

Informazioni sulle privacy policies relative all'uso della piattaforma e app mobile HiCloud Staff Management

Descrizione della piattaforma – Tipologia dei servizi offerti

HiCloud Staff Management è una piattaforma cloud per il controllo degli accessi negli edifici e la rilevazione delle presenze, che può essere utilizzata dai titolari di un sistema di sicurezza e controllo dei varchi di SAET I.S. ("Clienti") per digitalizzare ed ottimizzare alcuni processi di rilevazione dei tempi di permanenza negli stabili degli utenti autorizzati ("Utenti") fornendo dati di riscontro agli uffici amministrativi ed HR a sostegno delle loro attività di consuntivazione e rendicontazione (fatturazione delle attività di consulenza, formazione dei fogli presenza dei collaboratori).

Titolarità del trattamento

A seconda dei casi d'uso e del tipo di soggetto interessato, SAET I.S. può assumere il ruolo di titolare dei dati personali o di responsabile del loro trattamento ai fini del regolamento generale sulla protezione dei dati 2016/679 (di seguito "GDPR").

In particolare: SAET I.S. è Titolare del trattamento dei dati personali relativi ai clienti che concludono direttamente con essa un contratto, acquisendo un sistema di controllo degli accessi e presenze e/o i diritti d'uso della piattaforma software, in relazione all'esecuzione di quel contratto e per la gestione del rapporto derivante.

Relativamente invece agli utenti censiti nel sistema di controllo accessi (coloro cioè che hanno il diritto di accedere agli stabili) i dati vengono raccolti e caricati a sistema direttamente dai Clienti, senza che SAET I.S. abbia alcun rapporto o contatto con le persone interessate. In questo caso il trattamento dei dati avviene esclusivamente per conto dei proprietari dello stabile e secondo le loro istruzioni.

Pertanto, se Lei è titolare di un badge per l'accesso in uno stabile ed è autorizzato ad utilizzare la nostra piattaforma, agiamo esclusivamente come responsabili del trattamento dei Suoi dati, che sono stati raccolti dal titolare dell'immobile in esecuzione del rapporto che intrattenete con lui (di lavoro, di consulenza, ecc.)

In questo caso è il nostro cliente che ha preventivamente raccolto i Suoi dati, acquisendo a vario titolo il consenso al relativo trattamento, ha fissato (e comunicatoLe) gli scopi, così come i mezzi di raccolta dei dati, e li ha successivamente inseriti nella nostra piattaforma, per digitalizzare e remotizzare l'elaborazione delle informazioni.

Tipologia dei dati trattati

Se Lei non ha un rapporto diretto con SAET I.S., perché possa utilizzare la nostra Piattaforma e l'app, è necessario che uno dei nostri Clienti, titolare di uno immobile in cui Lei ha il diritto di accedere (ad esempio in virtù di un rapporto di lavoro) abbia creato per Lei un account Utente, inserendo alcune informazioni tra cui alcune informazioni di base (nome e cognome, indirizzo email professionale, codice fiscale, ecc.) e altri dati inerenti al Suo diritto di accedere negli stabili controllati e permanervi (ad esempio orari di lavoro, durata del contratto, indirizzo completo, reparto di appartenenza, assenze previste, ecc.), non vengono invece mai salvati dati relativi alla retribuzione o bancari.

L'app di HiCloud Staff Management consente di visualizzare per lo più dati già precaricati, come descritto sopra, tuttavia consente di modificare a run time alcuni dati relativi alla presenza o assenza di un utente nello stabile (modifiche dell'orario di lavoro, inserimento di assenze con le relative causali). In questi casi viene memorizzato anche l'identificativo dell'utente che ha disposto la modifica.

Al solo fine di garantire la qualità del prodotto e fornire il miglior servizio ai nostri clienti e agli utenti finali, inoltre, l'app potrebbe raccogliere alcuni dati relativi al dispositivo, come ID dello stesso, modello e produttore, sistema operativo, e relativa versione, indirizzo IP, ecc.

L'app non raccoglie invece informazioni di geolocalizzazione e tracciamento degli spostamenti. Quando viene utilizzata l'autenticazione biometrica in sostituzione del login, vengono chiamate direttamente funzionalità del sistema operativo sul dispositivo, e non vengono in alcun caso raccolti o salvati dati biometrici dell'utente (volto o impronta digitale).

Scopo del trattamento

Lo scopo per cui avviene il trattamento dei Suoi dati varia a seconda della categoria di utente a cui Lei appartiene.

