Quels dispositifs doivent être mis en place pour sécuriser les données de la badgeuse ?

Réponse courte

L'employeur doit mettre en œuvre des **mesures techniques et organisationnelles** appropriées pour garantir la confidentialité, l'intégrité et la disponibilité des données collectées par la badgeuse, conformément à l'article 32 du RGPD. L'accès aux données doit être limité aux seules personnes habilitées, et toute violation doit être documentée et notifiée à la **CNPD** dans un délai de **72 heures** si elle présente un risque pour les droits des salariés.

La consultation préalable de la **délégation du personnel** est obligatoire avant toute mise en place ou modification du dispositif, conformément à l'article L.261-1 du Code du travail. Le registre temps travail doit être tenu conformément à l'article L.211-29 et présenté à l'ITM sur demande.

Définition

La badgeuse désigne un dispositif électronique permettant l'enregistrement des heures d'arrivée et de départ des salariés. Les données collectées constituent des **données à caractère personnel** au sens du RGPD, dès lors qu'elles permettent d'identifier directement ou indirectement un salarié.

La sécurisation des données de la badgeuse recouvre l'ensemble des mesures visant à empêcher tout accès non autorisé, toute altération, perte ou divulgation des informations enregistrées. Elle relève à la fois du droit du travail et de la **protection des données** personnelles.

Questions fréquentes

Comment sécuriser les données de la badgeuse ?

L'employeur doit mettre en oeuvre des mesures techniques et organisationnelles appropriées selon l'article 32 du RGPD : contrôle d'accès restreint, traçabilité des accès, chiffrement, sauvegarde, suppression effective à l'expiration. L'accès doit être limité aux seules personnes habilitées du service RH ou de la direction.

Faut-il consulter la délégation pour la sécurisation ?

Oui, la consultation préalable de la délégation du personnel est obligatoire avant toute mise en place ou modification du dispositif selon l'article L.261-1. Le registre du temps de travail doit être tenu conformément à l'article L.211-29 et présenté à l'ITM sur demande.

Que faire en cas de violation de données ?

Toute violation doit être documentée et notifiée à la CNPD dans un délai de 72 heures si elle présente un risque pour les droits des salariés selon l'article 33 du RGPD. Une procédure de gestion des incidents doit être prévue avec qualification, notification et information des personnes concernées.

Quelles mesures techniques privilégier ?

Les mesures incluent le chiffrement des données en transit et au repos, la pseudonymisation, des sauvegardes régulières et sécurisées, l'effacement effectif à l'expiration. Les mesures doivent être proportionnées aux risques et aux catégories de données traitées par le système de pointage.

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Quelles sanctions en cas de défaut de sécurité ?

L'absence de mesures de sécurité appropriées expose à des sanctions de la CNPD pouvant atteindre 20 millions EUR ou 4 % du chiffre d'affaires mondial, ainsi qu'à des sanctions de l'ITM pour défaut de tenue du registre (251 à 25 000 EUR). La documentation est essentielle.

Qui peut accéder aux données de pointage ?

Seules les personnes habilitées (service RH, direction) peuvent accéder aux données. L'authentification doit être adaptée et la traçabilité des accès assurée par enregistrement des consultations et modifications. Les logs doivent être conservés pour permettre la détection de tout accès anormal.

Conditions d'exercice

Les obligations de sécurisation s'appliquent dès la mise en place du dispositif.

Condition	Détail
Finalité déterminée	Le traitement doit reposer sur une finalité explicite et légitime (gestion du temps de travail)
Accès restreint	Seules les personnes habilitées (service RH, direction) peuvent accéder aux données
Information individuelle	Chaque salarié doit être informé par écrit du dispositif, des finalités et de ses droits (article L.261-1)
Consultation préalable	La délégation du personnel doit être consultée avant toute décision définitive (article L.414-9)
Durée de conservation	Limitée au strict nécessaire ; la CNPD recommande un maximum d'un an après la fin de la période de référence
AIPD	Obligatoire si le dispositif permet un suivi systématique des salariés (article 35 RGPD)

Modalités pratiques

Les mesures suivantes doivent être mises en œuvre pour assurer la sécurité des données.

Modalité	Contenu
Contrôle d'accès	Restriction de l'accès par des moyens d'authentification adaptés
Traçabilité	Enregistrement des accès et modifications apportées aux données, conservation des logs
Chiffrement	Mise en œuvre de mesures de protection adaptées (chiffrement, pseudonymisation)
Sauvegarde	Réalisation de sauvegardes régulières et stockage sécurisé des copies
Suppression	Effacement effectif des données à l'issue de la période de conservation
Gestion des incidents	Procédure de notification des violations de données à la CNPD dans les 72 heures (article 33 RGPD)

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Pratiques et recommandations

Documenter l'ensemble des mesures de sécurité mises en œuvre et maintenir cette documentation à jour pour pouvoir la présenter lors des contrôles de l'ITM ou de la CNPD. **Informer les salariés** et **former régulièrement** le personnel ayant accès aux données sur les obligations de confidentialité et les procédures de signalement des incidents.

Tester périodiquement les mesures de sécurité afin de vérifier leur efficacité et les adapter aux évolutions technologiques.

Cadre juridique

Référence	Objet
Art. L.211-29 du Code du travail	Tenue du registre du temps de travail et présentation à l'ITM
Art. L.261-1 du Code du travail	Surveillance des salariés et information préalable obligatoire
Art. L.414-9 du Code du travail	Consultation obligatoire de la délégation du personnel
Articles 5, 30, 32, 33 et 35 du RGPD	Principes de traitement, registre, sécurité, notification des violations et analyse d'impact
Loi du 1er août 2018	Protection des données à caractère personnel et missions de la CNPD

L'absence de mesures de sécurité appropriées expose l'employeur à des sanctions de la CNPD pouvant atteindre 20 millions EUR ou 4 % du chiffre d'affaires mondial, ainsi qu'à des sanctions de l'ITM pour défaut de tenue du registre (251 à 25 000 EUR).

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.