Datenschutzerklärung

zur Software Keyvi im System Clex prime

Realisierung der Anforderungen des Art. 25 DS-GVO

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

Inhaltsverzeichnis

1. Betrieb der Software

Mit der Keyvi Verwaltungssoftware wird die Schließanlage zentral oder dezentral von einem oder mehreren PCs verwaltet. Bei einer clientseitigen, dezentralen Verwendung liegt die Datenbank zentral auf einem Server. Das Programm Keyvi wird von der nutzenden Organisation oder privaten Person betrieben und läuft auf deren eigenen Systemen. Die Verantwortung für den Schutz dieser Daten liegt bei den eben genannten.

Für die Verwendung von mobilen Schlüsseln werden personenbezogene Daten an einen Sicherheitsserver der Uhlmann & Zacher GmbH übergeben. Diese Daten werden verschlüsselt an den Clex Key Hub Server mit Standort in Deutschland übermittelt und sind dort so verschlüsselt gespeichert, dass Mitarbeiter von Uhlmann & Zacher oder Dritte diese Daten nicht im Klartext einsehen können.

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

2. Benutzerberechtigungskonzept

Die Software Keyvi erfüllt bereits in ihrer Standardausführung ein umfangreiches Benutzerberechtigungskonzept in Form eines benutzergruppenbasierten Rollenkonzepts zur Steuerung von Programmrechten, Türgruppenrechten und Türrechten. Benutzer einer Benutzergruppe können nur die ihnen zugeteilten Programmteile nutzen und nur die Daten der ihnen zugeteilten Türgruppen einsehen bzw. je nach Einstellung nur einsehen aber keine Änderungen vornehmen.

Der Systemadministrator kann den jeweiligen Softwarenutzern entsprechende Rollen zuteilen, welche nur diesen zur Verfügung stehen. Die Software Keyvi stellt nach Festlegung der Rollen dem Benutzer eine an seine Benutzerrollen angepasste Benutzeroberfläche bereit.

Für den Umgang mit sensiblen Ereignisdaten ermöglicht Keyvi die Definition eines zusätzlichen Passworts. Auch kann ein Vier-Augen Prinzip mit zwei separaten Passwörtern realisiert werden. Der Vier-Augen-Passwortschutz stellt somit sicher, dass der Zugriff auf Ereignisprotokolle nur nach gemeinsamem Eingeben der beiden getrennten Passwörter erfolgen kann (z.B. Personalabteilung und Betriebsrat).

Soll an bestimmten oder allen Türen kein Ereignisprotokoll erstellt werden, kann die Protokollfunktion an jeder einzelnen Tür deaktiviert werden. Eine unwiderrufbare Deaktivierung der Protokollfunktion ist ebenfalls in den Türoptionen möglich. Wird diese Option gewählt, kann die Protokollfunktion in Keyvi dauerhaft nicht wieder aktiviert werden. Die Nutzung der Funktion ist dann nur noch nach Neuprogrammierung der Geräte durch den Hersteller der Geräte-Software möglich.

3. Passwortspeicherung, Passwortübermittlung und Zurücksetzung

Für jeden neuen Mandanten bzw. jedes in der Software verwaltete Projekt ist bei der ersten Anmeldung ein Admin-Account (Namentlich: „!!“) als Standardbenutzer vorhanden. Um im weiteren Datenschutz zu gewährleisten, ist es zwingend erforderlich individuelle Passwörter für alle Administratoren und Benutzer-Accounts zu vergeben.

Um den Erst-Zugang neuer Nutzer zur Software zu ermöglichen, wird jedem Software-User ein persönliches Passwort durch einen Administrator zugeteilt. Das Passwort ist individuell und jedem Nutzer einzeln zugeordnet. Wurde die Funktion „Passwort bei Anmeldung ändern“ verwendet, werden die Benutzer nach der ersten Anmeldung aufgefordert ein eigenes Passwort zu wählen. Es wird dringend empfohlen diese Option zu nutzen. So kann gewährleistet werden, dass Passwörter die auf nicht sicheren Wegen, wie E-Mail oder Ausdrucken, verbreitet wurden, nach der ersten Benutzung ihre Gültigkeit verlieren. Auch kann so einfacher sichergestellt werden, dass auch wirklich nur eine Person den Account nutzt.

