Les badges d'accès peuvent-ils être utilisés pour contrôler la présence ?

Réponse courte

Les **badges d'accès** peuvent être utilisés pour contrôler la présence des salariés au Luxembourg, à condition de respecter les principes de **finalité déterminée**, de **proportionnalité** et de transparence. La finalité de gestion du temps de travail doit avoir été expressément annoncée dès l'installation, distincte de la simple finalité d'accès aux locaux ; tout détournement de finalité (usage évaluatif ou disciplinaire non annoncé) est illicite.

L'employeur doit consulter la **délégation du personnel** (L.414-9), informer individuellement chaque salarié des données collectées et de leurs usages, limiter les habilitations au service RH et inscrire le traitement au **registre**. Une **AIPD** est requise si le dispositif est couplé à de la biométrie ou à un suivi nominatif fin. Le détournement de finalité expose l'employeur à des sanctions RGPD jusqu'à **4 % du CA mondial**.

Définition

Le **badge d'accès** est un dispositif électronique individuel permettant d'identifier chaque salarié et d'enregistrer ses entrées et sorties dans les locaux de l'entreprise. Il génère des données relatives aux **horaires de présence et d'absence** susceptibles d'être traitées à des fins de gestion du temps de travail.

Cette utilisation constitue un **traitement de données à caractère personnel** soumis à l'article L.261-1 du Code du travail, à la loi du 1er août 2018 et au RGPD, avec un encadrement spécifique sur la finalité et la durée de conservation.

Questions fréquentes

Combien de temps conserver les données de pointage par badge au Luxembourg ?

Les données se conservent généralement 3 à 6 mois à des fins de gestion de la paie. Au-delà, l'anonymisation ou la suppression s'imposent sauf nécessité documentée dans le registre des traitements.

Les badges d'accès peuvent-ils être utilisés pour contrôler la présence des salariés ?

Oui, à condition de respecter la finalité déterminée, la proportionnalité et la transparence. La finalité de gestion du temps de travail doit avoir été annoncée dès l'installation, distincte de la finalité d'accès aux locaux.

Que risque l'employeur qui détourne les données de badge à des fins disciplinaires ?

Le détournement de finalité est en soi une violation du RGPD, indépendamment de la régularité initiale du dispositif. L'employeur s'expose à des sanctions administratives jusqu'à 4 % du chiffre d'affaires mondial.

Qui peut accéder aux données de pointage des salariés ?

L'accès doit être limité au seul service RH par habilitation tracée et journalisée. La liste des personnes autorisées est nominative et la consultation des données est documentée.

Un badge d'accès installé pour la sécurité peut-il servir à gérer le temps de travail ?

Non, sans nouvelle information et consultation. Un dispositif déployé pour la sécurité ne peut être réutilisé pour la gestion du temps de travail : ce détournement de finalité (article 5 RGPD) est illicite.

Une AIPD est-elle requise pour les badges d'accès des salariés ?

Oui, si le dispositif est couplé à de la biométrie ou à un suivi nominatif fin (article 35 RGPD). La consultation de la délégation du personnel reste obligatoire pour toute installation (L.414-9).

Conditions d’exercice

La finalité de contrôle de la présence doit être explicite et distincte de la finalité d'accès aux locaux ; un dispositif déployé pour la sécurité ne peut être réutilisé pour gérer le temps de travail sans nouvelle information et consultation.

Condition	Exigence
Finalité explicite	Gestion du temps de travail expressément annoncée, distincte du simple contrôle d'accès
Proportionnalité	Données limitées au strict nécessaire ; pas de croisement avec d'autres dispositifs sans justification
Information préalable	Notice individuelle précisant la finalité, la durée, les destinataires, les droits
Consultation délégation	Co-décision pour les entreprises ? 150 salariés (L.414-9)
AIPD si risque élevé	Obligatoire si couplage biométrique ou suivi nominatif fin (article 35 RGPD)
Habilitations restreintes	Accès limité au service RH et aux personnes nominativement désignées

Modalités pratiques

Les données de pointage se conservent quelques mois (généralement 3 à 6 mois) à des fins de gestion de la paie ; au-delà, l'anonymisation ou la suppression s'imposent sauf nécessité documentée.

Démarche	Précision
Inscription au registre	Article 30 RGPD : finalité, données, durée, destinataires, mesures de sécurité
AIPD	Obligatoire pour les dispositifs biométriques ou à suivi fin (article 35 RGPD)
Consultation délégation	Procès-verbal préalable signé (L.414-9)
Information individuelle	Notice écrite remise à chaque salarié avec mention des finalités et droits
Durée de conservation	3 à 6 mois pour les pointages, anonymisation au-delà sauf justification
Habilitations	Liste nominative des accès RH avec journalisation des consultations
Anonymisation périodique	Suppression ou anonymisation des historiques après expiration du délai

Pratiques et recommandations

Annoncer clairement la finalité de contrôle de la présence dès l'installation et l'inscrire au registre.

Limiter l'accès aux données de pointage au seul service RH par une habilitation tracée et journalisée.

Éviter tout couplage avec d'autres dispositifs (vidéosurveillance, géolocalisation) sans nouvelle base légale.

Informer chaque salarié, dès la remise du badge, de la finalité, de la durée et de ses droits RGPD.

Anonymiser ou supprimer les historiques de passages dès que la finalité de gestion est atteinte.

Réviser annuellement les habilitations et les durées de conservation avec la délégation du personnel.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Traitement de données pour surveillance des salariés (loi du 1er août 2018)
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel pour les installations de contrôle
Art. L.211-1 et suivants du Code du travail	Durée du travail, justifiant la finalité de pointage
Loi modifiée du 1er août 2018	Protection des personnes à l'égard du traitement des données à caractère personnel
Règlement (UE) 2016/679 (RGPD)	Articles 5 (finalité), 6 (licéité), 30 (registre), 35 (AIPD)
Lignes directrices CNPD	Recommandations sur le contrôle de la présence par badgeage

Le détournement de finalité (utilisation des données de badge à des fins évaluatives ou disciplinaires non annoncées) est en soi une violation du RGPD, indépendamment de la régularité initiale du dispositif. L'employeur s'expose à des sanctions administratives jusqu'à 4 % du chiffre d'affaires mondial.