Whitepaper | März 2023

dormakaba Informationen zum Datenschutz bei der Cloud-Lösung resivo.

resivo Datenschutz

dormakaba

Verpflichtungs-erklärung zum Datenschutz

Unsere Grundsätze der Datenverarbeitung (DSGVO Konformität)
Die Datenschutz-Grundverordnung (DSGVO) wurde von der Europäischen Union erlassen, um innerhalb Europas den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sicherzustellen. Mit der Konformität zur DSGVO ist dormakaba auch zum deutschen Bundesdatenschutzgesetz 6 (BDSG) und zum Schweizer Bundesgesetz über den Datenschutz (DSG) konform. dormakaba hält die Vorgaben der Gesetzesgrundlagen auf dem Stand der Rechtsprechung ausnahmslos ein.

Auftragsverarbeitungsvereinbarung ("AVV")
Die Beauftragung zur Verarbeitung der Daten zwischen Kunden und dormakaba wird im Auftrags-verarbeitungs-Vertrag (AVV Vertrag ist Teil des dormakaba SaaS Vertrags) schriftlich fixiert. Die Verarbeitung bezieht sich auf die Erbringung der Dienste im Rahmen des Vertrags. Der Auftrags-verarbeiter (dormakaba) darf die personenbezo-genen Kundendaten nicht für eigene Zwecke ver-arbeiten oder an Dritte weitergeben.

Organisation dormakaba
Um Ihre Daten sicher zu schützen

Technische und organisatorische Maßnahmen
dormakaba (Auftragsverarbeiter) ergreift technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten.

a) Vertraulichkeit
- Physische Zugangskontrolle: Schutz vor unbefugtem Zugang zu Datenverarbeitungssystemen. Einsatz von physischen Zugangskontrollsystemen, z.B. Chipkarten, Schlüssel, elektrische Türöffner, Wachdienst, Alarmanlagen, Videoüberwachung, Dokumentation von Besuchern und Ausgabe von Besucherausweisen.
- Systemzugangskontrolle: Schutz vor unbefugter Nutzung eines Systems. Verwendung von Benutzerrichtlinien für die Zuweisung von Passwörtern, Unterweisung in Sicherheitsrichtlinien.
- Datenzugriffskontrolle: Schutz vor unbefugtem Zugriff, Lesen, Kopieren, Verändern oder Entfernen von Daten innerhalb des Systems. Einsatz von Berechtigungskonzepten und On-Demand-Zugriffsrechten, Protokollierung des Zugriffs, Berücksichtigung des Need-to-know-Prinzips (Datensparsamkeit).
- Trennungskontrolle: getrennte Verarbeitung personenbezogener Daten, die für unterschiedliche Zwecke bereitgestellt oder erhoben wurden.
- Pseudonymisierung: Die Verarbeitung personenbezogener Daten erfolgt, soweit der Zweck der Verarbeitung dies zulässt, in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können.

b) Integrität
- Übertragungskontrolle: kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übermittlung. Verwendung von Übertragungskontrollsystemen, z. B. E-Mail-Verschlüsselung. Virtuelle Private Netzwerke (VPN), SSL-verschlüsselte Übertragungen an Dienstanbieter; elektronische Signatur.
- Eingabekontrolle: Kontrollen, die es ermöglichen, nachzuvollziehen, ob und wer personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder entfernt hat (z. B. durch den Einsatz eines Dokumentenmanagementsystems).

c) Verfügbarkeit und Widerstandsfähigkeit
- Verfügbarkeitskontrolle: Schutz vor versehentlicher oder absichtlicher Zerstörung oder Verlust, z. B. durch Notfallpläne, Back-up-Strategie, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, regelmäßige Penetrationstests der Infrastruktursicherheit, Informationssicherheitsmanagement.
- Rasche Wiederherstellung der Verfügbarkeit und des Zugriffs auf personenbezogene Daten, z. B. durch hochredundante Speicherung personenbezogener Daten, Verwendung eines zentralisierten Sicherheits-Patch-Managements.

d) Verfahren für die regelmäßige Prüfung, Bewertung und Evaluierung der TOMs
- Konzernweites Datenschutzmanagement, definierte Rollen und Verantwortlichkeiten für Datenschutzbeauftragte, Koordinatoren und Manager.
- Auftragsmanagement: Es erfolgt keine Datenverarbeitung im Auftrag des Kunden ohne entsprechende Weisungen des Kunden, z. B. durch klare Vertragsgestaltung, formalisiertes Auftragsmanagement, sorgfältige Auswahl von Dienstleistern, Prüfpflicht und Nachkontrollen.

