Declaration of data protection

for Keyvi software in the Clex prime

Realization of the requirements of Article 25 GDPR

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

Table of contents

1. Software operation

The Keyvi management software is used to manage the locking units centrally or locally from one or more PCs. In case of a client-side, distributed usage the database is stored centrally on a server. The Keyvi program is operated by the using organization or private person and runs on their own systems. The responsibility for the protection of these data lies with those just named.

For the use of mobile keys, personal data are transferred to a security server of Uhlmann & Zacher GmbH. These data are transmitted in encrypted form to the Clex Key Hub server located in Germany and are stored there in such an encrypted form that employees of Uhlmann & Zacher or third parties cannot view these data in plain text.

Uhlmann & Zacher GmbH | Gutenbergstraße 24 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | Email: contact@uundz.de | **www.UundZ.com**

2. User authorization concept

The Keyvi software already fulfills a comprehensive user authorization concept in its standard version in the form of a user group-based role concept for controlling program rights, door group rights and door rights. Users of a user group can only use those program parts they have been assigned and only view the data of the door groups assigned to them or only view but not make any changes after the setting.

The system administrator can assign corresponding roles to the respective software users which are only available to them. After definition of the roles, the Keyvi software provides the user with a user interface adapted to their user roles.

To deal with sensitive event data Keyvi allows for the definition of an additional password. A four-eyes principle with two separate passwords can also be implemented. The four-eyes password protection thus ensures that access to event logs can only take place after entering the two separate passwords together (for example Human Resources and Work Council).

If no event log is to be created at specific or all doors, the log function can be deactivated at each individual door. An irrevocable deactivation of the log function is also possible in the door options. If this option is selected, the log function in Keyvi cannot be reactivated permanently. Using the function is then only possible after the devices have been reprogrammed by the manufacturer of the device software.

3. Password storage, password transmission and resetting

For each new client or each new project managed in the software, an admin account (called: "!!") is available as the default user during the first login. In order to ensure data protection in the future, it is mandatory to assign individual passwords to all administrators and user accounts.

To enable initial access of new users to the software, a personal password is assigned to each software user by an administrator. The password is individual and assigned individually to each user. If the "Change password at login" function was used, the users are prompted after the initial login to select their own password. It is strongly recommended to use this option. This ensures that passwords distributed by non-secure means, such as e-mail or printouts, lose their validity after the first use. This also makes it easier to ensure that only one person actually uses the account.

The password is stored encoded, whereby the password is not saved directly in the database but is protected against direct reading out via a hash. Users can also change their password later on. In case of a forgotten password, administrators cannot set a new password for users. It is advisable to deactivate the existing account and set up a new access for the user.

Uhlmann & Zacher GmbH | Gutenbergstraße 24 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | Email: contact@uundz.de | **www.UundZ.com**

As an alternative to password assignment and storage in the database, the "Windows login" option can be selected individually for each Keyvi user. In this case the user logs in with their Windows login credentials which they do not have to enter again when logging into the program. A password must always be assigned to the user during user creation, even if the "Windows login" option is selected, but the user does not have to be informed of this password. You should never assign an empty password.

4. Access concept

Data records can be assigned to a person, a group of persons, a key, a door or a door group. As a rule a data record is linked with several of the listed entities.

The role concept (see above) is used by the system administrator to define, based on the organization, whether a user is granted access rights, be it editing or reading rights. Through this procedure it is ensured that access to individual data is only granted to the user who is also responsible for them. This also cover access to program functions. Control takes place through the user authorization concept described above.

5. Different authorizations

The Keyvi software has a wide spectrum of user access authorizations. Each of the stored data can only be read, created, edited, deleted, exported or printed within the framework of the assigned roles.

The different authorizations can, depending on the assigned role, be limited by default. This allows the system administrator to organize the access permissions freely. This allows user groups who only have read access to be created. These can only view the overviews. Program rights can also be restricted to individual door groups to allow individual sites or departments individual administration and to limit access to data to the group of people actually authorized.

6. Possibilities of limiting individual program functions for users

The software allows individual doors, door groups and program functions to be limited at the level of user groups. Furthermore, in addition to access, this can also be used to set the visibility of data related to doors, door groups and departments.

Uhlmann & Zacher GmbH | Gutenbergstraße 24 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | Email: contact@uundz.de | **www.UundZ.com**

7. Identification of data of a person in the software

The Keyvi software allows for several types of identification of data of a person. For one there is the possibility to search for specific terms in the form of a full text search or to filter out persons by using known characteristics.

The individual filters allow the respective user, who was equipped beforehand with corresponding rights, detailed filtering. The filtering includes the search for all conceivable data records, which include personal data. Filtering for the first name, last name, e-mail or address is possible without problems in the default version.

