NOTE TECHNIQUE

ANITEC
ALLIANCE NATIONALE
DES INTÉGRATEURS DE TECHNOLOGIES
CONNECTÉES, SÉCURISÉES ET PILOTÉES

Peut-on coupler une pointeuse pour les salariés avec un contrôle d'accès ?

Les directions Sûreté & Sécurité des entreprises, sont en règle générale, assez hostiles au fait de mélanger des systèmes de contrôle des accès et des solutions logicielles associés à des lecteurs. En effet, il est de plus en plus utilisé dans les entreprises, une associativité entre le système de contrôle d'accès, la vidéoprotection et le système de détection intrusion. Ses systèmes servent une finalité exclusive de protection des personnes et des biens et ne peuvent être utilisés à d'autres usages.

Le Code de Sécurité Intérieure, notamment sur son livre 2 (vidéoprotection) et son livre 6 (fonctionnement des Services Internes de Sécurité), rappelle l'importance du respect des libertés fondamentales et individuelles sur voie publique, comme au sein des établissements.

De plus, votre client final, s'il souhaitait associer des technologies, mélangeant des produits destinés à la protection des personnes et des biens et des produits destinés au contrôle et à la gestion des personnels via les ressources humaines, devrait mettre en œuvre une procédure assez lourde. Cette procédure AIP (analyse d'impact sur la protection des données) devrait servir à démontrer que les deux systèmes sont conformes au RGPD (Règlement Général sur la Protection des Données) et de répondre à la Directive Européenne NIS2.

Mai 2023

NOTE TECHNIQUE

Mai 2023

Que faire avec le contrôle des horaires ?

Depuis le 25 mai 2018, les systèmes de contrôle des horaires par badge n'ont plus à être déclarés à la CNIL, date d'entrée en application du RGPD.

Toutefois, pour se conformer aux règles de protection des données personnelles, votre client doit :

- Demander conseil et assistance à son DPO (Délégué à la Protection des Données), s'il dispose de cette ressource, en général, c'est l'ancien Correspondant Informatique & Liberté de l'entreprise.
- Vérifier, en fonction du projet, si le DPO de votre client, est en mesure de vous remettre les résultats de son analyse d'impact sur la vie privée. S'il n'a pas réalisé cette étude, vous pouvez co-réaliser avec le DPO de votre client cette analyse.
- Nous conseillons de présenter le résultat de cette analyse, ainsi que le produit potentiellement retenu, auprès des salariés ou de leurs représentants du CES (Comité Economique et Social), ceci afin d'éviter si le système est jugé intrusif, une déclaration auprès de la CNIL qui pourrait prendre des sanctions s'il juge la solution non-conforme ou poreuse à un risque lié à la vie privée.
- Il existe un certain nombre de solutions de pointeuses salarié notamment par technologie RFID et peu coûteuse sur le marché. Vous devez néanmoins porter une attention particulière aux achats sur Internet et d'éviter les « marques blanches » vendues dans des régions du monde non concerné par le RGPD et ou le contrôle social est particulièrement intrusif.
- Nous déconseillons fortement, l'utilisation d'une pointeuse salariée, en mesure par le biais d'un capteur vidéo de prendre une ou plusieurs photos des salariés durant leurs entrées-sorties de la journée dans le ou les bâtiments. De nombreux signalements ont été effectués en ce sens auprès de la CNIL, qui a mis en œuvre des mises en demeure et des rappels avec la menace d'une amende considérable.
- La solution manufacturée que vous souhaitez acheter, doit être en mesure de disposer d'une solution dite « Security By Design ». Ce qui signifie que cette solution est sécurisée depuis sa fabrication et respecte le RGPD.
- Il est important d'échanger avec le fabricant, pour qu'il puisse vous indiquer quelle est la méthode « d'anonymisation » des données de la solution. C'est ce point particulier qui viendra rassurer les ressources humaines de votre client ainsi que les salariés, représentants du CES.
- Une fois l'ensemble de ses points validés et respectés. Votre client devra inscrire le fichier et la solution dans son « registre d'activité des traitements informatiques et numériques » pour le présenter en cas de contrôle au personnel de la CNIL.
- La conservation des données relatives aux accès doit être supprimée 3 mois après leur enregistrement.

Pour vous aider dans votre démarche :

lacces-aux-locaux-et-le-controle-des-horaires-sur-le-lieu-de-travai