Qui peut accéder aux données issues de la surveillance des salariés ?

Réponse courte

L'accès aux données de surveillance est strictement limité aux **personnes nominativement habilitées** par l'employeur, dont la fonction le justifie au regard de la finalité déclarée. Sont concernés en pratique le responsable de traitement, le délégué à la protection des données, certains responsables RH ou sécurité, et le sous-traitant éventuel encadré par contrat conforme à l'article 28 du RGPD.

Les transmissions à des tiers externes ne sont possibles que sur **réquisition judiciaire**, obligation légale ou consentement explicite du salarié. Chaque consultation doit être **journalisée** (date, identité, motif), et les salariés disposent d'un droit d'accès aux données collectées (article 15 du RGPD). La liste des personnes habilitées figure au registre des traitements.

Définition

L'**habilitation d'accès** désigne l'autorisation formelle donnée par l'employeur à une personne précisément identifiée de consulter, exporter ou utiliser les données issues d'un dispositif de surveillance, dans la limite stricte de ses attributions professionnelles.

Cette habilitation s'inscrit dans le principe de **minimisation des accès** et concrétise le contrôle du responsable de traitement sur les flux de données personnelles, conformément aux articles 5, 29 et 32 du RGPD ainsi qu'à la loi modifiée du 1er août 2018.

Questions fréquentes

Comment tracer les consultations des données de surveillance ?

Chaque consultation doit être journalisée : identité, date, heure, motif et données consultées. Le journal doit être infalsifiable et constitue la première preuve de conformité en cas de contrôle CNPD.

Le partage d'identifiants pour accéder aux données de surveillance est-il autorisé ?

Non, aucun accès générique, partagé ou par défaut n'est admis. Chaque personne doit être identifiée individuellement avec authentification personnelle. Le partage d'identifiants constitue en soi une violation du RGPD.

Le salarié a-t-il un droit d'accès à ses propres données de surveillance ?

Oui, l'article 15 du RGPD garantit ce droit. La réponse doit être fournie sous 1 mois (article 12 RGPD), prolongeable de 2 mois si la demande est complexe. La procédure d'exercice doit être accessible.

Quand des données de surveillance peuvent-elles être transmises à un tiers externe ?

Uniquement sur réquisition judiciaire, obligation légale ou consentement explicite du salarié. Toute autre transmission constitue une violation sanctionnable. La régularité de la demande doit être vérifiée avant transmission.

Que faire en cas de mutation ou départ d'une personne habilitée ?

L'accès doit être révoqué immédiatement en cas de mutation, départ ou incident. La liste des habilités doit être révisée trimestriellement avec la hiérarchie et la sécurité informatique pour rester à jour.

Qui peut accéder aux données issues de la surveillance des salariés ?

L'accès est strictement limité aux personnes nominativement habilitées dont la fonction le justifie : responsable de traitement, DPO, certains responsables RH ou sécurité, et sous-traitant encadré par contrat conforme à l'article 28 RGPD.

Conditions d’exercice

Aucun accès générique, partagé ou par défaut n'est admis : chaque personne habilitée doit être identifiée individuellement et son accès tracé. Le partage d'identifiants est en soi une violation du RGPD.

Condition	Exigence
Désignation nominative	Liste écrite des personnes habilitées, mise à jour à chaque mouvement
Justification fonctionnelle	L'accès est lié à la fonction et limité à ce qui est strictement nécessaire
Authentification individuelle	Identifiants personnels, mots de passe robustes, double authentification
Journalisation	Trace horodatée de chaque consultation avec motif renseigné
Confidentialité	Engagement écrit de confidentialité signé par chaque personne habilitée

Modalités pratiques

La transmission à un tiers externe n'est possible que sur réquisition judiciaire, obligation légale ou consentement explicite du salarié ; toute autre communication constitue une violation sanctionnable.

Démarche	Précision
Liste des habilités	Document interne nominatif tenu à jour, intégré au registre des traitements
Engagement de confidentialité	Signature individuelle préalable à l'octroi de l'accès
Contrat de sous-traitance	Article 28 RGPD : engagements de sécurité et de confidentialité du prestataire
Journalisation des accès	Identité, date, heure, motif et données consultées
Droit d'accès du salarié	Réponse sous 1 mois (article 12 RGPD), prolongeable de 2 mois si complexe
Réquisition judiciaire	Vérification de la régularité de la demande avant transmission
Révocation	Retrait immédiat de l'accès en cas de mutation, départ ou incident

Pratiques et recommandations

Restreindre par défaut les accès et les ouvrir au cas par cas sur la base d'une justification écrite.

Réviser trimestriellement la liste des personnes habilitées avec la hiérarchie et la sécurité informatique.

Former chaque personne habilitée aux obligations RGPD et à la confidentialité avant l'octroi de l'accès.

Tracer chaque consultation à des fins probatoires par un journal infalsifiable.

Encadrer strictement les sous-traitants par contrat conforme à l'article 28 du RGPD, avec audit possible.

Sanctionner disciplinairement tout accès non justifié ou tout partage d'identifiants.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Traitement de données pour surveillance des salariés (loi du 1er août 2018)
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel pour les installations de contrôle
Loi modifiée du 1er août 2018	Protection des personnes à l'égard du traitement des données à caractère personnel
Art. 5, 15, 28, 29, 30, 32 du RGPD	Principes, droit d'accès, sous-traitance, instruction, registre, sécurité
Lignes directrices CNPD	Recommandations sur la gestion des accès aux données de surveillance

Un accès non autorisé aux données de surveillance constitue une violation de données notifiable à la CNPD et expose son auteur à des sanctions disciplinaires et pénales (article L.261-2). L'employeur reste responsable des accès consentis par ses préposés et sous-traitants. La traçabilité des consultations est la première preuve de conformité en cas de contrôle.