Die Passwortspeicherung erfolgt codiert, wobei das Passwort nicht direkt in der Datenbank gespeichert, sondern über einen Hash gegen direktes Auslesen geschützt wird. Benutzer können später auch selbständig ihr Passwort ändern. Im Falle eines vergessenen Passworts können Administratoren für Benutzer kein neues Passwort setzen. Es empfiehlt sich den bestehenden Account zu deaktivieren und dem Benutzer einen neuen Zugang einzurichten.

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

Alternativ zur Passwortvergabe und -speicherung in der Datenbank kann individuell je Keyvi-Nutzer die Option „Windows-Anmeldung“ gewählt werden. In diesem Fall loggt sich der Benutzer mit seinen Windows-Anmeldecredentials ein, die er bei der Anmeldung zum Programm nicht noch einmal eingeben muss. Es muss bei der Benutzererstellung selbst bei Wählen der Option „Windows-Anmeldung“ immer ein Passwort für den Benutzer vergeben werden, dass diesem aber nicht mitgeteilt werden muss. Niemals sollte ein leeres Passwort vergeben werden.

4. Zugriffskonzept

Datensätze können einer Person, einer Gruppe von Personen, einem Schlüssel, einer Tür oder einer Türgruppe zugeordnet sein. In der Regel ist ein Datensatz mit mehreren der genannten Entitäten verknüpft.

Über das Rollenkonzept (siehe oben) wird durch den Systemadministrator, basierend auf der Organisation, definiert, ob ein Benutzer Zugriffsrechte, sei es Bearbeitungs- oder Leserechte, bekommt. Durch dieses Vorgehen wird gewährleistet, dass der Zugriff auf einzelne Daten nur derjenige Nutzer bekommt, welcher auch dafür zuständig ist. Dies deckt auch den Zugriff auf Programmfunktionen ab. Die Steuerung erfolgt durch das bereits beschriebene Benutzerberechtigungskonzept.

5. Unterschiedliche Berechtigungen

Die Software Keyvi verfügt über ein breites Spektrum an Zugriffsberechtigungen der Nutzer. Jede der gespeicherten Daten kann nur im Rahmen der zugeteilten Rollen gelesen, erstellt, bearbeitet, gelöscht, exportiert oder gedruckt werden.

Die unterschiedlichen Berechtigungen können, je nach zugeteilter Rolle standardmäßig eingeschränkt werden. Dies ermöglicht eine freie Gestaltung der Zugriffsberechtigungen durch den Systemadministrator. Somit können Nutzergruppen nur mit Lesezugriff erstellt werden, welche lediglich die Übersichten einsehen können. Auch können Programmrechte auf einzelne Türgruppen eingeschränkt werden, um einzelnen Standorten oder Abteilungen eine individuelle Administration zu ermöglichen und den Zugriff auf Daten auf den tatsächlich berechtigten Personenkreis einzuschränken.

6. Möglichkeiten der Sperrung einzelner Programmfunktionen für Benutzer

Die Software ermöglicht die Sperrung von einzelnen Türen, Türgruppen und Programmfunktionen auf Ebene der Benutzergruppen. Darüber hinaus kann neben dem Zugriff hierüber auch die Sichtbarkeit der Daten bezogen auf Türen, Türgruppen und Abteilungen eingestellt werden.

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

7. Identifizierung von Daten einer Person in der Software

Die Software Keyvi ermöglicht mehrere Arten der Identifizierung von Daten einer Person. Zum einen besteht die Möglichkeit in Form einer Volltextsuche gezielt nach Begriffen zu suchen oder mit Zuhilfenahme von bekannten Merkmalen Personen herauszufiltern.

