L'employeur peut-il imposer un contrôle d'accès par empreinte digitale ?

Réponse courte

Le contrôle d'accès par **empreinte digitale** ne peut être imposé que pour la protection de **zones sensibles** (laboratoires, salles serveurs, valeurs importantes), jamais pour la simple gestion horaire ou des présences. L'empreinte digitale est une **donnée sensible** au sens de l'article 9 du RGPD applicable en entreprise, dont le traitement est interdit sauf exception strictement encadrée.

L'employeur doit démontrer la **nécessité absolue** du dispositif et l'absence d'alternative (badge, code), réaliser une **AIPD** (article 35 RGPD), consulter la délégation du personnel (article L.414-9) et offrir une **solution alternative** aux salariés exerçant leur refus légitime de la collecte. À défaut, le dispositif est nul et les sanctions disciplinaires fondées sur lui inopposables.

Définition

Le **contrôle d'accès par empreinte digitale** désigne l'usage de la reconnaissance biométrique pour autoriser ou refuser l'accès à des locaux, équipements ou systèmes. Il implique la collecte et le traitement d'un gabarit biométrique unique permettant l'identification certaine du salarié.

Ces données relèvent des **catégories particulières** de l'article 9 du RGPD et bénéficient d'une protection renforcée. Leur traitement est interdit sauf exception légale strictement encadrée par la loi modifiée du 1er août 2018.

Questions fréquentes

L'employeur peut-il imposer un contrôle d'accès par empreinte digitale au Luxembourg ?

Uniquement pour la protection de zones sensibles (laboratoires, salles serveurs, valeurs importantes). L'empreinte digitale est une donnée sensible (article 9 RGPD), interdite sauf exception strictement encadrée.

L'empreinte digitale peut-elle servir à pointer ou gérer les présences ?

Non, la CNPD exclut son usage pour la pointeuse, le contrôle horaire ou la gestion de présence ordinaire. La biométrie est admissible uniquement pour la sécurité de zones à risque particulier.

Où conserver le gabarit d'empreinte digitale du salarié ?

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

Que faire en cas de fuite de données d'empreinte digitale ?

Notification obligatoire à la CNPD sous 72 heures (article 33 RGPD). Compte tenu du caractère sensible des données et des risques pour les salariés, l'information des personnes concernées peut s'imposer (article 34 RGPD).

Quelles sanctions en cas de dispositif d'empreinte digitale non justifié ?

Sanctions administratives RGPD jusqu'à 4 % du chiffre d'affaires mondial, nullité des sanctions disciplinaires fondées sur le dispositif et action en discrimination si un salarié a été sanctionné pour refus légitime.

Un salarié peut-il refuser de donner son empreinte digitale ?

Oui légitimement. L'employeur doit prévoir une solution alternative non biométrique documentée et non discriminatoire. Sanctionner un refus légitime constitue une discrimination indemnisable au regard de l'article L.241-1.

Conditions d’exercice

L'empreinte digitale est admissible uniquement pour la sécurité de zones à risque particulier ; la CNPD exclut son usage pour la pointeuse, le contrôle horaire ou la gestion de présence ordinaire.

Condition	Exigence
Nécessité absolue	Protection de zones sensibles ; alternative classique inopérante
Finalité exclue	Interdit pour le contrôle horaire ou la gestion des présences
Donnée sensible	Article 9 RGPD : interdiction sauf exception encadrée
Stockage local privilégié	Gabarit conservé sur support individuel détenu par le salarié
Solution alternative	Procédure non biométrique pour tout salarié refusant
Égalité de traitement	Aucune discrimination fondée sur le refus légitime

Modalités pratiques

L'AIPD est obligatoire pour tout dispositif d'empreinte digitale ; la CNPD doit être consultée préalablement si le risque résiduel reste élevé après les mesures d'atténuation.

Démarche	Précision
Analyse d'impact (AIPD)	Article 35 du RGPD, démonstration de la nécessité
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, droits, alternative non biométrique
Stockage sécurisé	Chiffrement et stockage local du gabarit privilégiés
Solution alternative	Procédure documentée et non discriminatoire
Notification de violation	À la CNPD sous 72h en cas de fuite (article 33 RGPD)

Pratiques et recommandations

Privilégier le stockage local du gabarit sur un support individuel (badge à puce, smartphone du salarié).

Limiter strictement l'accès aux gabarits aux personnes habilitées avec journalisation des consultations.

Prévoir une solution alternative pour les salariés refusant légitimement, sans aucune conséquence professionnelle.

Conserver les données pour la seule durée nécessaire à la finalité, puis les effacer de façon irréversible.

Documenter les mesures de sécurité et la justification de la nécessité dans le registre des traitements.

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
Art. L.241-1 du Code du travail	Égalité de traitement et non-discrimination
Loi modifiée du 1er août 2018	Protection des données à caractère personnel
Règlement (UE) 2016/679 (RGPD)	Articles 5, 9, 32, 33, 35, 36
Lignes directrices CNPD	Recommandations sur la biométrie en milieu professionnel

L'absence de justification sérieuse ou la mise en œuvre sans AIPD expose l'employeur à des sanctions administratives jusqu'à 4 % du chiffre d'affaires mondial et à la nullité des sanctions disciplinaires fondées sur le dispositif. La sanction d'un salarié refusant légitimement la biométrie constitue une discrimination indemnisable.