Papier blanc | Mars 2023

Informations dormakaba sur la protection des données pour la solution cloud resivo.

Protection des données resivo

dormakaba

Déclaration d'engagement pour la protection des données

Nos principes de traitement de données (conformité avec le RGPD)
Le règlement général sur la protection des données (RGPD) a été adopté par l'Union européenne afin d'assurer la protection des personnes physiques au sein de l'Europe dans le cadre du traitement de données à caractère personnel. En étant en conformité avec le RGPD, dormakaba est également en conformité avec la loi fédérale allemande sur la protection des données 6 (BDSG) et à la loi fédérale suisse sur la protection des données (LPD). dormakaba respecte sans exception les prescriptions des bases légales en l'état de la jurisprudence.

Accord de traitement des commandes (« AVV »)
La commande pour le traitement des données entre le client et dormakaba est convenue par écrit dans le contrat de traitement des commandes (celui-ci fait partie du contrat dormakaba SaaS). Le traitement se rapporte à la fourniture des services dans le cadre du contrat. Le sous-traitant (dormakaba) ne peut pas traiter les données à caractère personnel du client à ses propres fins, ni les transmettre à des tiers.

Organisation dormakaba

Pour protéger vos données de manière sécurisée

Mesures techniques et organisationnelles
dormakaba (sous-traitant) prend des mesures techniques et organisationnelles afin de garantir un niveau de sécurité adapté aux risques.

a) Confidentialité

- Contrôle d'accès physique : protection contre l'accès non autorisé aux systèmes de traitement des données. Utilisation de systèmes de contrôle d'accès physique, par ex. cartes à puce, clés, ouvre-portes électriques, service de garde, systèmes d'alarme, vidéosurveillance, documentation des visiteurs et remise de badges visiteurs.
- Contrôle d'accès au système : protection contre l'utilisation non autorisée d'un système. Utilisation de directives utilisateur pour l'attribution de mots de passe, instruction sur les stratégies de sécurité.
- Contrôle d'accès aux données : protection contre l'accès non autorisé, la lecture, la copie, la modification ou la suppression non autorisés de données au sein du système. Utilisation de concepts d'autorisation et de droits d'accès à la demande, journalisation des accès, prise en compte du principe du besoin d'en connaître (économie des données).
- Contrôle de séparation : traitement séparé de données à caractère personnel mises à disposition ou collectées à des fins différentes.
- Pseudonymisation : le traitement des données à caractère personnel est effectué, dans la mesure où le but du traitement l'autorise, de manière à ce que les données ne puissent plus être attribuées à une personne concernée spécifique, sans avoir recours à des informations supplémentaires.

b) Intégrité

- Contrôle de la transmission : pas de lecture, de copie, de modification ou de suppression non autorisée lors de la transmission électronique. Utilisation de systèmes de contrôle de la transmission, p. ex. cryptage des e-mails. Réseaux privés virtuels (VPN), transmissions cryptées SSL aux fournisseurs de services ; signature électronique.
- Contrôle de saisie : contrôles qui permettent de retracer si des saisies, des modifications, des suppressions de données à caractère personnel ont été effectuées et par qui dans les systèmes de traitement des données (par ex. en utilisant un système de gestion de documents).

c) Disponibilité et résistance

- Contrôle des disponibilités : protection contre la destruction ou la perte accidentelle ou intentionnelle, par ex. grâce à des plans d'urgence, d'une stratégie de sauvegarde, d'une alimentation en tension sans interruption (UPS), d'une protection antivirus, d'un pare-feu, de tests de pénétration réguliers de la sécurité de l'infrastructure, d'une gestion de la sécurité de l'information.
- Rétablissement rapide de la disponibilité et de l'accès aux données à caractère personnel, par exemple en stockant les données personnelles de manière hautement redondante, en utilisant une gestion centralisée des correctifs de sécurité.

d) Procédures permettant de vérifier, d'apprécier et d'évaluer régulièrement les TOMs

- Gestion de la protection des données à l'échelle du groupe, rôles et responsabilités définis pour les délégués à la protection des données, les coordinateurs et les responsables.
- Gestion des commandes : aucun traitement de données n'est effectué pour le compte du client, sans instructions correspondantes de la part de ce dernier, par ex. grâce à une conception claire des contrats, d'une gestion formalisée des commandes, d'une sélection minutieuse des prestataires de services, d'une obligation de vérification et d'inspections de suivi ultérieurs.

