Guidance on data security and data protection compliance when using biometric facial recognition with the Kentix iDFace Max

Basic functionality, data flow and security architecture

The Kentix iDFace Max processes biometric data according to the principle of privacy by design. The entire architecture of the device is designed to reduce personal data to the technically necessary minimum and only process it locally. The complete data flow and the security architecture are described below.

1. capture and management of user images in KentixONE

Administrators and users with the appropriate authorization can create and manage user profiles in KentixONE. A reference photo is stored in the respective user profile for the use of biometric facial recognition. Key points:

- Uploading a photo controls whether a user is included in biometric recognition.
- Administrators are responsible for compliance with data protection regulations (e.g. user consent, image rights, deletion periods).
- The reference photo remains exclusively in the KentixONE system and is not automatically transferred to devices.

2. local template creation in iDFace Max

As soon as a user photo is added or updated in KentixONE, the iDFace Max receives a corresponding change notification. . The iDFace Max then performs the following steps:

a. Local conversion

The device loads the corresponding user photo into the work memory, where it is converted into a biometric template. This is a mathematical representation of characteristic facial features.

b. Local storage of the template

The template becomes:

1. only stored locally in the device,
2. stored in encrypted form,
3. clearly assigned to the user ID.

Biometric templates are not transferred to the network or the cloud. They are not transferred back to KentixONE. Templates are not synchronized between multiple iDFace Max devices. This means that all biometric feature data remains completely on the respective device.

3. handling raw image data

By default, no raw image data is stored on the iDFace Max.

Exception: An optional streaming function can be activated in the menu. In this case, event-based still images or video streams can be generated and transmitted to authorized systems (e.g. alarm events). This function is deactivated by default and must be deliberately activated by an administrator.

4. deletion of templates

If a user’s reference photo is deleted in KentixONE or the user profile is removed, the associated biometric template is automatically deleted completely from the local memory the next time the user information is synchronized

Aspects for data protection-compliant operation

Legal basis

The following procedures are common for creating the legal framework for a company. Which procedures are permissible in individual cases is determined by national legislation and, if applicable, application-specific regulations such as employee data protection

1. individual user consent

Aspects such as

- Voluntary nature of consent (if necessary, an alternative means of access must be

provided)
- Information for all users
- Revocability of consent

2. appeal to high security

For access to particularly sensitive areas (e.g. data centers, laboratories), regulations can be put in place that place the protection of the area above the data protection rights of the user

3. collective agreement (works agreement)

Companies can include aspects of the use of biometric data for employees in company agreements. Aspects such as purpose, data types, deletion periods, access rights and alternatives must be clearly regulated and specified. In most cases, these company agreements must be approved by the employee representatives.

Data protection compliant installation

- Only point the camera at access areas, not at common areas and work areas, not at publicly accessible areas
- Visible signs: “Video/biometric recording”
- Security hardening of the device performed

Data protection compliant operation

The regulations for general data protection also apply in full to biometric data. Aspects such as:

- Restriction of data collection and transfer
- Deletion concept
- Access control to the devices and databases only for administrators with need-to-know
- Logging of all access to the devices and databases
- System hardening
- Regular rights check
- Transparency towards users
- Documentation

must be observed.

Biometric facial data are considered special categories of personal data according to Art. 9 GDPR. This means that additional requirements from national legislation and/or application-specific regulations may be mandatory. These must be checked for each individual case before commissioning.

System hardening

Configuration of software, communication and interfaces of the device enables adaptation to the applicable guidelines. The following aspects must be set and configured during commissioning:

- Devices – Password
- Definition HTTPS/ HTTP
- Deactivation/activation SSH
- Deactivation/activation web interface
- Internal device audit logs
- Firmware updates
- Network ports

The latest and detailed information on the options and configuration for system hardening can be found here: https://www.controlid.com.br/manual/security-hardening-guide-en.pdf