Quelles sont les obligations de l'entreprise en matière de sécurité des données de surveillance ?

Réponse courte

L'employeur doit mettre en place des **mesures techniques et organisationnelles appropriées** pour garantir la sécurité, l'intégrité et la confidentialité des données de surveillance (article 32 du RGPD) : contrôle des accès, chiffrement, pseudonymisation, journalisation des consultations, habilitation nominative et durée de conservation strictement limitée à la finalité.

Toute violation de données doit faire l'objet d'une notification à la CNPD sous 72 heures (article 33 RGPD) et, en cas de risque élevé, être communiquée aux salariés concernés (article 34 RGPD). Le **registre des traitements** doit être tenu à jour et l'AIPD réalisée pour les dispositifs à risque élevé. L'absence de mesures adaptées expose l'employeur à des sanctions jusqu'à 2 % du chiffre d'affaires mondial.

Définition

Les **données de surveillance** sont les informations collectées par l'employeur via des dispositifs de contrôle des salariés : vidéosurveillance, géolocalisation, contrôle d'accès, surveillance informatique, biométrie. Elles constituent des **données à caractère personnel** dès lors qu'elles permettent d'identifier directement ou indirectement une personne.

Leur sécurité repose sur les **principes d'intégrité et de confidentialité** posés par l'article 5(1)(f) du RGPD et sur les mesures techniques et organisationnelles de l'article 32, étendues par contrat à toute sous-traitance du contrôle (article 28). La sécurité fait partie intégrante de l'**accountability** du responsable de traitement.

Questions fréquentes

Comment encadrer un sous-traitant intervenant sur les données de surveillance ?

Le sous-traitant doit être encadré par contrat conforme à l'article 28 RGPD avec engagements de sécurité et de confidentialité. La responsabilité du donneur d'ordre reste engagée en cas de manquement du prestataire.

Dans quel délai notifier une violation de données de surveillance à la CNPD ?

Toute violation de données doit être notifiée à la CNPD sous 72 heures (article 33 RGPD). En cas de risque élevé pour les salariés, elle doit aussi être communiquée aux personnes concernées (article 34 RGPD).

Que signifie la protection by design pour un dispositif de surveillance ?

L'article 25 RGPD impose d'intégrer la protection des données dès la conception du dispositif, avec des paramètres restrictifs par défaut. Les mesures de sécurité doivent être proportionnées au niveau de risque du traitement.

Quelle sanction en cas d'absence de mesures de sécurité adaptées ?

L'absence de mesures de sécurité adaptées expose l'employeur à des sanctions jusqu'à 2 % du chiffre d'affaires mondial (article 83(4) RGPD), à des actions civiles et à la nullité des sanctions disciplinaires fondées sur des données compromises.

Quelles mesures techniques sont attendues pour la sécurité des données de surveillance ?

Authentification forte avec habilitation nominative et traçabilité, chiffrement et pseudonymisation (article 32(1)(a)), journalisation de chaque consultation, audits réguliers (article 32(1)(d)) et mécanismes de sauvegarde et continuité.

Quelles sont les obligations de sécurité des données de surveillance des salariés ?

L'employeur doit mettre en place des mesures techniques et organisationnelles appropriées (article 32 RGPD) : contrôle des accès, chiffrement, pseudonymisation, journalisation des consultations, habilitation nominative et durée de conservation strictement limitée à la finalité.

Conditions d’exercice

La sécurité doit être adaptée au niveau de risque : plus le traitement est sensible (biométrie, surveillance permanente), plus les mesures doivent être robustes ; les contrôles doivent être documentés.

Condition	Exigence
Adéquation au risque	Mesures proportionnées à la sensibilité du traitement
Confidentialité	Accès limité aux personnes habilitées, contrats de confidentialité
Intégrité	Garantie contre l'altération ou la destruction non autorisée
Disponibilité	Sauvegardes, plan de continuité, restauration
Protection by design	Article 25 RGPD, dès la conception du dispositif
Protection by default	Paramètres de protection les plus restrictifs par défaut

Modalités pratiques

La notification à la CNPD sous 72 heures en cas de violation est impérative ; l'absence de procédure interne de gestion des incidents constitue elle-même un manquement aux mesures organisationnelles.

Démarche	Précision
Contrôle des accès	Authentification forte, habilitation nominative, traçabilité
Chiffrement et pseudonymisation	Article 32(1)(a) RGPD, à privilégier dès que possible
Journalisation	Trace de chaque consultation et opération sur les données
Registre des traitements	Article 30 RGPD, mesures de sécurité décrites
Notification de violation	À la CNPD sous 72 heures (article 33 RGPD)
Communication aux salariés	En cas de risque élevé (article 34 RGPD)
Audits réguliers	Article 32(1)(d) RGPD : tests et évaluations

Pratiques et recommandations

Réaliser une AIPD pour tout dispositif de surveillance susceptible d'engendrer un risque élevé.

Former les personnes habilitées à la sécurité et à la confidentialité des données.

Auditer régulièrement la sécurité technique et organisationnelle du dispositif.

Encadrer par contrat tout sous-traitant intervenant sur les données (article 28 RGPD).

Documenter chaque incident, mesure correctrice et notification à la CNPD.

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(1)(f), 24, 25, 28, 30, 32, 33, 34, 35
Lignes directrices CNPD	Sécurité des traitements et notification des violations

L'absence de mesures de sécurité adaptées ou la conservation excessive des données expose l'employeur à des sanctions jusqu'à 2 % du chiffre d'affaires mondial (article 83(4) RGPD), à des actions civiles des salariés pour atteinte aux droits fondamentaux et à la nullité des sanctions disciplinaires fondées sur des données compromises.