Datenschutzerklärung

zur Software Keyng –Smartphone App (für Android & iOS)

Realisierung der Anforderungen des Art. 25 DS-GVO (Datenschutz-Grundverordnung)

Nachfolgend sind die Maßnahmen zur Sicherstellung der Datenschutzkonformität gemäß Art. 25 DS-GVO beschrieben.

Entwickler

Die Keyng Smartphone Applikationen für iOS und Android Betriebssysteme sind Anwendungen zur Verwaltung von Clex private Schließanlagen und werden entwickelt von der Uhlmann & Zacher GmbH, Gutenbergstr. 2-4, 97297 Waldbüttelbrunn.

Datenschutzbeauftragter

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

Benötigte Zugriffsrechte der App und verwendete Daten

- Bluetooth & NFC
  Die Applikation benötigt für die Kommunikation mit Transponderschlüsseln und Schlössern Zugriff auf die Funk-Module des mobilen Endgerätes.

- Standort (Bedingt durch Bluetooth Kommunikation)
  Standortdaten werden nicht direkt in der App verwendet. Durch die Bluetooth-Kommunikation und die Interaktion mit BLE Geräten lassen sich jedoch unter Umständen von anderen Personen Rückschlüsse auf vergangene Standorte des Benutzers ziehen. Auf den Schlössern werden Interaktionen protokolliert die von allen Personen im Besitz eines Servicekeys Ihrer Schließanlage einsehen und auswerten könnten.

- Kontakte (lesen)
  Zur Auswahl von Personen zur Erstellung von mobilen Schlüsseln wird das Adressbuch des Telefons gelesen und direkt in der App dargestellt. Von den ausgewählten Kontakten werden Name, E-Mail und mobile Telefonnummer in der App gespeichert.

- Dateisystem (lesen & schreiben)
  Zum manuellen Export- und Import der Datenbank durch den Benutzer benötigt die Applikation Zugriff auf das Dateisystem.

Darüber hinaus benötigt die App keine weiteren Zugriffsrechte.

Allgemeine Datenverarbeitungs-Informationen zur Verarbeitung personenbezogener Daten durch die Uhlmann & Zacher GmbH

Uhlmann & Zacher GmbH | Gutenbergstraße 2–4 | 97297 Waldbüttelbrunn | Tel.: +49 931 40672-0 | E-Mail: contact@UundZ.de | **http://www.UundZ.de**

Datenschutzerklärung

zur Software Keyng –Smartphone App (für Android & iOS)

Personenbezogene Daten werden nur auf Ihrem eigenen mobilen Endgerät erhoben und gespeichert. Daten werden nur erfasst, wenn diese selbständig eingeben oder durch bewusste Interaktion mit Hardware erzeugt werden. Kontaktdaten und Objektdaten zu Ihrer Schließanlage werden von der App nur auf Befehl des Benutzers an andere Applikationen auf dem gleichen Gerät und nur zum Versand von E-Mails und SMS durch den Benutzer übergeben.
Es werden keine personenbezogenen Daten oder Nutzungsdaten von der Uhlmann & Zacher GmbH erhoben oder an diese übermittelt.

Die folgenden Informationen beziehen sich auf Maßnahmen zum Datenschutz für Personendaten die Sie selbst als Nutzer innerhalb der App von Dritten erheben, sowie Anforderungen des Art. 25 DS-GVO gegenüber Ihnen als Verwalter einer Schließanlage unter Zuhilfenahme der Keyng Applikation.

Realisierung der Anforderungen des Art. 25 DS-GVO

Nachfolgend sind die Maßnahmen zur Sicherstellung der Datenschutzkonformität gemäß Art. 25 DS-GVO beschrieben.

