

# Reconnaissance faciale en entreprise : que dit la CNPD ?

## Réponse courte

La **CNPD** adopte une position **très restrictive** sur la reconnaissance faciale. Considérée comme un traitement de données biométriques sensibles au sens de l'article 9 du RGPD, elle ne peut être déployée que dans des cas exceptionnels, justifiés par une **nécessité impérieuse de sécurité** que d'autres moyens ne peuvent satisfaire.

Pour les usages courants (contrôle d'accès, pointage, suivi du temps de travail), la CNPD considère le dispositif **disproportionné**. L'employeur doit conduire une **analyse d'impact (AIPD)**, consulter la **délégation du personnel** et démontrer l'absence d'**alternative moins intrusive**. Le simple consentement des salariés ne suffit pas, du fait du **déséquilibre** dans la relation de travail.

## Définition

La **reconnaissance faciale** est un traitement biométrique permettant d'identifier ou d'authentifier une personne à partir des caractéristiques de son visage. Elle relève de l'article 9 du RGPD qui interdit en principe le traitement des données biométriques destinées à identifier une personne de manière unique.

Au Luxembourg, ce type de traitement fait l'objet d'une vigilance particulière de la **CNPD**, qui l'évalue à l'aune des principes de **nécessité, proportionnalité et minimisation**.

## Questions fréquentes

### Faut-il informer les visiteurs de la reconnaissance faciale ?

Oui, une notice détaillée et une signalétique sur site doivent informer les personnes concernées, y compris les visiteurs. Cette obligation découle des articles 13 et 14 du RGPD au titre du principe de transparence et du droit à l'information.

### Le consentement du salarié suffit-il pour la reconnaissance faciale ?

Non, le consentement du salarié ne constitue pas une base légale valable, car le lien de subordination prive le consentement de son caractère libre. La CNPD rappelle régulièrement ce principe pour les traitements biométriques en entreprise.

### Peut-on utiliser la reconnaissance faciale pour le pointage ?

Non, pour les usages courants (contrôle d'accès, pointage, suivi du temps de travail), la CNPD considère le dispositif disproportionné. Le badge ou la carte à puce répondent aux mêmes besoins sans collecter de données sensibles.

### Quand saisir la CNPD pour consultation préalable ?

Il convient de saisir la CNPD pour consultation préalable lorsque l'AIPD révèle un risque élevé résiduel, conformément à l'article 36 du RGPD. Cette consultation est fortement recommandée pour tout projet de reconnaissance faciale en entreprise.

### Que dit la CNPD sur la reconnaissance faciale en entreprise ?

La CNPD adopte une position très restrictive. Considérée comme un traitement de données biométriques sensibles au sens de l'article 9 du RGPD, la reconnaissance faciale ne peut être déployée que dans des cas exceptionnels justifiés par une nécessité impérieuse de sécurité.

## Quelles conditions pour déployer la reconnaissance faciale ?

L'employeur doit démontrer une nécessité impérieuse (centres de données, coffres), conduire une AIPD complète, consulter la délégation du personnel et démontrer l'absence d'alternative moins intrusive. La consultation préalable CNPD est recommandée si risque élevé.

## Conditions d'exercice

Seules une finalité impérieuse (centres de données, coffres), une nécessité démontrée et une AIPD obligatoire (art. 35 RGPD) justifient le dispositif, avec consultation de la délégation et notice individuelle aux personnes concernées.

Condition	Détail
Finalité impérieuse	Sécurité de zones critiques (centres de données, coffres)
Nécessité absolue	Démonstration qu'aucune autre solution ne convient
Proportionnalité	Limitation au strict minimum de personnes et de zones
AIPD obligatoire	Analyse d'impact préalable détaillée
Consultation	Avis de la délégation du personnel
Information	Notice individuelle aux personnes concernées

## Modalités pratiques

Tout projet de reconnaissance faciale exige une étude documentée des alternatives, une AIPD écrite, une consultation de la délégation et, en cas de risque résiduel élevé, une consultation préalable de la CNPD (art. 36).

Étape	Détail
Étude des alternatives	Documentation des solutions écartées et justification
AIPD	Analyse écrite des risques et mesures de mitigation
Consultation préalable CNPD	Recommandée si risque élevé résiduel (art. 36 RGPD)
Délégation	Avis écrit de la délégation du personnel
Information	Notice détaillée et signalétique sur site
Sécurité	Chiffrement, hébergement sécurisé, accès journalisé

## Pratiques et recommandations

**Écarter** la reconnaissance faciale pour le pointage horaire et les contrôles d'accès courants : la **CNPD** la juge disproportionnée.

**Privilégier** systématiquement le badge ou la carte à puce qui répondent aux mêmes besoins sans données sensibles.

**Conduire** une AIPD complète et la conserver pour la présenter en cas de contrôle de l'autorité.

**Saisir** la CNPD pour consultation préalable lorsque l'AIPD révèle un risque élevé résiduel, conformément à l'article 36 du RGPD.

**Consulter** la délégation du personnel et formaliser son avis dans un procès-verbal, conformément à l'article [L.261-1](#) du Code du travail.

## Cadre juridique

Le cadre repose sur les textes européens et luxembourgeois suivants.

Référence	Objet
Art. 9 RGPD	Interdiction de principe des traitements de données biométriques
Art. 35 RGPD	Analyse d'impact relative à la protection des données
Art. 36 RGPD	Consultation préalable de l'autorité de contrôle
Art. <a href="#">L.261-1</a> Code du travail	Surveillance des salariés et protection des données
Art. <a href="#">L.414-9</a> Code du travail	Consultation de la délégation du personnel
Loi du 1er août 2018	Régime général au Luxembourg

Le consentement du salarié ne constitue pas une base légale valable pour la reconnaissance faciale en entreprise, car le **lien de subordination** prive le consentement de son caractère libre. La **CNPD** rappelle régulièrement ce principe.

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.