lub załącznik mogą ujawniać dane o zdrowiu. Organizacja ogranicza je do informacji koniecznych i prawnie dopuszczalnych. Aplikacja nie służy do gromadzenia historii leczenia, diagnoz ani pełnej dokumentacji medycznej. Zwykłe zdjęcie profilowe nie jest wykorzystywane do rozpoznawania twarzy.

3 Cele i podstawy prawne Operatora

Operator wykorzystuje dane do zawarcia i wykonywania umowy z klientem będącym osobą fizyczną oraz działań przed jej zawarciem na żądanie tej osoby na podstawie art. 6 ust. 1 lit. b RODO. Obsługa przedstawicieli i osób kontaktowych, sprawdzanie reprezentacji, prowadzenie korespondencji, obsługa reklamacji, bezpieczeństwo własnej infrastruktury i ochrona roszczeń opierają się na art. 6 ust. 1 lit. f RODO. Interesem jest sprawna i bezpieczna obsługa współpracy oraz ochrona praw Operatora. Obowiązki podatkowe i dokumentacyjne są realizowane na podstawie art. 6 ust. 1 lit. c RODO w związku z odpowiednimi przepisami.

Dane niezbędne do zawarcia umowy, rozliczeń lub obsługi zgłoszenia są wymagane do realizacji danego celu; ich brak może uniemożliwić jego wykonanie. Podanie innych informacji jest dobrowolne. Samo utworzenie konta lub kontakt z Operatorem nie stanowią zgody na newsletter lub marketing telefoniczny.

Podstawy przetwarzania danych o pracy ustala organizacja. Dotyczy to również właściwej przesłanki z art. 9 ust. 2 RODO dla informacji o zdrowiu. Obowiązek ewidencji czasu nie oznacza automatycznie uprawnienia do zapisywania całej trasy GPS. Akceptacja regulaminu, potwierdzenie zapoznania się z informacją i uprawnienie systemowe telefonu mają różne znaczenie; nie są zbiorczą zgodą na przetwarzanie danych pracowniczych.

4 Uprawnienia urządzenia i GPS

Lokalizacja pozwala potwierdzać miejsce rozpoczęcia i zakończenia pracy. GPS Pro może zapisywać trasę podczas aktywnej zmiany, także w tle. Rozpoczęcie przerwy nie kończy zmiany i samo w sobie nie zatrzymuje rejestracji. Także wylogowanie z aplikacji nie musi zakończyć aktywnej zmiany. Zapis zatrzymuje się przez zakończenie zmiany; system telefonu może ograniczyć go wcześniej. Pozostawienie aktywnej zmiany po rzeczywistym zakończeniu pracy może spowodować zbędny zapis. Użytkownik powinien zakończyć zmianę i sprawdzić jej status. Błędny zapis należy zgłosić organizacji.

Uprawnienia zmienia się w ustawieniach systemu. Cofnięcie dostępu ogranicza funkcję, lecz nie usuwa wcześniejszych danych. Organizacja przekazuje zasady korzystania z lokalizacji i rozwiązanie zastępcze, jeśli funkcja nie może być używana zgodnie z prawem, w szczególności na prywatnym urządzeniu. Błędy i luki GPS nie są samodzielnym dowodem niewykonywania pracy.

Aparat i wybrane zdjęcia służą dodawaniu treści przez użytkownika. Mikrofon służy do nagrywania uruchomionej wiadomości głosowej. Powiadomienia informują o zdarzeniach; ich treść może być widoczna na zablokowanym ekranie zgodnie z ustawieniami urządzenia. Biometrię przy odblokowaniu obsługuje system telefonu, który przekazuje aplikacji wynik, a nie wzorzec twarzy lub odcisku palca.

5 Odbiorcy i przetwarzanie międzynarodowe

Odbiorcami danych organizacji są jej uprawnieni użytkownicy, uczestnicy właściwych rozmów i wyznaczeni odbiorcy raportów. Operator korzysta z dostawców hostingu, poczty, kopii, obsługi mediów, map i powiadomień. Szczegółowy wykaz usług i zakresów zawiera dokument 06 Dostawcy i przekazywanie danych. Dane mogą otrzymać również upoważnieni doradcy, księgowość, obsługa prawna oraz organy uprawnione przepisami, w niezbędnym zakresie.

Backend i baza PostgreSQL są utrzymywane w Railway w regionie us-west2 w Stanach Zjednoczonych. Resend obsługuje e-maile z podstawowym przetwarzaniem w USA. Globalne usługi panelu, powiadomień, mediów i automatyzacji mogą obejmować przetwarzanie albo dostęp spoza Europejskiego Obszaru Gospodarczego. Usługa nie jest ograniczona do polskich ani wyłącznie europejskich serwerów.

Transfer poza EOG wymaga podstawy z rozdziału V RODO. Operator zapewnia ją przez właściwą decyzję stwierdzającą odpowiedni stopień ochrony, gdy obejmuje konkretnego odbiorcę i transfer, albo odpowiednie zabezpieczenia, w szczególności standardowe klauzule umowne wraz z oceną i potrzebnymi środkami uzupełniającymi. Umowa z klientem nie zastępuje tych zabezpieczeń. Kopię informacji o zabezpieczeniach można uzyskać na kontakt@clockit.pl, z ochroną cudzych danych i tajemnic.