Inhaltsverzeichnis

Uhlmann & Zacher GmbH | Gutenbergstraße 2–4 | 97297 Waldbüttelbrunn | Tel.: +49 931 40672-0 | E-Mail: contact@UundZ.de | **http://www.UundZ.de**

1. Betrieb der Software

Mit der Keyng Verwaltungssoftware wird eine Clex private Schließanlage dezentral von einem mobilen Endgerät aus verwaltet. Das Programm Keyng wird von der nutzenden Organisation oder einer privaten Person betrieben und läuft auf deren eigenem mobilen Endgerät. Die Verantwortung für den Datenschutz liegt bei den eben genannten.

2. Benutzerberechtigungskonzept

Die Software Keyng ist konzipiert für nur einen Benutzer. Dieser Nutzer ist Besitzer des mobilen Endgerätes. Nutzer haben Sorge zu tragen, dass nur sie selbst Zugriff auf ihr mobiles Gerät haben und es wird empfohlen die Sicherheitsfunktionen wie automatisches Sperren und Biometrische Daten zur Autorisierung am Gerät einzuschalten.

3. Passwortspeicherung, Passwortübermittlung und Zurücksetzung

Die Software Keyng verfügt über kein eigenes Passwortmanagement. Es werden deshalb auch keine Login-Daten oder Passwörter gespeichert.

4. Zugriffskonzept

Der Benutzer hat Zugriff auf die selbst eingegebenen Daten zu Schlüsseln und Schlössern wie Vor- und Nachnamen, und Beschreibungen. Mit Hilfe eines passenden Service-Schlüssels können Benutzer auch Daten aus kompatiblen Schlössern auslesen.

5. Unterschiedliche Berechtigungen

Zu den auf dem persönlichen mobilen Endgerät gespeicherten Daten hat jeweils nur der Benutzer Zugriff. Auf den kompatiblen Schlössern werden Seriennummern jedes berechtigten Schlüssels gespeichert. Durch andere Benutzer im Besitz eines gleichen Service-Schlüssels können diese Nummern und damit verbundene Ereignisse ebenfalls angezeigt werden.

6. Möglichkeiten der Sperrung einzelner Programmfunktionen für Benutzer

Eine Benutzerabhängige Sperrung einzelner Funktionen der Software ist nicht vorgesehen.

Uhlmann & Zacher GmbH | Gutenbergstraße 2–4 | 97297 Waldbüttelbrunn | Tel.: +49 931 40672-0 | E-Mail: contact@UundZ.de | **http://www.UundZ.de**

7. Identifizierung von Daten einer Person in der Software

Der Benutzer hat mit Hilfe des Service-Schlüssels auch Zugriff auf die technischen Daten der Schlösser, aktuelle Berechtigungen und Ereignisprotokolle aus den Schlössern. Berechtigungen von Schlüsseln an Schlössern werden sowohl in der App, als auch im jeweils betroffenen Schloss gespeichert.

Im Schloss werden jedoch nur Seriennummern der Schlüssel abgespeichert, nicht jedoch die Zuordnung dieser zu realen Personen. Es können auch Ereignisse von Schlüsseln am Schloss ausgelesen werden welche von anderen Benutzern zu früheren Zeitpunkten am Schloss berechtigt wurden. Eine automatische Zuordnung der IDs zu realen Personen kann nur erfolgen falls der gleiche Schlüssel vom Benutzer namentlich verwaltet wird. Auch andere Benutzer können im Gegenzug mithilfe des passenden Servicekeys Ereignisse von Schlüsseln aus Schlössern auslesen. Eine automatische Zuordnung zu realen Personen im Ereignisprotokoll oder in der Liste der Berechtigungen kann von diesen anderen Benutzern nur dann erfolgen, falls auch Ihrem System diese Zuordnung bereits bekannt war.

8. Möglichkeiten zur Wahrung der Betroffenenrechte

8.1 Recht auf Auskunft gemäß Art. 15 DS-GVO

In den Daten zu den gespeicherten Schlüsseln können persönliche Daten wie Namen, Vornamen, Email-Adresse und Telefonnummer oder im Feld „Bemerkung“ auch andere personenbezogene Daten gespeichert sein.

