Informazioni sulle privacy policies relative all'uso della piattaforma e app mobile SAET Tebe

Descrizione della soluzione e tipologia dei servizi offerti

SAET Tebe è una mobile app che consente di utilizzare un dispositivo cellulare (purché dotato di tecnologia NFC) per identificare univocamente l'utente all'interno dei sistemi di controllo accessi prodotti da SAET I.S. e connessi alla piattaforma HiCloud Access Control.
Per poter utilizzare l'app pertanto è necessario che Lei sia titolare di un identificativo valido all'interno di un sistema di controllo degli accessi, e che questo identificativo venga associato al suo dispositivo cellulare tramite il recupero di un codice OTP.
I sistemi di controllo accessi sono utilizzati dai proprietari o gestori di immobili per controllare l'accesso di persone e veicoli all'interno degli edifici e delle aree in cui questi sono suddivisi, programmando i permessi di ingresso e utilizzando varchi automatizzati, controllati da apparati programmabili che consentono o no il transito in funzione dell'utente e di altri parametri (come la data, l'ora, ecc.). Il titolare del sistema di controllo accessi potrebbe anche utilizzare i dati relativi agli accessi come riscontro o come base di partenza per una successiva ed autonoma elaborazione dei tempi di permanenza nei plessi aziendali ai fini di individuazione del tempo lavorativo.

Titolarità del trattamento

Come fornitore di sistemi di controllo accessi e delle relative piattaforme di gestione e controllo, SAET I.S. può assumere ai fini del regolamento generale sulla protezione dei dati 2016/679 (di seguito "GDPR") il ruolo di titolare dei dati personali o di responsabile del loro trattamento, a seconda dei casi d'uso e del tipo di soggetto interessato.
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/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, fornendo le proprie credenziali) i dati personali vengono raccolti e caricati a sistema direttamente dai Clienti (che hanno acquistato gli apparati di controllo accessi e li programmano per regolare gli ingressi), 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.
Poiché l'app Tebe consente di utilizzare il proprio apparato cellulare come credenziale per "farsi riconoscere" dai sistemi (e quindi ricevere il consenso all'accesso), normalmente l'utilizzatore di tale app rientra in questa seconda tipologia di utente: pertanto se a Lei è stato concesso di entrare in certi stabili, utilizzando un badge, un dato biometrico o l'app per identificarsi, 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, di ospitalità, ecc.)
In questi casi, il nostro cliente avrà preventivamente raccolto i Suoi dati, acquisendo a vario titolo il consenso al relativo trattamento, avrà fissato (e Le avrà comunicato) gli scopi, così come i mezzi di raccolta dei dati, e li avrà successivamente inseriti nella nostra piattaforma, per digitalizzare e remotizzare la gestione dei permessi.

Tipologia dei dati trattati

Se Lei non ha un rapporto diretto con SAET I.S., affinché possa utilizzare l'app, è necessario che uno dei nostri Clienti, titolare di un immobile in cui Lei ha il diritto di accedere abbia creato per Lei identificativo associato ad uno o più sistemi di identificazione (un badge, un set di dati biometrici,

un identificativo per mobile app Tebe, ecc.). Talvolta, alcuni nostri clienti anonimizzano o pseudonimizzano questi dati (ad esempio stabiliscono che un certo identificativo può accedere ad un immobile, senza associare l'identificativo a nome e cognome). Il sistema è perfettamente compatibile con questa gestione, la quale richiede ovviamente che in un'altra base di dati siano salvate le associazioni tra identificativi e generalità delle persone. Tuttavia più spesso, il responsabile degli accessi inserisce nelle nostre piattaforme (previo valido consenso al trattamento) alcune informazioni relative alle persone che avranno titolo ad entrare. Si tratta di informazioni di base (nome e cognome, indirizzo, numero di telefono, indirizzo email professionale, codice fiscale, ecc.) e altri dati correlati al Suo diritto di accedere negli stabili controllati e permanervi (che sono normalmente correlati alle Sue mansioni, ai Suoi orari e simili. Non vengono invece mai salvati dati relativi alla retribuzione o bancari.
Per garantire la sicurezza degli edifici e delle persone che si trovano all'interno, come anche per agevolare le procedure di evacuazione in caso di calamità ed emergenze, il sistema conserva lo storico di tutti i transiti, con data ora e varco utilizzato: questo archivio consente di localizzare l'identificativo (e quindi normalmente la persona che ne è titolare) come presente o assente dall'edificio o da una sua area circoscritta in un dato momento. Il titolare del trattamento vi avrà, tra l'altro, comunicato per quanto tempo questi dati vengono conservati.
Come si desume da quanto sin qui detto, l'app Tebe consente di utilizzare il dispositivo cellulare per effettuare una timbratura e sbloccare un varco (se autorizzati) effettuando un'operazione che verrà registrata e conservata negli archivi per conto del titolare del sistema di controllo accessi, l'app consente anche all'utente di visualizzare le proprie timbrature in un certo lasso temporale.
Al solo fine di individuare e prevenire malfunzionamenti, 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 versione, indirizzo IP e simili. Queste informazioni vengono utilizzate unicamente a scopo di studio e miglioramento tecnologico.
Anche se ogni timbratura è per sua natura "geolocalizzata" perché il terminale di lettura ed il varco si trovano in un luogo noto, l'app non raccoglie alcuna informazione 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 biomoetrici 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 e utilizza l'app Tebe per farsi riconoscere dagli apparati, 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 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, i suoi transiti sono archiviati per garantire la sicurezza degli stabili, la prevenzione di danni al patrimonio e l'incolumità delle persone, nonché la correttezza del suo operato, nell'interesse dell'organizzazione che Le ha concesso i diritti di accesso all'immobile, la quale definisce la propria politica di trattamento dei dati personali e ne è responsabile. Alcuni dati relativi al Suo utilizzo dell'app Tebe inoltre potrebbero 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).

Standard adottati per la protezione dei dati

Ci impegniamo costantemente per individuare ed 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. A tal fine selezioniamo come fornitori di infrastrutture cloud i leader del mercato, che danno prova di impiegare 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. Normalmente la conservazione e l'elaborazione dei dati contenuti nel sistema di controllo accessi sono indispensabili per consentire agli aventi diritto il regolare passaggio attraverso i varchi controllati dal sistema. Ciò premesso, le richieste di competenza di SAET IS possono essere inviate a info@saet.org