Die einzelnen Filter erlauben dem jeweiligen Nutzer, welcher zuvor mit entsprechenden Rechten ausgestattet wurde, eine detaillierte Filterung. Die Filterung umfasst die Suche nach allen nur denkbaren Datensätzen, welche personenbezogene Daten umfassen. Eine Filterung nach Vorname, Nachname, E-Mail oder Adresse ist problemlos im Standard möglich.

So kann mit Hilfe von bekannten Berechtigungen auf Türen eine Liste von berechtigten Gruppen, Abteilungen oder Einzelpersonen erstellt werden. Ist dem Benutzer die Schlüssel-ID bekannt, kann auch über die persönlich zugeteilten Schlüssel die entsprechende Person identifiziert werden

Falls Ereignisprotokolle erfasst werden, erfolgt die Zuordnung des Namens von Personen anhand des zugeteilten Schlüssels automatisch in der Listenansicht sobald das Ereignisprotokoll von den Türen zurück an die Keyvi-Datenbank transferiert wurde. Deshalb sollten nur berechtigte und im Datenschutz geschulte Benutzer Zugriff auf Ereignisprotokolle bekommen.

8. Möglichkeiten zur Wahrung der Betroffenenrechte

8.1 Recht auf Auskunft gemäß Art. 15 DS-GVO

Die persönlichen Daten einer Person (Vorname, Name, Adress- und Kontaktdaten, räumliche und organisatorische Zuteilung wie Zuordnung zu Schließgruppe etc.) sind im Schlüsselausgabeprotokoll enthalten. Bei Anfrage kann das Protokoll neu erstellt und noch einmal ausgedruckt werden.

Sind Ereignisse protokolliert worden, kann zusätzlich über die Funktion “Ereignisse von Schlüssel“ im Menüpunkt „Übersichten“ ein Ausdruck aller erfassten Ereignisse des persönlichen Schlüssels ausgedruckt werden.

8.2 Recht auf Berichtigung gemäß Art. 16 DS-GVO

Falsche Daten in den Stammdaten einer Person können jederzeit durch einen berechtigten Benutzer geändert werden. Es kann anschließend ein neues Schlüsselausgabeprotokoll erstellt werden, um der Person die Änderungen zu dokumentieren.

8.3 Recht auf Löschung gemäß Art. 17 DS-GVO

Zum Löschen der Daten zu einer Person, muss im Menüpunkt „Stammdaten“ die Funktion „Stammdaten Personen ausgewählt werden. Dort kann die entsprechende Person gesucht, ausgewählt und gelöscht werden. Namensdaten wie Name und Vorname sind bis zum Eintritt des automatischen Löschdatums weiter in den Ereignisprotokollen gespeichert, sofern Protokolle eingerichtet wurden.

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

Soll eine umgehende Löschung auch aus den Ereignisprotokollen erfolgen, müssen diese zum Zeitpunkt der Löschung ebenfalls gelöscht werden.

In der Schlüsselhistorie und in der Personenhistorie werden Vor- und Nachname der Personen dauerhaft, nicht löschbar gespeichert. Diese Daten werden dann genutzt, wenn zu einem Zeitpunkt nach Löschen der Person ein Ereignis aus einer elektronischen Tür eingelesen wird, dass zu einem Zeitpunkt erzeugt wurde, an dem die Person noch existiert hatte. Anhand des Zeitpunkts wird der zu diesem Zeitpunkt verwendete Name der Person identifiziert, damit Ereignisse niemals einer falschen Person zugeordnet werden. Die Personen- und Schlüsselhistorie ist durch Benutzer der Software nicht einsehbar.

In den Logdateien sind Personendaten ebenfalls vorhanden. Die Logdatei kann als Ganzes gelöscht werden.

Die an die Uhlmann & Zacher übergebenen verschlüsselten personenbezogenen Daten auf dem Clex Key Hub können vom Keyvi Benutzer gelöscht werden, indem sämtliche der entsprechenden Person zugeordnete mobilen Schlüssel gelöscht werden. Nach Übermittlung der Löschaufträge werden diese Daten auch auf dem Clex Key Hub entfernt.