FAQ : données des personnes collectées dans resivo

Qui enregistre et traite les données ?
Collaborateur de la gestion du bâtiment utilisant resivo.
Locataire d'un bien locatif se trouvant dans un bâtiment équipé de resivo.

Quelles sont les données enregistrées et traitées ?
Collaborateurs de la gestion du bâtiment : les collaborateurs de la gestion du bâtiment utilisent resivo admin portal et resivo utility app. Les deux applications sont accessibles à l'utilisateur après un enregistrement en bonne et due forme.

Cet enregistrement nécessite (données de base) :
- Prénom et nom
- Adresse e-mail (adresse e-mail professionnelle).

Afin de pouvoir visualiser les noms des collaborateurs, il faut disposer d'une autorisation pour se connecter au système resivo. Par ailleurs, les activités des collaborateurs sont enregistrées dans un journal des modifications pendant 180 jours. Ce qui a pour but d'assurer le suivi des modifications. Les activités pouvant être effectuées dans resivo admin portal et dans l'application utility app (par exemple, processus d'emménagement, création d'une clé, etc.) sont enregistrées. Conformément à « Privacy by Design » (la protection des données est déjà intégrée au niveau technique dans le processus de traitement des données), il n'est pas possible d'extraire les données et elles seront automatiquement effacées après 180 jours.

Informations sur les locataires :
Les informations nécessaires sont généralement créées en respectant la protection des données. Ce qui signifie que seules les informations sur les locataires pertinentes pour le système peuvent être saisies dans le système resivo.

Informations concrètes sur les locataires (données de base) :
- Nom et prénom
- Lien vers le bien locatif en question
- Adresse e-mail et/ou numéro de téléphone mobile du locataire
- Début du bail
- Fin de bail
- Médias d'accès du locataire

Plus d'informations sur les locataires
(facultatives et choix délibéré de la société de logement) :
- Informations d'accès du locataire aux portes communes (journal d'accès)

Les informations sur les locataires peuvent être visualisées de par leur conception pour les utilisateurs sélectionnés de resivo admin portal qui
a) disposent d'une autorisation d'accès pour ce bâtiment et
b) ont une autorisation de rôle pour consulter des informations sur les locataires (rôle : gestion des locataires).

Les informations sur les locataires ne peuvent plus être consultées par la gestion du bâtiment après le processus de déménagement. Le journal d'accès des portes communes est le seul à pouvoir encore contenir des informations sur les locataires des 90 derniers jours. De par sa conception, le journal d'accès peut être consulté pour les utilisateurs de resivo admin portal qui a) disposent d'une autorisation d'accès pour ce bâtiment et b) possèdent l'autorisation de rôle pour consulter le journal d'accès (rôle : journal d'accès).

Combien de temps les données sont-elles conservées ?
- Données de base des collaborateurs de la gestion du bâtiment : aussi longtemps que l'utilisateur n'est pas activement supprimé
- Journal des modifications : 180 jours
- Données de base informations sur les locataires : supprimées immédiatement après le déménagement
- Informations d'accès : après 90 jours

Mesures grâce auxquelles dormakaba protège ses informations et les données de ses locataires

- Système d'utilisateurs selon les rôles
- Aucune option d'extraction par conception
- Suppression des données par défaut, lorsque celles-ci ne sont plus pertinentes (déménagement, intervalle de 90 jours, intervalle de 180 jours)
- Connexion protégée par mot de passe
- Espace client fermé
  - Un accès au système peut uniquement être attribué au client (également aux collaborateurs du support dormakaba, aux équipes de vente dormakaba, à la gestion des produits dormakaba ou encore aux partenaires d'installation et de support)
- Accès réduit à la base de données – uniquement un nombre très limité de collaborateurs dormakaba (développement) qui sont soumis à un accord spécial de protection des données et de confidentialité.
- Sécurité des informations. dormakaba et le centre de données hébergeant les systèmes dormakaba sont certifiés ISO 27001. Ce qui permet de protéger les données à caractère personnel des clients et de leurs collaborateurs. La certification est maintenue pendant la durée du contrat.

