Data privacy policy

for the Software Keyng -Smartphone App (for Android & iOS)

Implementation of the requirements of Article 25 GDPR (General Data Protection Regulation)

The measures to ensure data privacy compliance in accordance with Article 25 GDPR are described below.

Developers

The Keyng smartphone applications for iOS and Android operating systems are applications for managing Clex private locking systems and are developed by Uhlmann & Zacher GmbH, Gutenbergstr. 2-4, 97297 Waldbüttelbrunn.

Data privacy officer

Mr Konrad Griebel; Phone: +49 (0) 931 406720; E-Mail: contact(at)uundz.de

Access rights of the app

- The applications require access to your location for communication with the locking units. This access right is required to display locking units within reach of the Bluetooth® module of the mobile terminal and to communicate with the locking units.
- The application requires access to the wireless modules of the mobile terminals for communication with transponder keys and locks. (Bluetooth® & NFC).
- The application requires access to the file system for the manual export and import of the database by the user.
- The apps require access to the camera of your smartphone and the file folder. This enables you to accept invitations of locking system administrators by scanning QR codes or the opening of images with QR codes.

The app does not require any further access rights beyond these.

General data processing information about Uhlmann & Zacher GmbH processing personal data

The Keyng app is an offline application. Personal data is only collected and stored on your own mobile device. Data is only collected if it is entered by the user or generated through conscious interaction with the hardware. No personal data or usage data is collected or sent to Uhlmann & Zacher GmbH.

Uhlmann & Zacher GmbH | Gutenbergstr. 2—4 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | E-Mail: contact@UundZ.de | **www.UundZ.com**

Data privacy policy

for the Software Keyng -Smartphone App (for Android & iOS)

The following information refers to data privacy measures for personal data that you collect from third parties as a user, as well as requirements of Art. 25 GDPR from you as the administrator of a locking system using the Keyng application.

Implementation of the requirements of Article 25 GDPR

The measures to ensure data privacy compliance in accordance with Article 25 GDPR are described below.

Table of contents

1. Software operation

With the Keyng management software, a Clex private locking system is managed locally from a mobile device. The Keyng program is operated by the organisation using it or an individual and runs on his/her own mobile device. The responsibility for data privacy lies with those mentioned above.

Uhlmann & Zacher GmbH | Gutenbergstr. 2–4 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | E-Mail: contact@UundZ.de | **www.UundZ.com**

2. User authorisation concept
The Keyng software is designed for only one user. This user is the owner of the mobile device. Users have to ensure that only they have access to their mobile device and it is advisable to enable the security features such as automatic locking and biometric data for authorisation on the device.

3. Storing, sending and resetting passwords
The Keyng software does not have its own password management. Therefore, login data or passwords are not stored.

4. Access concept
The user has access to the data pertaining to keys and locks entered by himself/herself such as first and last names, and descriptions. Using a suitable service key, users can also read data from compatible locks.

5. Different authorisation levels
Only the user has access to the personal data stored on the mobile device. Serial numbers of each authorised key is stored on the compatible locks. Other users who possess the same service key can also view these numbers and associated events.

6. Options to block individual program functions for users
A user-dependent blocking of individual software functions is not provided

Uhlmann & Zacher GmbH | Gutenbergstr. 2—4 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | E-Mail: contact@UundZ.de | **www.UundZ.com**

7. Identification of personal data in the Software

Using the service key, the user also has access to the technical data of the locks, current authorisations and event logs from the locks. Authorisations of keys on locks are stored both in the app as well as in the concerned lock.

However, only serial numbers of the keys are stored in the lock, but not the assignment of these to individuals. Even events of keys in the lock that were earlier authorised by other users on the lock can be read. An automatic assignment of the IDs to individuals can only be done if the same key is managed by the user by name. Even other users can in turn read events from locks using the appropriate service key. Automatic assignment to individuals in the event log or in the authorization list can be done by these other users only if your system was already aware of this assignment.

8. Options to safeguard the rights concerned

8.1 Right of access under Art. 15 GDPR

The data for the stored keys may contain personal data such as last names and first names, e-mail address and phone number, as well as other personal data in the "Description" field.

To view and share the data for the information purposes, select the respective key in the "Key" tab and either note the data entered there or take a screenshot via the screenshot function of your mobile device.

8.2 Right to rectification under Article 16 GDPR

The data for the stored keys can be changed in the "Key" tab. To do this, select the respective key by clicking on the list, and then click the "Pen" icon to edit the data in the "Data" tab of the key. Events in the event log cannot be changed later.

8.3 Right to erasure under Art. 17 GDPR

To delete a key and the associated data from the list of keys, the authorisation of the key has to be first revoked for each lock. Then, click the "Edit" button in the list of saved keys, and then click on the red "minus symbol" next to the respective key. If only the personal data associated with the key has to be deleted, it is adequate to overwrite the stored data with other data. Proceed as described in section 8.2.

Neither individual entries with personal data nor the entire list can be deleted from the event log even in the software itself. These can only be deleted from the user's device by deleting the application.

8.4 Right to restriction under Art. 18 GDPR

This right cannot be reasonably implemented due to the nature of the data collected in conjunction with the locking system software and is not likely to be used by the concerned individuals.

Uhlmann & Zacher GmbH | Gutenbergstr. 2–4 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | E-Mail: contact@UundZ.de | **www.UundZ.com**

8.5 Obligation to notify under Art. 19 GDPR

Only personal data is collected and stored on the system of the software operator. A notification to third parties is currently not required after any change or deletion.

8.6 Right to data portability under Art. 20 GDPR

This right cannot be reasonably implemented due to the nature of the data collected in conjunction with the locking system software and is not likely to be used by the concerned individuals.

8.7 Right to object under Art. 21 GDPR

In the event of an objection under Article 21 GDPR, please proceed as described under "8.3 Right to erasure under Art. 17 GDPR".

9. Technical measures to protect the data

Users of the software have to ensure that unauthorised persons do not have access to their personal mobile device. It is advisable to always enable security features such as automatic locking and biometric data for device authorisation. In addition, the security key for accessing data in the locks should always be protected from third party access.

Waldbüttelbrunn, 22/11/2022 - Konrad Griebel, Data privacy officer

Uhlmann & Zacher GmbH | Gutenbergstr. 2—4 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | E-Mail: contact@UundZ.de | **www.UundZ.com**