8.4 Recht auf Einschränkung gemäß Art. 18 DS-GVO

Dieses Recht ist aufgrund der Art der erfassten Daten im Zusammenhang mit Zutrittskontrollsystemen 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 Daten auf dem System des Betreibers der Software in nicht-anonymisierter Form 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 Zutrittskontrollsystemen nicht sinnvoll durchsetzbar und findet aller Voraussicht nach hier keine Anwendung durch betroffene Personen.

8.7 Recht auf Widerspruch gemäß Art. 21 DS-GVO

Widerspricht eine Person der Verarbeitung ihrer Daten kann die Person aus dem System gelöscht werden. Zum Löschen der Daten zu einer Person, muss im Menüpunkt „Stammdaten“ die Funktion „Stammdaten Personen“ ausgewählt werden. Dort kann die entsprechende Person gesucht, ausgewählt und gelöscht werden. Vor Löschung des Datensatzes der Person müssen zuerst mit der Person verknüpfte berechtigte Schlüssel entzogen werden.

Widerspricht die Person lediglich der Erfassung von Ereignissen in einem Protokoll und werden aktuell Ereignis-Protokolle an Türen erstellt an denen die Person berechtigt ist, empfiehlt es sich eben-

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

falls die Person zu löschen. Die Person sollte erst dann wieder im System angelegt werden, nachdem an allen Türen an denen der Benutzer berechtigt sein wird die Protokollfunktion dauerhaft deaktiviert wurde.

In der Schlüsselhistorie und in der Personenhistorie werden Vor- und Nachname der Personen dauerhaft, nicht löschbar gespeichert. Diese Daten werden dann genutzt, wenn zu einem Zeitpunkt nach Löschen der Person ein Ereignis aus einer elektronischen Tür eingelesen wird, dass zu einem Zeitpunkt erzeugt wurde, an dem die Person noch existiert hatte. Anhand des Zeitpunkts wird der zu diesem Zeitpunkt verwendete Name der Person identifiziert, damit Ereignisse niemals einer falschen Person zugeordnet werden. Die Personen- und Schlüsselhistorie ist durch Benutzer der Software nicht einsehbar.

In den Logdateien sind Personendaten ebenfalls vorhanden. Die Logdatei kann als Ganzes gelöscht werden.

9. Technische Maßnahmen zum Schutz der Daten

Die Administratoren und Nutzer der Software Keyvi haben Sorge zu tragen, dass keine unberechtigten Personen physischen oder virtuellen Zugriff auf Laufwerke und Verzeichnisse haben, auf denen Keyvi Datenbankdateien ablegt. Keyvi benutzt standardmäßig entweder eine „Microsoft Access“ oder „Microsoft SQL“ Datenbank. Die Daten in der Datenbank sind mit Ausnahme von Passwörtern nicht grundsätzlich durch weitere Verfahren verschlüsselt. Die Sicherheit der Datenbanken wird deshalb stark bestimmt vom Sicherheitsniveau der gewählten Speicherorte innerhalb der Systeme der Betreiber-Organisation.

Sollte der Betreiber des Schließsystems die Datenbank zur Wartung einem externen Dienstleister – (z.B. dem Hersteller der Software) überlassen, können und sollten sämtliche personenbezogene Daten beim Export der Datenbank anonymisiert werden. Dafür steht die Option „Personen Anonymisierung“ im Reiter „Datenschutz“ der Einstellungen des Mandanten im Servicemodus zur Verfügung. Dabei werden vor dem Export alle personenbezogenen Daten aus Datenbank und den Log-Dateien gelöscht und Kalenderdaten mit zufälligen Daten überschrieben. Achtung: Die Funktion „Personen Anonymisierung“ darf nur mit einer Kopie der Datenbank durchgeführt werden, niemals mit der Arbeitsdatenbank, sonst sind alle Personendaten unwiderruflich gelöscht.

Waldbüttelbrunn, 22.11.2022 – Konrad Griebel, Datenschutzbeauftragter

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