Une entreprise peut-elle utiliser la biométrie pour contrôler l'accès des salariés ?

Réponse courte

L'usage de la **biométrie** pour le contrôle d'accès est admis uniquement si la **nécessité absolue** est démontrée et qu'aucune alternative moins intrusive (badge, code) n'est suffisante. Les données biométriques sont des **données sensibles** au sens de l'article 9 du RGPD applicable en entreprise : leur traitement est interdit sauf exceptions strictes, le consentement du salarié n'étant pas une base légale valable en raison du lien de subordination.

L'employeur doit réaliser une **AIPD** systématique (article 35 RGPD), consulter la CNPD si le risque résiduel reste élevé (article 36), consulter la délégation du personnel (article L.414-9) et anticiper le refus légitime du salarié en limitant l'usage aux **zones à risque particulier** (laboratoires, salles serveurs, accès sensibles). La biométrie reste une solution de dernier recours, jamais admise pour le simple contrôle horaire.

Définition

Les **données biométriques** sont des caractéristiques physiques, physiologiques ou comportementales permettant d'identifier de manière unique une personne : empreinte digitale, reconnaissance faciale, iris, géométrie de la main, voix.

Elles sont qualifiées de **catégories particulières de données** par l'article 9 du RGPD lorsqu'elles servent à identifier une personne, et bénéficient d'une protection renforcée : leur traitement est interdit en principe, sauf exceptions strictes prévues par la loi modifiée du 1er août 2018.

Questions fréquentes

Faut-il consulter la CNPD avant d'installer un dispositif biométrique ?

Oui, la consultation préalable de la CNPD (article 36 RGPD) s'impose si le risque résiduel reste élevé après les mesures d'atténuation. Une AIPD est systématiquement obligatoire (article 35 RGPD).

Faut-il proposer une alternative aux salariés refusant la biométrie ?

Oui, une procédure non biométrique documentée doit être disponible pour tout salarié refusant légitimement la collecte. La sanction d'un salarié exerçant ce refus constitue une discrimination indemnisable au regard du Code du travail luxembourgeois.

La biométrie peut-elle servir au pointage ou au contrôle horaire ?

Non, la CNPD exclut expressément la biométrie pour le simple contrôle horaire, le pointage ou la gestion de présence ordinaire. Elle reste une solution de dernier recours pour des zones à risque particulier.

Le consentement du salarié suffit-il pour utiliser ses données biométriques ?

Non. Les données biométriques sont sensibles (article 9 RGPD) et le consentement n'est pas une base légale valable en raison du lien de subordination. Une base légale alternative et une AIPD sont obligatoires.

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

Où conserver le gabarit biométrique d'un salarié ?

Le stockage local sur un support individuel détenu par le salarié (badge à puce, smartphone) doit être privilégié. Cela limite les risques de fuite massive et renforce la sécurité du dispositif.

Une entreprise peut-elle utiliser la biométrie pour contrôler l'accès des salariés au Luxembourg ?

Oui, mais uniquement si la nécessité absolue est démontrée et qu'aucune alternative moins intrusive (badge, code) n'est suffisante. L'usage est limité aux zones à risque particulier comme laboratoires ou salles serveurs.

Conditions d’exercice

La biométrie est admise uniquement pour des zones à risque particulier ; elle est exclue pour la simple gestion horaire, le pointage ou le contrôle de présence ordinaire.

Condition	Exigence
Nécessité absolue	Sécurité de zones sensibles ; alternative classique inopérante
Donnée sensible	Article 9 RGPD : interdiction sauf exception strictement encadrée
Consentement invalide	Le lien de subordination prive le consentement de validité
Proportionnalité	Périmètre limité aux zones à risque, jamais pour la pointeuse
Stockage local	Gabarit conservé sur support individuel du salarié à privilégier
Alternative obligatoire	Solution non biométrique disponible pour les salariés refusant

Modalités pratiques

L'AIPD est systématiquement obligatoire pour la biométrie au regard du caractère sensible des données ; la consultation préalable de la CNPD s'impose si le risque résiduel reste élevé après les mesures d'atténuation.

Démarche	Précision
Analyse d'impact (AIPD)	Article 35 du RGPD, obligatoire et approfondie
Consultation préalable CNPD	Article 36 du RGPD si risque résiduel élevé
Consultation de la délégation	Procès-verbal préalable (article L.414-9)
Information individuelle	Finalité, durée, destinataires, droits, alternative non biométrique
Sécurité renforcée	Chiffrement, stockage local, authentification forte
Registre des traitements	Mention spécifique des catégories particulières (article 9)
Solution alternative	Procédure documentée pour les salariés ne consentant pas

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

Pratiques et recommandations

Privilégier le stockage local du gabarit biométrique sur un support individuel détenu par le salarié.

Limiter strictement l'accès aux données aux personnes habilitées avec traçabilité documentée.

Réévaluer régulièrement la nécessité du dispositif et la pertinence de la biométrie face aux alternatives.

Prévoir une procédure de secours en cas de défaillance technique ou de refus légitime du salarié.

Former le personnel utilisateur à la sécurité du dispositif et aux droits des personnes concernées.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Traitement de données pour surveillance des salariés
Art. L.414-9 du Code du travail	Consultation/co-décision de la délégation du personnel
Loi modifiée du 1er août 2018	Protection des données à caractère personnel
Règlement (UE) 2016/679 (RGPD)	Articles 5, 9, 13-14, 32, 35, 36
Lignes directrices CNPD	Recommandations sur la biométrie en milieu professionnel

La biométrie reste une solution de dernier recours : son usage pour le simple contrôle horaire est expressément interdit par la CNPD. L'employeur engage sa responsabilité pénale (L.261-2) et administrative (jusqu'à 4 % du chiffre d'affaires mondial) en cas de mise en œuvre non justifiée.

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.