This way a list of authorized groups, departments or individuals can be created using known permissions on doors. If the key ID is known to the user, the corresponding person can also be identified via the personally assigned keys.

If event logs are collected, the assignment of the name of persons based on the assigned key will be carried out automatically in the list view as soon as the event log has been transferred from the doors back to the Keyvi database. Therefore only authorized users and those trained in data protection should receive access to the event logs.

8. Possibilities for safeguarding the rights of the data subjects

8.1 Right to information according to Article 15 GDPR

A person's personal data (first name, last name, address and contact data, area and organizational assignment such as assignment to a locking group, etc.) are contained in the key issue log. If requested, the log can be created again and printed again. If events have been logged, a printout of all logged events of the personal key can additionally be printed out via the "Events of key" function in the "Overviews" menu item.

8.2 Right to rectification according to Article 16 GDPR

Incorrect data in the master data of a person can be changed at any time by an authorized user. A new key issue log can then be created to document the changes to the person.

8.3 Right to deletion according to Article 17 GDPR

To delete the data of a person the "Master data persons" function has to be selected in the "Master data" menu item. There the corresponding person can be searched for, selected and deleted. Name data such as first name and last name continue to be stored in the event logs until the automatic deletion date occurs, in as far as have been set up.

Uhlmann & Zacher GmbH | Gutenbergstraße 24 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | Email: contact@uundz.de | **www.UundZ.com**

If immediate deletion is required also from the event logs, these must also be deleted at the time of deletion.

In the key history and in the person history, first and last name of the persons are stored permanently and cannot be deleted. These data are only used if at a time after deletion of the person an event is read in from an electronic door that was generated at a time when the person still existed in the system. The time identifies the name of the person used at that time, so that events are never assigned to the wrong person. The personal and key history cannot be viewed by users of the software.

Personal data also exist in the log files. The log file can be deleted as a whole.

The encrypted personal data transferred to Uhlmann & Zacher on the Clex Key Hub can be deleted by the Keyvi User by deleting all mobile keys assigned to the corresponding person. After the deletion requests are submitted, these data are also removed on the Clex Key Hub.

8.4 Right to restriction according to Article 18 GDPR

This right is not reasonably enforceable in the context of access control systems due to the nature of the data collected and, in all likelihood, will not be applied here by data subjects

8.5 Obligation to notify according to Article 19 GDPR

Only data on the system of the operator of the software are collected and stored in a non-anonymized form. A notification to third parties after modification or deletion is currently not required.

8.6 Right to data portability according to Article 20 GDPR

This right is not reasonably enforceable in the context of access control systems due to the nature of the data collected and, in all likelihood, will not be applied here by data subjects.

8.7 Right of objection according to Article 21 GDPR

If a person objects to the processing of their data, the person can be deleted from the system. To delete the data of a person you have to select the "Master data persons" function in the "Master data" menu item. There the corresponding person can be searched for, selected and deleted. Before deleting the data record of the person, authorized keys associated with the person must first be revoked.

If the person only objects to the recording of events in a log and event logs are currently created at doors where the person is authorized, it is recommended to also delete the person. The person should only be created again in the system after the log function has been permanently deactivated on all doors to which the user will be authorized.

In the key history and in the person history, first and last name of the persons are stored permanently and cannot be erased. These data are only used if at a time after deletion of the person an event is read in from an electronic door that was generated at a time when the person still existed in the system. The time identifies the name of the person used at that time, so that events are never assigned to the wrong person. The personal and key history cannot be views by users of the software.

Personal data also exist in the log files. The log file can be deleted as a whole.

Uhlmann & Zacher GmbH | Gutenbergstraße 24 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | Email: contact@uundz.de | **www.UundZ.com**

9. Technical measures for data protection

The administrators and users of the Keyvi software shall ensure that no unauthorized persons have physical or virtual access to drives and directories on which Keyvi stores data and files. By default Keyvi uses either a "Microsoft Access" or "Microsoft SQL" database. With the exception of passwords, the data in the database are not generally encrypted by other methods. The safety of the data is therefore determined to a high degree by the security level of the selected storage locations within the operator organization's systems.

If the operator of the locking system entrusts the database to an external service provider for maintenance (for example the manufacturer of the software), all personal data can and should be anonymized during the export of the database. To this purpose the "Person anonymization" option is available in the "Data protection" tab of the settings of the client in the Service mode. In the process all personal data from the database and the log files are deleted and calendar data are overwritten with random data. Caution: The "Person anonymization" function must only be performed with a copy of the database - never with the working database. Otherwise all personal data are irrevocably deleted.

Waldbüttelbrunn, 22/11/.2022 — Konrad Griebel, Data protection officer

Uhlmann & Zacher GmbH | Gutenbergstraße 24 | 97297 Waldbüttelbrunn | Phone: +49 931 40672-0 | Email: contact@uundz.de | **www.UundZ.com**