Whitepaper | Marzo 2023

Informazioni dormakaba sulla protezione dei dati per la soluzione cloud resivo.

Protezione dei dati resivo

dormakaba

Dichiarazione d'intenti in materia di protezione dei dati

I nostri principi in materia di trattamento dei dati (conformità al RGPD)
Il Regolamento generale sulla protezione dei dati (RGPD) è stato emanato dall'Unione Europea per garantire la protezione delle persone fisiche in materia di trattamento dei dati personali all'interno del territorio europeo. Con la conformità al RGPD, dormakaba rispetta anche l'art. 6 della legge federale tedesca in materia di dati personali (BDSG) e la legge federale svizzera in materia di protezione dei dati (DSG). dormakaba soddisfa i requisiti della base giuridica in conformità con la giurisprudenza senza eccezioni.

Accordo sul trattamento dell'ordine
L'incarico al trattamento dei dati tra i clienti e dormakaba viene fissato per iscritto nell'accordo sul trattamento dell'ordine (tale accordo è parte integrante del contratto SaaS dormakaba).
Il trattamento si riferisce alla fornitura dei servizi nell'ambito del contratto. L'addetto al trattamento dell'ordine (dormakaba) non può trattare i dati personali dei clienti per scopi propri o inoltrarli a terzi.

Organizzazione dormakaba
Per proteggere i vostri dati

Misure tecniche e organizzative
dormakaba (addetto al trattamento dell'ordine) adotta delle misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio.

a) Riservatezza
- Controllo fisico degli accessi: Protezione contro l'accesso non autorizzato al sistema di trattamento dei dati. Impiego di sistemi di controllo fisico degli accessi, ad es. chip card, chiavi, apriporta elettrici, servizio di sicurezza, impianti di allarme, videosorveglianza, documentazione di visitatori e consegna di schede ID visitatore.
- Controllo dell'accesso al sistema: Protezione contro l'utilizzo non autorizzato di un sistema. Utilizzo di direttive utente per l'assegnazione di password, formazione in materia di direttive sulla sicurezza.
- Controllo degli accessi ai dati: Protezione contro accesso, lettura, copia, modifica o rimozione non autorizzati dei dati all'interno del sistema. Impiego di concetti di autorizzazione e di diritti d'accesso on demand, registrazione dell'accesso, considerazione del principio Need to know (minimizzazione dei dati).
- Controllo di separazione: elaborazione separata dei dati personali rilasciati o richiesti per diversi motivi.
- Pseudonimizzazione: Se lo scopo dell'elaborazione lo consente, l'elaborazione dei dati personali avviene in modo che i dati senza richiesta di informazioni aggiuntive non possano essere assegnati a più di una determinata persona.

b) Integrità
- Controllo di trasferimento, impossibilità di lettura, copia, modifica o rimozione non autorizzati in caso di trasferimento elettronico. Utilizzo di sistemi di controllo trasferimento, ad es. e-mail criptate. Reti private virtuali (VPN), trasferimenti al fornitore di servizi con crittografia SSL; firma elettronica.
- Controllo di immissione: Controlli che permettono di visualizzare se e chi ha immesso, modificato o rimosso dei dati personali nei sistemi di trattamento dei dati (ad es. con l'impiego di un sistema di gestione dei documenti).

c) Disponibilità e resistenza
- Controllo di disponibilità: Protezione contro la cancellazione intenzionale o non intenzionale, ad es. tramite piani di emergenza, strategie di back up, gruppo di continuità, protezione antivirus, firewall, regolari test di penetrazione di sicurezza dell'infrastruttura, gestione della sicurezza delle informazioni.
- Rapido ripristino della disponibilità e dell'accesso ai dati personali, ad es. tramite salvataggio ad alta ridondanza dei dati personali, utilizzo di una gestione patch di sicurezza centralizzata.

d) Processo per la regolare verifica, analisi e valutazione delle TOM
- Gestione della protezione dei dati a livello dell'intera azienda, ruoli e responsabilità definiti per responsabili della protezione dei dati, coordinatori e manager.
- Gestione dell'ordine: Non avviene alcun trattamento dei dati nell'ordine del cliente senza esplicite istruzioni del cliente, ad es. chiara realizzazione del contratto, gestione dell'ordine formalizzata, selezione accurata di fornitori di servizi, obbligo di verifica e controlli successivi.

