Travail &
Données personnelles

L'accès aux locaux et le contrôle des horaires

Parce que les locaux professionnels ne sont pas ouverts à tous et que les employeurs comme les employés ont besoin de connaître les horaires effectués, les contrôles d'accès et du temps de travail existent depuis bien longtemps. Le développement des technologies facilite ces contrôles mais permet aussi de collecter bien plus d'informations sur les personnes concernées. Des limites à leur utilisation sont donc indispensables pour préserver les droits et libertés de chacun.

Dans quel but ?

L'employeur peut mettre en place des outils – y compris biométriques – de contrôle individuel de l'accès pour sécuriser :

- l'entrée dans les bâtiments,
- les locaux faisant l'objet d'une restriction de circulation.

Ces dispositifs peuvent concerner les employés comme les visiteurs.

Des dispositifs non biométriques peuvent également être utilisés pour gérer les horaires et le temps de présence des employés.

Quelles garanties pour la vie privée ?

Le système mis en place ne doit pas servir au contrôle des déplacements à l'intérieur des locaux.

Le dispositif ne doit pas entraver la liberté d'aller et venir des représentants du personnel dans l'exercice de leur mandat, ou être utilisé pour contrôler le respect de leurs heures de délégation.

Qui peut accéder aux données ?

Les informations ne sont accessibles qu'aux membres habilités des services gérant le personnel, la paie, ou la sécurité.

L'employeur doit prévoir des mesures pour assurer la sécurité des informations concernant ses salariés et éviter que des personnes qui n'ont pas qualité pour y accéder puissent en prendre connaissance. Ainsi, il doit prévoir des habilitations pour les accès informatiques avec une traçabilité des actions effectuées (savoir qui se connecte à quoi, quand et pour quoi faire).

Quelle durée de conservation ?

- Les données relatives aux accès doivent être supprimées **3 mois après leur enregistrement.**
- Les données utilisées pour le suivi du temps de travail, y compris les données relatives aux motifs des absences, **doivent être conservées pendant 5 ans.**

L'information des salariés

Les instances représentatives du personnel doivent être informées ou consultées avant toute décision d'installer un dispositif de contrôle des horaires ou d'accès aux locaux.

Chaque employé doit être notamment informé :
- des finalités poursuivies,
- de la base légale du dispositif (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur),
- des destinataires des données issues du dispositif,
- de la durée de conservation des données,
- de son droit d'opposition pour motif légitime,
- de ses droits d'accès et de rectification,
- de la possibilité d'introduire une réclamation auprès de la CNIL.

Cette information peut se faire au moyen d'un avenant au contrat de travail ou d'une note de service, par exemple.

L'accès aux locaux et le contrôle des horaires

Quelles sécurités ?

Pour éviter notamment que des personnes non autorisées accèdent aux données du dispositif, il est impératif de prendre des mesures de sécurité. Par exemple, l'accès au logiciel de gestion du contrôle d'accès ou des horaires doit être limité aux personnes qui ont besoin d'en connaître et se faire avec un identifiant et un mot de passe.

Il faut également impérativement prévoir :

- une politique d'habilitation,
- une sécurisation des échanges,
- une journalisation des accès aux données et des opérations, effectuées.

Une étude des risques sur la sécurité des données est également souhaitable afin de définir les mesures les mieux adaptées, notamment lorsqu'un dispositif biométrique est mis en place.

Quelles formalités ?

Les dispositifs sans biométrie

Le contrôle d'accès sans biométrie est à privilégier, dès lors qu'un système de badge est suffisant ou que les locaux ne sont pas particulièrement sensibles.

Attention, la CNIL estime que la biométrie est un moyen disproportionné de contrôle des horaires des employés.

Les dispositifs avec biométrie

Le contrôle d'accès biométrique doit faire l'objet d'une analyse d'impact sur la protection des données (PIA). Cette démarche permet d'identifier les risques associés aux données personnelles concernées par le dispositif, et à en réduire soit la vraisemblance soit la gravité.

L'aide du fournisseur, de l'intégrateur ou de l'installateur du dispositif peut être utile.

Dans ces situations, l'employeur doit privilégier le stockage du gabarit biométrique de l'employé sur un support individuel.

Si l'organisme a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en œuvre de ce dispositif.
L'employeur doit inscrire ce dispositif de contrôle dans son registre des activités de traitement de données.

Quels recours ?

En cas de difficulté, vous pouvez saisir :

- le service des plaintes de la CNIL,
- l'inspection du Travail,
- le procureur de la République.

Textes de référence

- **Le code civil :**
  Article 9 (protection de l'intimité de la vie privée)
- **Le code du travail :**
  Article L. 1121-1 (droits et libertés dans l'entreprise)
  Article L. 1222-3 et L. 1222-4 (information des employés)
  Article L. 2323-32 (information/consultation du comité d'entreprise)
- **Le code pénal :**
  Articles 226-1 et suivants (protection de la vie privée)
- Le Règlement européen sur la protection des données personnelles (RGPD)

Voir aussi

- Le contrôle d'accès biométrique sur les lieux de travail.
- L'analyse d'impact relative à la protection des données
- Guide de la sécurité des données personnelles

Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur **www.cnil.fr**. Vous pouvez également appeler la permanence juridique de la CNIL au **01 53 73 22 22**, les lundi, mardi, jeudi et vendredi de 10h à 12h et de 14h à 16h.