Whitepaper März 2023

FAQ: Gesammelte Personendaten in resivo

Von wem werden Daten gespeichert und verarbeitet?
Mitarbeiter der Gebäudeverwaltung, die resivo nutzen. Mieter eines Mietobjektes, welches sich in einem mit resivo ausgestatteten Gebäude befindet.

Welche Daten werden gespeichert und verarbeitet?
Mitarbeiter der Gebäudeverwaltung: Die Mitarbeiter der Gebäudeverwaltung verwenden das resivo admin portal sowie die resivo utility app. Beide Applikationen sind dem Benutzer nach einer ordentlichen Registrierung zugänglich.

Diese Registrierung erfordert (Stammdaten):
- Vorname und Nachname
- Email-Adresse (geschäftliche Email-Adresse).

Um die Namen der Mitarbeiter einsehen zu können, bedarf es einer Berechtigung, sich ins resivo System einloggen zu können. Weiter werden die Tätigkeiten der Mitarbeiter in einen Änderungslog für 180 Tagen gespeichert. Dies soll dazu dienen, damit Änderungen nachverfolgt werden können. Es werden die Tätigkeiten gespeichert, die im resivo admin portal und in der utility app durchführbar sind (beispielsweise Einzugsprozess, Erstellung eines Schlüssels, etc. Gemäß «Privacy by Design» (Datenschutz ist bei Datenverarbeitungsvorgängen bereits technisch intergriert) können die Daten nicht extrahiert werden und werden automatisch nach 180 Tagen gelöscht.

Mieterinformationen:
Die benötigten Informationen werden grundsätzlich datenschutzfreundlich erstellt. Dies bedeutet, dass nur systemtechnisch relevante Mieterinformationen in das resivo System eingegeben werden können.

Konkrete Mieterinformationen (Stammdaten):
- Vor- und Nachname
- Verlinkung zu dem betroffenen Mietobjekt
- Email-Adresse und / oder mobile Telefonnummer des Mieters
- Start des Mietverhältnisses
- Ende des Mietverhältnisses
- Zutrittsmedien des Mieters

Weitere Mieterinformationen
(optional und bewusster Entscheid der Wohnbaugesellschaft):
- Zutrittsinformationen des Mieters an Gemeinschaftstüren (Zutrittslog)

Die Mieterinformationen sind per Design für ausgewählte resivo admin portal Nutzer ersichtlich, welche
a) die Zugriffsberechtigung für dieses Gebäude haben und
b) die Rollenberechtigung für das Einsehen von Mieterinformationen haben (Rolle: Mieterverwaltung).

Die Mieterinformationen sind nach dem Auszugsprozess für die Gebäudeverwaltung nicht mehr ersichtlich. Lediglich das Zutrittslog der Gemeinschaftstüren kann noch Mieterinformationen der letzten 90 Tage beinhalten. Das Zutrittslog ist per Design für resivo admin portal Nutzer einsehbar, welche a) die Zugriffsberechtigung für dieses Gebäude haben und b) die Rollenberechtigung für das Einsehen des Zutrittslogs haben (Rolle: Zutrittslog).

Wie lange werden die Daten gespeichert?
- Stammdaten der Mitarbeiter der Gebäudeverwaltung: so lange bis der User aktiv gelöscht wird
- Änderungslog: 180 Tage
- Stammdaten Mieterinformationen: direkt nach dem Auszug gelöscht
- Zutrittsinformationen: nach 90 Tagen

Maßnahmen, mit denen dormakaba ihre Mieter-informationen und ihre Daten schützt

- Rollenbasiertes Nutzersystem
- Per Design keine Extrahierungsmöglichkeiten
- Per Default Löschung der Daten, wenn nicht mehr relevant (Auszug, 90 Tage-Intervall, 180-Tage Intervall)
- passwortgeschützter Login
- Geschlossener Kundenbereich
  - Zugriff vom System kann ausschliesslich für den Kunden vergeben werden (auch für dormakaba Support Mitarbeiter, dormakaba Verkaufsmitarbeiter, dormakaba Produkt Management oder aber auch für Installations- und Supportpartner)
- Reduzierter Zugriff auf die Datenbank – nur eine sehr limitierte Anzahl an dormakaba Mitarbeitern (Entwicklung), die einer speziellen Datenschutz- und Vertraulichkeitsvereinbarung unterliegen.
- Informationssicherheit. Dormakaba und das für dormakaba genutzte Rechenzentrum ist ISO 27001- zertifiziert. Dadurch werden die personen-bezogenen Daten der Kunden und deren Mitarbeiter geschützt. Die Zertifizierung wird während der Laufzeit des Vertrages aufrechterhalten.

