Aide à la sécurité et à la conformité des données lors de l’utilisation de la reconnaissance faciale biométrique du Kentix iDFace Max.

Fonctionnalité de base, flux de données et architecture de sécurité

Le Kentix iDFace Max traite les données biométriques selon le principe Privacy by Design. Toute l’architecture de l’appareil est conçue pour réduire les données personnelles au minimum techniquement nécessaire et pour les traiter exclusivement localement. Le flux complet des données et l’architecture de sécurité sont décrits ci-dessous.

1. capture et gestion des images d’utilisateurs dans KentixONE

Les administrateurs et les utilisateurs disposant d’une autorisation adéquate peuvent créer et gérer des profils d’utilisateur dans KentixONE. Pour l’utilisation de la reconnaissance faciale biométrique, une photo de référence est enregistrée dans le profil utilisateur correspondant. Points essentiels :

- Le téléchargement d’une photo contrôle l’inclusion ou non d’un utilisateur dans la reconnaissance biométrique.
- Les administrateurs sont responsables du respect des exigences en matière de protection des données (par exemple, consentement de l’utilisateur, droit à l’image, délais de suppression).
- La photo de référence reste exclusivement dans le système KentixONE et n’est pas transmise automatiquement aux appareils.

2. création de modèles locaux dans iDFace Max

Dès qu’une photo d’utilisateur est ajoutée ou mise à jour dans KentixONE, l’iDFace Max reçoit une information de modification correspondante. . L’iDFace Max exécute ensuite les étapes suivantes :

a. Conversion locale

L’appareil télécharge la photo de l’utilisateur dans l’espace de travail, où elle est convertie

en un modèle biométrique. Il s’agit d’une représentation mathématique des caractéristiques faciales.

b. Stockage local du modèle

Le modèle sera :

1. sont exclusivement stockées localement dans l’appareil,
2. sont stockés sous forme cryptée,
3. clairement associé à l’identifiant de l’utilisateur.

Les modèles biométriques ne sont pas transférés sur le réseau ou dans le nuage. Ils ne sont pas retransmis à KentixONE. Les modèles ne sont pas synchronisés entre plusieurs appareils iDFace Max. Ainsi, toutes les données de caractéristiques biométriques restent intégralement sur l’appareil concerné.

3. traitement des données d’images brutes

Par défaut, l’iDFace Max n’enregistre pas de données d’images brutes.

Exception : une fonction optionnelle de diffusion en continu peut être activée dans le menu. Dans ce cas, des images fixes ou des flux vidéo basés sur des événements peuvent être générés et transmis aux systèmes autorisés (par exemple, des événements d’alarme). Cette fonction est désactivée par défaut et doit être délibérément activée par un administrateur.

4. suppression de modèles

Si la photo de référence d’un utilisateur est supprimée dans KentixONE ou si le profil de l’utilisateur est supprimé, le modèle biométrique correspondant sera automatiquement supprimé de la mémoire locale lors de la prochaine synchronisation des informations sur l’utilisateur.

Aspects pour une exploitation conforme à la protection des données

Base juridique

Les procédures suivantes sont courantes pour établir le cadre juridique d’une entreprise. La législation nationale et, le cas échéant, les règles spécifiques à l’application, telles que la protection des données des travailleurs, déterminent les procédures autorisées dans chaque cas.

1. consentement individuel de l’utilisateur

Il faut tenir compte d’aspects tels que

- le caractère volontaire du consentement (le cas échéant, un autre moyen d’accès doit être fourni)
- Information de tous les utilisateurs
- Révocabilité du consentement

2. invocation de la haute sécurité

Pour l’accès à des zones particulièrement sensibles (par exemple les centres de données, les laboratoires), des règles peuvent être mises en place qui placent la protection de la zone au-dessus des droits de protection des données de l’utilisateur.

3. convention collective (accord d’entreprise)

Les entreprises peuvent choisir d’inclure les aspects liés à l’utilisation des données biométriques dans les accords d’entreprise pour leurs employés. Les aspects tels que l’objectif, les types de données, les délais de suppression, les droits d’accès et les alternatives doivent être clairement définis et nommés. Dans la plupart des cas, ces accords d’entreprise doivent être approuvés par les représentants du personnel.

Mise en place conforme à la protection des données

- Diriger la caméra uniquement vers les zones d’accès, pas vers les zones de séjour et de travail, pas vers les zones accessibles au public
- Panneaux visibles : « Enregistrement vidéo/biométrique ».
- Hardening de sécurité de l’appareil effectué

Fonctionnement conforme à la protection des données

Les règles relatives à la protection générale des données s’appliquent également pleinement aux données biométriques. Des aspects tels que

- Limitation de la collecte et du partage des données
- Concept de suppression
- Contrôle d’accès aux appareils et bases de données uniquement pour les administrateurs ayant besoin de savoir
- Enregistrement de tous les accès aux appareils et aux bases de données
- Durcissement du système
- Vérification régulière des droits
- Transparence vis-à-vis des utilisateurs
- Documentation

sont à prendre en compte.

Les données faciales biométriques sont considérées comme des catégories particulières de données à caractère personnel en vertu de l’article 9 du RGPD. Par conséquent, des exigences supplémentaires découlant de la législation nationale et/ou des réglementations spécifiques à l’application peuvent être obligatoires. Celles-ci doivent être vérifiées au cas par cas avant la mise en service.

Durcissement du système

La configuration du logiciel, des communications et des interfaces de l’appareil permet de l’adapter aux directives en vigueur. Les aspects suivants doivent être réglés et configurés lors de la mise en service :

- Périphériques - Mot de passe
- Définition HTTPS/ HTTP
- Désactivation/activation de SSH
- Désactivation/inactivation de l’interface web
- Journaux d’audit internes à l’appareil
- Mises à jour du micrologiciel
- Ports réseau

Vous trouverez ici les informations les plus récentes et les plus détaillées sur les possibilités et la configuration du durcissement du système :
https://www.controlid.com.br/manual/security-hardening-guide-en.pdf