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

Descrizione della piattaforma – Tipologia dei servizi offerti

HiCloud Anti-intrusion è una piattaforma per la gestione ed il controllo centralizzati di diversi sottosistemi di allarme, che può essere utilizzata dagli addetti alla sicurezza e dai security manager per gestire a distanza numerosi e svariati impianti preposti alla sicurezza di edifici siti in località diverse. Grazie all'utilizzo dell'infrastruttura in cloud, il sistema consente di controllare un elevatissimo numero di dispositivi, con immediata evidenza delle anomalie e tempestiva segnalazione delle situazioni che richiedono un intervento. L'app mobile, in particolare, consente di monitorare da remoto, con un dispositivo di telefonia mobile, lo stato dei dispositivi (raggruppati secondo un criterio gerarchico per maggiore sintesi di informazione), di visualizzare lo storico di sistema e le anomalie rilevate, di inviare comandi per interagire con i dispositivi remoti; se sono presenti telecamere di sicurezza, consente altresì di visualizzare i flussi video e di recuperare i filmati registrati in occasione degli allarmi.

Titolarità del trattamento

La piattaforma può essere utilizzata, a diverso titolo, da svariati soggetti, che intrattengono con SAET o con una sua concessionaria un peculiare rapporto, di volta in volta differente. A seconda dei casi d'uso e del tipo di soggetto interessato, ma soprattutto della ragione per cui è concesso l'accesso alla piattaforma, possono variare natura, finalità e fondamento giuridico del trattamento dei dati personali, e può cambiare il ruolo che SAET I.S. assume ai fini del regolamento generale sulla protezione dei dati 2016/679 (di seguito "GDPR").
In particolare la società è Titolare del trattamento dei dati personali relativi alle persone ed enti che intrattengono con essa una relazione diretta, poiché ne sono, ne sono stati o potenzialmente potrebbero diventarne, concessionari, rivenditori autorizzati o clienti, ad esempio acquisendo uno o più sistemi di allarme e/o la licenza per l'uso della piattaforma software, in relazione all'esecuzione del singolo contratto in questione e per la gestione del rapporto derivante.
I titolari di licenza Hicloud, possono poi, a loro volta, censire all'interno del sistema, come utenti dello stesso, i propri collaboratori e dipendenti, o qualsiasi persona cui intendono fornire l'accesso all'interfaccia di gestione centralizzata degli allarmi, senza che SAET I.S. abbia alcun rapporto o contatto con i soggetti interessati. In questo caso il trattamento da parte nostra dei dati avviene esclusivamente per conto del cliente che li ha inseriti, il quale di norma sarà il titolare di uno o più immobili, dei relativi impianti di sicurezza e delle informazioni relative alle persone a cui ha concesso il diritto di utilizzo della piattaforma.
Pertanto, se Le sono state fornite dal titolare di una licenza Hicloud le credenziali per l'utilizzo del portale e dell'app, noi agiamo esclusivamente come responsabili del trattamento dei Suoi dati, che sono stati raccolti dal proprietario dell'impianto di sicurezza, in esecuzione del rapporto che intrattenete con lui (di lavoro, di consulenza, ecc.).
In questo caso è il cliente di Hicloud che ha preventivamente raccolto i Suoi dati, acquisendo a vario titolo il consenso al relativo trattamento, ha fissato (e Le ha comunicato) gli scopi, così come i mezzi di raccolta dei dati, e li ha successivamente inseriti nella nostra piattaforma, creando il Suo profilo utente.

Tipologia dei dati trattati

Come si è visto, 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 una licenza per l'uso di HIcloud, e solitamente di uno o più impianti di sicurezza, abbia creato per Lei un account Utente.
La creazione di un nuovo utente richiede unicamente l'inserimento di un indirizzo email valido, al

quale il sistema invierà un link per la registrazione. In sede di registrazione vengono richieste al nuovo utente alcune informazioni di base (nome e cognome, numero di telefono, ecc.).
L'accettazione dell'invito implica il Suo l'assenso al trattamento dei Suoi dati da parte del mittente dell'invito.
Viene anche chiesto di creare (e confermare) una password da utilizzare per l'autenticazione dell'accesso: la password viene salvata in forma criptata e nessuno, né appartenente a SAET, né alla sua rete commerciale, né all'organizzazione del cliente, può conoscerla.
Durante l'utilizzo, e quindi ad avvenuto login, per garantire la sicurezza degli stabili e il corretto funzionamento degli impianti, ma anche per scongiurare usi dannosi ed infedeli dell'applicativo, viene salvato il log di tutti i comandi inviati dall'utente. A parte questo, l'app di HiCloud Antintrusion non consente di raccogliere, inserire, visualizzare, editare o comunque trattare dati personali dell'utente, ma si limita a consentire il controllo da remoto degli apparati elettronici. Se tra i dispositivi controllati vi sono delle telecamere, l'interfaccia può consentire la visualizzazione dei relativi flussi video, acquisiti in tempo reale, o memorizzati in concomitanza degli allarmi. Le immagini catturate da una telecamera possono ovviamente contenere informazioni riconducibili al concetto di dati personali, ma la loro acquisizione e memorizzazione non è connessa all'utilizzo dell'app o del sito web, quanto piuttosto all'installazione dell'apparato e alla sua interconnessione al cloud. Tutte le informazioni relative al trattamento di dati personali connesse all'utilizzo di telecamere pertanto vengono fornite per l'accettazione nel momento della posa in opera.
L'installatore cura altresì la posa della dovuta segnaletica in corrispondenza delle aree soggette in qualsiasi modo a ripresa.
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 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 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 è stato invitato dal titolare di una licenza di Hicloud come utente del proprio sistema di centralizzazione e telegestione degli allarmi, SAET non ha alcuna facoltà di disporre 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, con particolare riguardo ai login e all'invio di comandi che possono impattare sul livello di sicurezza degli impianti. In tal caso, Lei potrà fare riferimento alle politiche di gestione dei dati dell'organizzazione che le ha concesso il diritto di accesso, invitandola ad utilizzare la piattaforma, 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 ed è stato invitato da un cliente Hicloud ad utilizzare la piattaforma, come operatore autorizzato alla gestione di funzioni relative alla sicurezza degli stabili, 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, a 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 compentenza di SAET IS possono essere inviate a info@saet.org