Zur Anzeige und Weitergabe der Daten zum Zwecke der Auskunft wählen Sie den jeweiligen Schlüssel im Tab „Schlüssel“ aus und notieren entweder die dort erfassten Daten oder erstellen Sie ein Bildschirmfoto über die Screenshot-Funktion ihres mobilen Gerätes.

8.2 Recht auf Berichtigung gemäß Art. 16 DS-GVO

Die Daten zu den gespeicherten Schlüsseln können im Tab „Schlüssel“ geändert werden. Wählen Sie dazu den jeweiligen Schlüssel durch tippen aus der Liste aus und tippen dann auf das „Stift“-Symbol zum Bearbeiten der Daten im Reiter „Daten“ des Schlüssels. Ereignisse im Ereignisprotokoll können nachträglich nicht geändert werden.

8.3 Recht auf Löschung gemäß Art. 17 DS-GVO

Uhlmann & Zacher GmbH | Gutenbergstraße 2–4 | 97297 Waldbüttelbrunn | Tel.: +49 931 40672-0 | E-Mail: contact@UundZ.de | **http://www.UundZ.de**

Um einen Schlüssel mitsamt den zugeordneten Daten aus der Liste der Schlüssel zu löschen, muss dem Schlüssel zuerst an jedem Schloss die Berechtigung entzogen werden. Tippen Sie dann in der Liste der gespeicherten Schlüssel auf den Button „Bearbeiten" und anschließend auf das rote „Minus-Symbol" neben dem jeweiligen Schlüssel. Sollen lediglich die dem Schlüssel zugeordneten persönlichen Daten gelöscht werden reicht es die gespeicherten Daten mit anderen Daten zu überschreiben. Gehen Sie dazu vor wie im Punkt 8.2 beschrieben.

Aus den Ereignis-Protokollen können in der Software selbst weder einzelne Einträge mit personenbezogenen Daten noch die gesamte Liste gelöscht werden. Diese können nur durch Löschen der Applikation vom Endgerät des Benutzers gelöscht werden.

8.4 Recht auf Einschränkung gemäß Art. 18 DS-GVO

Dieses Recht ist aufgrund der Art der erfassten Daten im Zusammenhang mit Schließanlagensoftware nicht sinnvoll durchsetzbar und findet aller Voraussicht nach hier keine Anwendung durch betroffene Personen

8.5 Mitteilungspflicht gemäß Art. 19 DS-GVO

Es werden nur personenbezogene Daten auf dem System des Betreibers der Software erfasst und gespeichert. Eine Mitteilung an Dritte ist nach Änderung oder Löschung aktuell nicht erforderlich.

8.6 Recht auf Datenübertragbarkeit gemäß Art. 20 DS-GVO

Dieses Recht ist aufgrund der Art der erfassten Daten im Zusammenhang mit Schließanlagensoftware nicht sinnvoll durchsetzbar und findet aller Voraussicht nach hier keine Anwendung durch betroffene Personen

8.7 Recht auf Widerspruch gemäß Art. 21 DS-GVO

Im Falle eines Widerspruchs gemäß Art. 21 DS-GVO gehen Sie bitte vor wie unter „8.3 Recht auf Löschung gemäß Art. 17 DS-GVO" beschrieben vor.

9. Technische Maßnahmen zum Schutz der Daten

Nutzer der Software haben Sorge zu tragen, dass keine unberechtigten Personen Zugriff zu ihrem persönlichen mobilen Endgerät haben. Es wird empfohlen die Sicherheitsfunktionen wie automatisches Sperren und biometrische Daten zur Autorisierung am Gerät immer einzuschalten. Zudem ist der Sicherheitsschlüssel zum Zugriff auf die Daten in den Schlössern stets vor Fremdzugriff zu schützen.

Waldbüttelbrunn, 06.07.2021 – Konrad Griebel, Datenschutzbeauftragter

Uhlmann & Zacher GmbH | Gutenbergstraße 2–4 | 97297 Waldbüttelbrunn | Tel.: +49 931 40672-0 | E-Mail: contact@UundZ.de | **http://www.UundZ.de**