contrast

Privacy Talk

YOUR BUSINESS • NOVEMBER 2020

# Can I use fingerprint authentication to secure my business premises?

## What you need to know.

The idea that a lock must be practical and secure applies to both your private life and to your business. In the latter case, dozens of employees often have access to your buildings - meaning that the use of a key, a badge and/or an access code is not necessarily the most secure option. Your staff may lose the key or badge or forget their access code. In a worst-case scenario, these items (possibly written down) might even be stolen. The use of fingerprint authentication therefore seems to offer a safer, more practical option for securing your premises.

From a privacy perspective, however, the use of fingerprint authentication should not be taken for granted. Indeed, fingerprints are "biometric data", comprised of unique and personal patterns that need to be treated with extreme care. In principle, therefore, the processing of such data is prohibited, and it can only be allowed if a ground for exception within the meaning of Article 9.2 GDPR is applicable. For example, it is possible to process fingerprints if the explicit consent of the data subject has been obtained.

Obtaining such valid consent is not altogether obvious in an employer-employee relationship. A valid consent has to be given “freely”, and it is generally assumed that employees are seldom in a position to freely give, refuse or revoke their consent, in light of the de facto dependency resulting from the employer-employee relationship. Nevertheless, we believe that this can be accommodated by explicitly offering employees an alternative that is less invasive in terms of impact on privacy (e.g. a personal badge).

## What you need to do.

If you want to use fingerprint authentication to secure your business premises, you must obtain the explicit consent of your staff to process their fingerprints. To this end, we recommend providing your staff with a specific consent form that, firstly, clearly describes the purpose for which the fingerprints will

be used (i.e. to secure your premises against unauthorised access) and, secondly, allows them to give their explicit consent.

This consent form should also clearly and explicitly state that if the employee does not want his/her fingerprint to be used for authentication purposes, it is possible to opt for an alternative (e.g. a personal badge). If the employee does agree to the use of his/her fingerprints, he/she will sign the consent form and thus give his/her explicit consent. The form should also mention that the given consent can be revoked at any time and should, furthermore, provide details on how this revocation is to be done (e.g. via a message to a central contact person). In that case, the employee will again be offered the alternative.

You may only store fingerprints for as long as this is necessary to secure your business premises. The fingerprints of your employee must therefore be immediately and irreversibly erased from all relevant systems once he/she leaves employment. Moreover, your staff has all of the rights provided for by the GDPR with regard to the processing of their personal data.

In addition, you must of course not lose sight of the other obligations under the GDPR and you must, amongst other things, take all possible organisational and technical measures to ensure the security of the data in your possession and, in addition, include the fingerprint authentication in your record of processing activities and in the privacy policy for your staff.