FAQ: dati personali raccolti da resivo

Da chi vengono salvati e trattati i dati?
Dipendenti dell'amministrazione dell'edificio che utilizzano resivo. Inquilini di un immobile in locazione all'interno di un edificio dotato di resivo.

Quali dati vengono salvati e trattati?
Dipendenti dell'amministrazione dell'edificio: i dipendenti dell'amministrazione dell'edificio utilizzano il portale admin resivo e l'app utility resivo. L'utente può accedere a entrambe le applicazioni dopo una normale registrazione.

Per la registrazione sono necessari (dati modello):
- nome e cognome
- indirizzo e-mail (indirizzo e-mail aziendale).

Per poter visualizzare i nomi dei dipendenti, viene richiesta l'autorizzazione a effettuare il login al sistema resivo. Inoltre, le attività dei dipendenti vengono salvate in un log di modifica per 180 giorni per il tracciamento delle modifiche. Vengono salvate le attività eseguibili nel portale admin resivo e nell'app utility (ad es. processo di ingresso, generazione di una chiave, ecc.). In conformità con "Privacy by Design" (la protezione dei dati è già tecnicamente integrata nelle procedure di trattamento dei dati), i dati non possono essere estratti e vengono cancellati automaticamente dopo 180 giorni.

Informazioni degli inquilini:
in linea di massima, le informazioni necessarie vengono create preservando la privacy. Questo significa che si possono inserire nel sistema resivo solo le informazioni degli inquilini importanti dal punto di vista tecnico per il sistema.

Informazioni concrete degli inquilini (dati modello):
- nome e cognome
- collegamento all'immobile in locazione interessato
- indirizzo e-mail e/o numero di telefono dell'inquilino
- inizio del rapporto di locazione
- fine del rapporto di locazione
- supporti di accesso dell'inquilino

Altre informazioni degli inquilini
(opzionale e scelta informata dell'impresa edile):
- informazioni d'accesso dell'inquilino alle porte comuni (log di accesso)

Per design, le informazioni degli inquilini sono visibili agli utenti selezionati del portale admin resivo che
a) hanno l'autorizzazione d'accesso per questo edificio e
b) hanno l'autorizzazione di ruolo per la visualizzazione delle informazioni degli inquilini (ruolo: gestione inquilini).

Le informazioni degli inquilini non sono più visibili all'amministrazione dell'edificio dopo il processo di uscita. Solo il log d'accesso delle porte comuni può contenere le informazioni degli inquilini degli ultimi 90 giorni. Per design, il log d'accesso è visibile agli utenti del portale admin resivo che a) hanno l'autorizzazione d'accesso a questo edificio e b) l'autorizzazione dei ruoli alla visualizzazione del log d'accesso (ruolo: log d'accesso).

Per quanto tempo vengono salvati i dati?
- Dati modello dei dipendenti dell'amministrazione dell'edificio: fino a quando l'utente attivo viene cancellato
- Log di modifica: 180 giorni
- Dati modello informazioni degli inquilini: cancellati direttamente dopo l'uscita
- Informazioni d'accesso: dopo 90 giorni

Misure di dormakaba per la protezione delle proprie informazioni degli inquilini e dei loro dati

- Sistema utente basato su ruoli
- Nessuna possibilità di estrazione per design
- Cancellazione di default dei dati non più importanti (uscita, intervallo di 90 giorni, intervallo di 180 giorni)
- Login protetto da password
- Area clienti chiusa: l'accesso dal sistema può essere assegnato solo al cliente (anche per il supporto dipendenti dormakaba, dipendenti di vendita dormakaba, gestione prodotti dormakaba ma anche per partner di installazione e supporto)
- Accesso ridotto alla banca dati: solo un numero molto ristretto di dipendenti dormakaba (sviluppo), soggetti a uno specifico accordo di protezione dei dati e di riservatezza.
- Sicurezza delle informazioni. Dormakaba e il centro informatico utilizzato per dormakaba è certificato secondo la norma ISO 27001. Così si proteggono i dati personali dei clienti e dei loro dipendenti. La certificazione viene garantita per la durata del contratto.

