contrast

VOS ACTIVITÉS • NOVEMBRE 2020

Puis-je utiliser l'authentification par empreinte digitale pour sécuriser mes locaux d’entreprise ?

Ce que vous devez savoir.

Le fait qu'une serrure doit être pratique et sûre s'applique aussi bien à votre sphère privée qu'à votre entreprise. Dans ce dernier cas, des dizaines d'employés ont souvent accès à vos bâtiments. L'utilisation d'une clé, d'un badge et/ou d'un code d'accès n'est pas nécessairement la meilleure solution. Votre personnel peut perdre la clé ou le badge ou oublier son code d'accès. Dans le pire des cas, ces objets (écrits ou non) sont volés. L'utilisation de l'authentification par empreinte digitale semble donc être une option plus pratique et plus sûre pour sécuriser vos locaux d’entreprise.

Cependant, l'utilisation de l'authentification par empreinte digitale n'est pas si évidente du point de vue de la protection de la vie privée. Une empreinte digitale est une « donnée biométrique », c'est-à-dire un modèle unique et personnel qui doit être manipulé avec une extrême prudence. Le traitement de ces données est donc en principe interdit et n'est autorisé que s'il existe un motif d'exclusion au sens de l'article 9.2 du GDPR. A titre d’exemple, il est possible de traiter les empreintes digitales si le consentement explicite de la personne concernée a été obtenu.

L'obtention d'un consentement valable n'est pas si évidente dans une relation employeur-employé. Un consentement valable doit être donné « librement » et il est généralement considéré que la relation d’autorité de l’employeur à l’égard de l’employé empêche un consentement « libre ». Nous pensons toutefois qu'il est possible d'y remédier en offrant explicitement au personnel une alternative qui a un impact moins important sur la protection de la vie privée (par exemple, un badge personnel).

contrast

Ce que vous devez faire.

Si vous souhaitez utiliser l'authentification par empreinte digitale pour la sécurité de vos locaux d’entreprise, vous devez obtenir le consentement explicite des membres de votre personnel pour le traitement de leurs empreintes digitales. À cette fin, nous vous recommandons d'établir un formulaire de consentement concret qui indique clairement le but dans lequel les empreintes digitales seront utilisées (à savoir, pour sécuriser vos locaux d’entreprise contre tout accès non autorisé).

Ce formulaire de consentement doit également indiquer clairement et explicitement que si l'employé ne souhaite pas que son empreinte digitale soit utilisée à des fins d'authentification, une alternative (telle qu’un badge personnel) peut être choisie. Si l'employé accepte que ses empreintes digitales soient utilisées, il signera le formulaire de consentement et donnera de ce fait son accord explicite. Le formulaire doit également indiquer que le consentement donné peut être révoqué à tout moment et la manière dont cette révocation doit être effectuée (par exemple par message à une personne de contact centrale). Dans ce cas, l'employé se verra proposer l'alternative.

Vous ne pouvez pas conserver les empreintes digitales plus longtemps que nécessaire pour la sécurité de vos locaux d’entreprise. Les empreintes digitales des membres de votre personnel doivent être effacées de manière irréversible des systèmes concernés lorsque ceux-ci quittent leur emploi. Les membres de votre personnel disposent également de tous les droits accordés par le GDPR en ce qui concerne le traitement de leurs données à caractère personnel.

En outre, vous ne devez bien entendu pas perdre de vue les autres obligations découlant du GDPR et devez, entre autres, prendre toutes les mesures techniques et organisationnelles possibles pour garantir la sécurité des données en votre possession. Par ailleurs, vous devez également inclure l'authentification des empreintes digitales dans votre registre des activités de traitement et dans la politique de confidentialité du personnel.