Sicherheitsfunktionen innerhalb des Produktes:

Authentifizierung und Passwörter:

- Login (Zwei-Faktor-Authentifizierung. Nutzern, die sich bei der SaaS-Software anmelden, wird die Möglichkeit geboten, eine Zwei-Faktor-Authentifizierung für ihr Konto zu aktivieren, um die Sicherheit zu erhöhen).
  - Verschlüsselung Jegliche Kommunikation der dormakaba resivo Apps über öffentliche Netze ist durch HTTPS mit Transport Layer Security (AES 128 GCM SHA 256, 128 bit keys, TLS 1.3 mit PFS) verschlüsselt und geschützt. D.h. jegliche Datenübertragung geschieht ausschließlich verschlüsselt.

- Passwortstärke – resivo Nutzer (Mieter sowie auch Mitarbeiter von Verwaltungen) können nur Passwörter vergeben mit mindestens 8 Zeichen und mit jeweils mindestens einem Grossbuchstaben, einem Kleinbuchstaben, einem Sonderzeichen und einer Ziffer.

Nutzerrollen und Rechtekonzept

- Für die Nutzung der resivo utility app sowie des resivo admin portals gibt es verschiedene Nutzerrollen und ein Rechtekonzept. Eine, mehrere oder alle der folgenden Berechtigungen kann einem Benutzer zugewiesen werden:
  - Benutzerverwaltung: Benutzer erstellen, hinzufügen und löschen. Berechtigungen zuweisen oder entziehen. Empfehlenswert für Nutzer, die in einer Gebäudeverwaltung die App-Administrator oder Superior Rolle über nehmen sollen.
  - Gebäudeverwaltung: Mit dieser Berechtigung können Gebäude, Mietobjekte, Mietobjekttüren hinzugefügt, bearbeitet oder gelöscht werden.
  - Zutrittsverwaltung: Generalschlüssel oder Gastzutritt hinzufügen, Öffnen von Gemeinschaftstüren per Fernöffnung.
  - Mieterverwaltung: Mieter anlegen, ein- und ausziehen, Einladung zur resivo home app. Geeignet für Personen, die sich um das Mietermagement kümmern.
  - Komponentenverwaltung: Gemeinschaftstüren erstellen, unterhalten (Batteriewechsel, Firmware-Update) und löschen. Geeignet für Benutzer, die die Inbetriebnahme und Wartungsarbeiten leisten sowie Support anbieten.

Informations- und Kommunikationsmanagement:

- Push-Notifikation, SMS und / oder Email-Benachrichtigungen, wenn neue Bewohner hinzugefügt werden und Zugang zu einem Mietobjekt erhalten
- SMS und / oder Email-Benachrichtigungen, wenn Zugang zu einem Mietobjekt angefragt wird

Protokolle:

- Zutrittslog, Beschreibung siehe SaaS Vertrag
- History Log (Änderungslog)

dormakaba resivo

resivo von dormakaba ist ein zukunftsweisendes, Cloud-basiertes Zutrittsmanagementsystem. Dadurch bietet es Verwaltungen, Hausbesitzern und Mietenden wesentliche Vorteile gegenüber herkömmlichen mechanischen Schließsystemen. Die Sorge um verlorene oder gestohlene Schlüssel entfällt. Wohnungsübergaben werden einfacher und mieterfreundlicher. resivo spart Zeit durch einfachere Prozesse bei Zutrittserteilung für Lieferanten, Dienstleistungsanbieter und Handwerker. Die Bewohner bestimmen selbst, wer wann Zutritt zur Wohnung erhält – auch aus der Ferne. Mit resivo eröffnet sich eine ganz neue Dimension der Gebäudenutzung voller Vorteile.

Türtechnik

Systemlösungen
Zutritt und Zeit

Mechanische
Schliesssysteme

Hotelzutritts-
systeme

Automatische
Türsysteme

Services

Haben Sie Fragen? Wir beraten Sie gerne und freuen uns auf Sie.

Visit us:

resivo.dormakaba.com

DE, 03/2023
Technische Änderungen vorbehalten

dormakaba.com

dormakaba
Deutschland GmbH
DORMA Platz 1
DE-58256 Ennepetal
T +49 2333 793-0
info.de@dormakaba.com
dormakaba.de

dormakaba
Austria GmbH
Ulrich-Bremi-Strasse 2
AT-3130 Herzogenburg
T +43 2782 808-0
office.at@dormakaba.com
dormakaba.at

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

dormakaba
Schweiz AG
Mühlebühlstrasse 23
CH-8620 Wetzikon
T +41 848 85 86 87
info.ch@dormakaba.com
dormakaba.ch