Se Lei è un cliente SAET I.S. o ha comunque un rapporto diretto con la nostra organizzazione, il trattamento dei dati può essere funzionale a gestire il rapporto, dalla richiesta di contatto, informazioni o dimostrazioni alla redazione di offerte commerciali, negoziazione e sottoscrizione di accordi contrattuali, fino alla fase di esecuzione dei medesimi.

Se invece lei viene censito da un cliente SAET come utilizzatore di un sistema di controllo accessi/presenze, SAET non ha alcuna facoltà di disposizione dei suoi dati ed opera come responsabile del trattamento, non li utilizza per scopi propri che non siano quelli di garantire la sicurezza della piattaforma informatica ed il suo buon funzionamento, raccogliendo i log di sistema. In tal caso, Lei potrà fare riferimento alle politiche di gestione dei dati dell'organizzazione che l'ha inserita nel proprio sistema di controllo accessi e presenze, e che opera come titolare del trattamento, e che li utilizza per gli scopi da essa stessa individuati.

Base giuridica del trattamento

Anche la base giuridica del trattamento è diversa a seconda del tipo di utente: se Lei è un cliente di SAET, la base giuridica è il consenso da Lei prestato ai sensi dell'art. 6 comma 1 lettera a) GDPR o, a seconda dei casi, art. 9 par. 2 lettera a) GDPR, o ancora le necessità connesse all'esecuzione di un contratto con voi ai sensi dell'Art. 6, lett. B.

Se invece Lei è un utilizzatore finale, censito da uno dei nostri clienti come utente titolare di permessi di accesso in uno stabile dotato di impianti SAET, alcuni dati relativi al Suo utilizzo dell'app vengono salvati in appositi file di log (data e ora dell'accesso, notifica di accesso riuscito, il tipo di dispositivo e la versione del sistema operativo). Queste registrazioni sono funzionali a proteggere la nostra infrastruttura informatica in cloud dagli attacchi, per trovare e correggere gli errori e per monitorare l'utilizzo delle risorse di calcolo e storage (interesse rilevante ai sensi dell'art. 6, comma 1, lett. F GDPR). Le ricordiamo inoltre che alcuni dati sulle operazioni da Lei compiute sono salvati nell'interesse dell'organizzazione che le ha concesso i diritti di accesso al sistema, per verificare la correttezza del Suo operato.

Standard adottati per la protezione dei dati

Cerchiamo sempre di utilizzare i migliori standard di sicurezza disponibili ed adottiamo misure organizzative appropriate per impedire accessi non autorizzati ai dati personali, mantenerne l'accuratezza nel tempo e garantire il corretto utilizzo delle informazioni.

Applichiamo gli stessi criteri anche quando collaboriamo con partner commerciali e tecnologici. Selezioniamo come fornitori di infrastrutture cloud i leader del mercato, che utilizzano misure di sicurezza adeguate e forniscono garanzie sufficienti, comprese le

misure tecniche e organizzative, per assicurare una protezione adeguata dei dati che affidiamo loro.

Tutti i nostri dipendenti e consulenti sono vincolati alla riservatezza dei dati personali di cui vengano a conoscenza nello svolgimento dei loro compiti e adottiamo procedure interne (tra cui la formazione continua) per garantire la sicurezza, la disponibilità e la resilienza dei nostri sistemi e servizi.

[Luogo di conservazione dei dati](#)

Tutti i dati che in qualsiasi modo possono essere visualizzati o raccolti tramite l'app sono salvati nella Region eu-west-1 di AWS (Amazon Web Services), e pertanto fisicamente in Irlanda, eventuali copie dei dati ad uso studio possono risiedere sui nostri server in Italia. Pertanto tutti i dati sono ospitati nell'intero ciclo di trattamento nel territorio dell'Unione Europea.

[Diritti dei titolari dei dati](#)

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione, la limitazione o l'aggiornamento. In taluni casi può essere richiesta la cancellazione o è possibile l'opposizione al loro trattamento oppure la rettificazione ai sensi del Regolamento UE n. 679/2016. Questi diritti tuttavia non sono assoluti: se la conservazione e il trattamento dei dati non è basato sul solo consenso, ma è necessario od obbligatorio anche in relazione all'esecuzione di un contratto o in dipendenza di obblighi normativi, la richiesta di cancellazione potrebbe non essere vincolante. Le richieste di competenza di SAET IS possono essere inviate a info@saet.org