La pointeuse peut-elle être intégrée dans un système de contrôle d'accès aux bâtiments ?

Réponse courte

L'intégration d'une **pointeuse** dans un système de contrôle d'accès aux bâtiments est techniquement et juridiquement possible au Luxembourg, sous réserve du respect strict des règles relatives à la **protection des données** et des droits des salariés. Cette intégration suppose une analyse préalable de proportionnalité et de nécessité, car elle combine deux finalités distinctes : la sécurité des locaux et la gestion du **temps de travail**.

L'employeur doit s'assurer que le dispositif intégré ne conduit pas à une surveillance **disproportionnée** des salariés. La consultation de la **délégation du personnel** est obligatoire avant toute mise en place. Chaque finalité doit être documentée séparément dans le registre des traitements, et une analyse d'impact (AIPD) peut être requise si le système génère un risque élevé pour les droits des salariés, notamment en cas d'utilisation de données biométriques.

Définition

La **pointeuse** désigne un dispositif permettant d'enregistrer les heures d'arrivée et de départ des salariés à des fins de gestion du temps de travail. Un **système de contrôle d'accès** vise à restreindre l'entrée et la sortie des personnes dans des locaux ou zones déterminés.

L'**intégration** consiste à utiliser un même dispositif ou une même base de données pour assurer simultanément le contrôle d'accès et l'enregistrement des temps de présence, en respectant les obligations d'information pour chaque finalité. Cette fusion implique le traitement croisé de données d'identification et de présence.

Questions fréquentes

Comment documenter les finalités combinées ?

Chaque finalité doit être documentée séparément dans le registre des traitements RGPD. La finalité de sécurité et la finalité de temps de travail doivent avoir leurs propres bases légales, durées de conservation et modalités d'accès aux données par les services concernés.

Comment éviter le détournement de finalité ?

Les données collectées pour le contrôle d'accès ne peuvent servir au contrôle du temps de travail sans information préalable explicite. Il faut séparer logiquement les bases de données, définir des profils d'accès distincts pour la sécurité et les RH, et auditer régulièrement les usages.

Faut-il consulter la délégation du personnel ?

Oui, la consultation de la délégation est obligatoire avant toute mise en place selon l'article L.261-1. Le dossier complet doit être transmis avec description des finalités, données collectées, mesures de sécurité et modalités d'accès. Une codécision s'applique au-delà de 150 salariés.

L'AIPD est-elle obligatoire pour cette intégration ?

L'AIPD est obligatoire si le système intègre des données biométriques ou génère un risque élevé selon l'article 35 du RGPD. Elle doit documenter la nécessité, la proportionnalité, les mesures de sécurité et la séparation des finalités entre accès et temps de travail.

Peut-on intégrer pointeuse et contrôle d'accès aux bâtiments ?

Oui, l'intégration est possible au Luxembourg sous réserve du respect strict des règles de protection des données. Elle suppose une analyse préalable de proportionnalité car elle combine deux finalités distinctes : la sécurité des locaux et la gestion du temps de travail des salariés.

Quelle technologie privilégier pour cette intégration ?

Il faut privilégier des dispositifs non biométriques (badge, code) pour l'accès aux bâtiments. Les profils d'accès aux données doivent être distincts pour la sécurité et les RH. Les durées de conservation s'appliquent séparément à chaque finalité conformément au principe de minimisation.

Conditions d’exercice

L'intégration est subordonnée au respect de conditions cumulatives.

Critère	Détail
Finalités distinctes	Chaque finalité (sécurité et temps de travail) doit être documentée séparément
Proportionnalité	Le dispositif ne doit pas aller au-delà de ce qui est strictement nécessaire
Information préalable	Chaque salarié doit être informé individuellement et par écrit (art. L.261-1)
Consultation délégation	Information préalable de la délégation du personnel obligatoire
AIPD	Obligatoire si le système intègre des données biométriques ou génère un risque élevé
Non-détournement	Les données collectées pour l'accès ne peuvent servir au contrôle du temps sans information

Modalités pratiques

La mise en place du système intégré suit un processus structuré.

Étape	Détail
Documentation	Rédiger une description détaillant chaque finalité, les données collectées et les mesures de sécurité
AIPD	Réaliser une analyse d'impact si données biométriques ou traitement à grande échelle
Information délégation	Transmettre le dossier complet à la délégation du personnel
Information individuelle	Remettre à chaque salarié un document décrivant les deux finalités et les droits associés
Séparation des accès	Limiter l'accès aux données de temps de travail aux seules personnes habilitées RH
Conservation distincte	Appliquer des durées de conservation différentes selon la finalité

Pratiques et recommandations

Privilégier des dispositifs non biométriques (badge, code) pour l'accès aux bâtiments, le pointage biométrique étant soumis à des conditions strictes.

Séparer logiquement les données d'accès et les données de temps de travail dans le système d'information.

Définir des profils d'accès distincts pour le service sécurité et le service RH, afin d'éviter tout croisement non autorisé.

Réaliser des audits réguliers pour vérifier que les données d'accès ne sont pas utilisées à des fins non déclarées.

Documenter les mesures techniques et organisationnelles dans le registre des activités de traitement.

Cadre juridique

Référence	Objet
Art. L.211-29	Obligation de tenue d'un registre du temps de travail
Art. L.261-1	Information préalable pour le traitement de données de surveillance
Art. L.414-9	Codécision dans les entreprises de 150+ salariés
RGPD art. 5	Principes de finalité, minimisation et limitation de la conservation
RGPD art. 9	Traitement des données biométriques
RGPD art. 35	Analyse d'impact obligatoire si risque élevé

L'utilisation combinée d'une pointeuse et d'un système de contrôle d'accès ne doit jamais conduire à une surveillance permanente des salariés. Le croisement non autorisé des données d'accès et de temps de travail constitue un détournement de finalité sanctionnable par la CNPD.