Fonctions de sécurité contenues dans le produit :

Authentification et mots de passe :

- Connexion (authentification à deux facteurs. Les utilisateurs qui se connectent au logiciel SaaS ont la possibilité d'activer une authentification à deux facteurs sur leur compte pour renforcer la sécurité).
  - Cryptage Toute communication des applications dormakaba resivo via des réseaux publics est cryptée et protégée par HTTPS avec Transport Layer Security (AES 128 GCM SHA 256, 128 bit keys, TLS 1.3 avec PFS). C'est-à-dire que toute transmission de données se fait exclusivement de manière cryptée.

- Force du mot de passe – les utilisateurs resivo (locataires et collaborateurs de l'administration) ne peuvent attribuer que des mots de passe d'au moins 8 caractères et comportant chacun au moins une lettre majuscule, une lettre minuscule, un caractère spécial et un chiffre.

Rôles d'utilisateur et concepts de droits

- Il existe différents rôles d'utilisateur et un concept de droits pour l'utilisation de l'application resivo utility app ainsi que pour le portail resivo admin portal. Une, plusieurs ou toutes les autorisations suivantes peuvent être attribuées à un utilisateur :
  - Gestion des utilisateurs : créer, ajouter et effacer des utilisateurs. Attribuer ou retirer des autorisations. Recommandé pour les utilisateurs qui doivent assumer le rôle d'administrateur de l'application ou le rôle de superviseur au sein de la gestion du bâtiment.
  - Gestion du bâtiment : cette autorisation permet d'ajouter, de modifier ou de supprimer des bâtiments, des biens locatifs et des portes de biens locatifs.
  - Gestion des accès : ajouter une clé générale ou un accès invité, ouvrir des portes communes grâce à l'ouverture à distance.
  - Gestion des locataires : créer des locataires, emménager et déménager, invitation à l'application resivo home app. Convient aux personnes qui s'occupent de la gestion des locataires.
  - Gestion des composants : créer, entretenir (changement de batterie, mise à jour du microprogramme) et supprimer des portes communes. Convient aux utilisateurs qui assurent la mise en service, les travaux de maintenance et le support.

Gestion des informations et de la communication :

- notification push, notifications par SMS et/ou par e-mail lorsque de nouveaux résidents sont ajoutés et obtiennent l'accès à un bien locatif
- Notifications par SMS et/ou par e-mail lorsqu'un accès à un bien locatif est demandé

Protocoles :

- Journal d'accès, description voir contrat SaaS
- Journal d'historique (journal des modifications)

dormakaba resivo

resivo de dormakaba est un système de gestion des accès basé sur le cloud et orienté vers l'avenir. Il offre ainsi aux administrations, aux propriétaires et aux locataires des avantages significatifs par rapport aux systèmes de fermeture mécaniques conventionnels. Il n'y a pas lieu de s'inquiéter des clés perdues ou volées. Les remises d'appartements deviennent plus faciles et moins compliquées pour les locataires. resivo permet de gagner du temps grâce à la simplification des procédures d'attribution d'accès aux fournisseurs, aux prestataires de services et aux artisans. Les résidents décident eux-mêmes qui a accès à l'appartement et quand – même à distance. resivo ouvre une toute nouvelle dimension offrant de nombreux avantages pour l'utilisation des bâtiments.

Ferme-portes et verrouillages

Contrôle d'accès et gestion des temps

Cylindres sur organigrammes

Serrures de gestion hôtelières

Portes automatiques et obstacles physiques

Service

Avez-vous des questions ? Nous serons heureux de vous conseiller.

Visit us:

resivo.dormakaba.com

FR, 03/2023
Sous réserve de modifications techniques

dormakaba
Belgium N.V.
Monnikenwerve 17-19
BE-8000 Brugge
T +32 50 45 15 70
info.be@dormakaba.com
dormakaba.be

dormakaba
Luxembourg SA
Duchscherstrooss 50
LU-6868 Wecker
T +352 26710870
info.lu@dormakaba.com
dormakaba.lu

dormakaba
France S.A.S.
2-4 rue des Sarrazins
FR-94046 Créteil cedex
T +33 1 41 94 24 00
marketing.fr@dormakaba.com
dormakaba.fr

dormakaba
Suisse SA
Chemin de Budron A5
CH-1052 Le Mont-sur-Lausanne
T +41 848 85 86 87
info.ch@dormakaba.com
dormakaba.ch

dormakaba.com