Mapy, GIF-y i miniatury z zewnętrznych źródeł mogą powodować bezpośrednie żądanie urządzenia do dostawcy, obejmujące IP, parametry urządzenia, obszar mapy lub wpisaną frazę. Otwarcie odnośnika do zewnętrznego serwisu wiąże się także z zasadami tego serwisu. Zakres zgód na pamięć urządzenia opisuje dokument 11.

6 Okresy przechowywania

Dane powierzone są obsługiwane zgodnie z dokumentem 08 Retencja i zwrot danych: trasy GPS do 90 dni od pomiaru, czat i załączniki do 12 miesięcy od wiadomości, rutynowe logi do 90 dni. Dla dokumentacji zatrudnienia i ewidencji organizacja ustala właściwy okres wynikający z celu i przepisów oraz zabezpiecza jej wymagane archiwum. Okresy szczególne i odbiór po zakończeniu usługi określa ten sam dokument. Organizacja może polecić wcześniejsze usunięcie zbędnych danych.

Własne zapytania handlowe Operator przechowuje do zamknięcia sprawy, nie dłużej niż 12 miesięcy od ostatniego kontaktu, chyba że są częścią dokumentacji umowy, reklamacji lub sporu. Dane umowy i rozliczeń są przechowywane w czasie współpracy, a następnie przez właściwy okres obowiązkowej dokumentacji oraz przedawnienia roszczeń, z uwzględnieniem zdarzeń zmieniających jego bieg. Materiał konkretnego incydentu lub sporu może być wyodrębniony na czas postępowania i realizacji związanych z nim obowiązków. Pozostałych danych nie zachowuje się z tego powodu bezterminowo.

7 Prawa osób

W granicach RODO przysługują prawa dostępu i kopii, sprostowania, usunięcia, ograniczenia i przenoszenia danych, gdy zachodzą ustawowe warunki. Przy uzasadnionym interesie można wnieść sprzeciw związany ze szczególną sytuacją osoby. Odrębną zgodę można cofnąć bez wpływu na zgodność wcześniejszego przetwarzania. Skargę można skierować do Prezesa Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl, bez konieczności wcześniejszego kontaktu z Operatorem.

Żądania dotyczące dokumentacji pracy kieruje się do organizacji będącej administratorem. Operator przekazuje otrzymane żądanie właściwej organizacji i wspiera jego wykonanie. W sprawach własnych celów Operatora kontakt jest wskazany w punkcie 1. Weryfikacja tożsamości jest proporcjonalna; nie

wymaga podawania hasła ani sekretu 2FA. Odpowiedź jest udzielana bez zbędnej zwłoki, zasadniczo w ciągu miesiąca; przedłużenie wymaga ustawowej podstawy i informacji w pierwszym miesiącu.

ClockIt nie podejmuje samodzielnie decyzji kadrowych o skutkach prawnych lub podobnie istotnych, opartych wyłącznie na automatycznym przetwarzaniu. Podsumowania, szacowane wynagrodzenia i automatyczne zakończenia zmian wymagają weryfikacji uprawnionej osoby.

8 Aktywacja, zabezpieczenia i usunięcie konta

Administrator rejestrujący firmę otrzymuje losowe hasło startowe ważne 24 godziny, a przy pierwszym logowaniu konfiguruje 2FA i ustawia własne hasło. Startowe hasło jest przejściowo przechowywane w zaszyfrowanej kolejce i usuwane z niej po wysłaniu; treść wiadomości obsługuje dostawca e-maila. Pracownik zaproszony przez organizację otrzymuje odrębny link do ustawienia własnego hasła. Odzyskanie dostępu korzysta z hasła tymczasowego ważnego 15 minut i wymuszonej zmiany hasła. Stałe hasła są przechowywane jako skróty.

TOTP 2FA korzysta z sześciocyfrowych kodów zmieniających się co 30 sekund. Zapamiętanie własnego urządzenia pozwala honorować dowód zaufania do 30 dni, z możliwością wcześniejszego unieważnienia. Wylogowanie nie usuwa automatycznie dowodu zaufania. Synchronizacja Google Authenticator lub innego uwierzytelniacza podlega także warunkom wybranej aplikacji.

Archiwizacja, wylogowanie i odinstalowanie nie są usunięciem dokumentacji organizacji. Organizacja może odebrać dostęp i zlecić właściwe usunięcie. Archiwizacja może zachować powiązania historyczne i przypisanie e-maila. Obowiązek zachowania określonej dokumentacji nie uzasadnia zachowania wszystkich pozostałych treści. Eksport i końcowe usuwanie opisuje dokument 08.

9 Informacja o zmianach

Operator udostępnia oznaczone wersje dokumentów. Zmiany istotne dla korzystania z usługi przekazuje odpowiednim kanałem, w szczególności na kontakt organizacji. Aktualizacja polityki nie zastępuje odrębnej zgody, gdy wymaga jej prawo. Powierzone treści nie są sprzedawane ani wykorzystywane do własnej reklamy lub trenowania modeli AI.