Funzioni di sicurezza all'interno del prodotto

Autenticazione e password:

- Login (autenticazione a due fattori: per aumentare la sicurezza, agli utenti che si registrano con il software SaaS viene offerta la possibilità di attivare l'autenticazione a due fattori per il proprio account).
  - Crittografia: qualsiasi comunicazione su reti pubbliche dell'app resivo di dormakaba è crittografata e protetta da HTTPS con Transport Layer Security (AES 128 GCM SHA 256, chiavi a 128 bit, TLS 1.3 con PFS). Significa che qualsiasi trasferimento dei dati avviene esclusivamente in maniera criptata.

- Forza della password: gli utenti resivo (inquilini e dipendenti delle amministrazioni) possono assegnare password con almeno 8 caratteri e con almeno un carattere maiuscolo, un carattere minuscolo, un carattere speciale e un numero.

Ruoli degli utenti e concetto dei diritti

- Per l'utilizzo dell'app utility resivo e del portale admin resivo ci sono diversi ruoli utente e un concetto di diritti. Una, alcune o tutte le seguenti autorizzazioni possono essere assegnate all'utente:
  - Gestione utenti: creazione, aggiunta e cancellazione dell'utente. Assegnazione o revoca delle autorizzazioni. Consigliata a utenti che devono acquisire il ruolo di Amministratore app o Superiore nell'amministrazione dell'edificio.
  - Amministrazione dell'edificio: con questa autorizzazione è possibile aggiungere, modificare o cancellare edifici, immobili in locazione o porte degli immobili in locazione.
  - Gestione accessi: aggiunta della chiave generale o dell'accesso di ospiti, apertura di porte comuni tramite apertura a distanza.
  - Gestione inquilini: creazione, ingresso e uscita inquilino, invito all'app resivo home. Adatta per persone che si occupano di gestione degli inquilini.
  - Gestione dei componenti: creazione, manutenzione (sostituzione delle batterie, aggiornamento del firmware) e cancellazione di porte comuni. Adatto a utenti che forniscono servizi di messa in funzione, manutenzione e assistenza.

Gestione delle informazioni e delle comunicazioni:

- notifiche push, notifiche per SMS e/o e-mail nel caso in cui si aggiungano nuovi inquilini e si riceva l'accesso a un immobile in locazione
- notifiche per SMS e/o e-mail nel caso in cui venga richiesto l'accesso a un immobile in locazione

Protocolli:

- log d'accesso, descrizione, vedere contratto SaaS
- storico dei log (log di modifica)

dormakaba resivo

resivo di dormakaba è un sistema di gestione degli accessi basato sul cloud, con lo sguardo rivolto al futuro. È in grado di offrire agli amministratori, ai proprietari di casa e agli inquilini notevoli vantaggi rispetto ai cilindri di sicurezza e ai piani di chiusura tradizionali. Non occorre più preoccuparsi per le chiavi perse o sottratte. La consegna degli appartamenti diventa più semplice e comoda per gli inquilini. resivo permette di risparmiare tempo grazie a processi più semplici all'assegnazione dei diritti di accesso per fornitori, fornitori di servizi e artigiani. Sono i residenti stessi a stabilire chi ha accesso al loro appartamento e quando – anche a distanza. Con resivo si inaugura una dimensione dell'utilizzo degli edifici completamente nuova e ricca di vantaggi.

Accessori e
prodotti per porte

Controllo accessi
e raccolta dati

Cilindri di sicurezza
e piani di chiusura

Prodotti e soluzioni
per Hotel

Porte e varchi
automatici

Servizi

Avete domande? Saremo lieti di offrirvi consulenza, vi aspettiamo.

Visit us:

resivo.dormakaba.com

IT, 03/2023
Con riserva di modifiche tecniche

dormakaba.com

dormakaba
Italia S.r.l.
IT-Milano (MI)
T +39 02 494842

IT-Castel Maggiore (BO)
T +39 051 4178311

info.it@dormakaba.com
dormakaba.it

dormakaba
Schweiz AG
Lerchentalstrasse 2a
CH-9016 St. Gallen
T +41 848 85 86 87
info.ch@dormakaba.com
dormakaba.ch