Faut-il recueillir le consentement du salarié pour surveiller son poste informatique ?

Réponse courte

Le consentement du salarié n'est **pas requis** et n'est d'ailleurs **pas une base juridique valide** dans la relation de travail, en raison du déséquilibre structurel entre employeur et salarié. La surveillance du poste informatique repose sur l'**intérêt légitime** de l'employeur ou l'exécution du contrat (article 6 du RGPD), à condition de respecter les principes de **nécessité** et de **proportionnalité**.

L'employeur doit en revanche informer préalablement chaque salarié, consulter la délégation du personnel (article L.414-9 du Code du travail pour les entreprises d'au moins 150 salariés) et tenir le registre des traitements. L'absence d'information préalable rend le dispositif illicite et les preuves obtenues sont **irrecevables** devant le tribunal du travail. Une analyse d'impact est obligatoire si le traitement présente un risque élevé.

Définition

La **surveillance du poste informatique** désigne l'ensemble des dispositifs techniques permettant à l'employeur de contrôler l'utilisation des outils numériques mis à disposition du salarié : accès Internet, courriels professionnels, fichiers, journaux de connexion, applications. Ce contrôle constitue un traitement de **données à caractère personnel** au sens du RGPD.

Il s'inscrit dans le pouvoir de direction de l'employeur mais doit respecter les droits fondamentaux du salarié, notamment la vie privée et la protection des données.

Questions fréquentes

Faut-il recueillir le consentement du salarié pour surveiller son poste informatique ?

Non, le consentement n'est pas requis et n'est pas une base juridique valide dans la relation de travail en raison du déséquilibre structurel entre employeur et salarié. La surveillance repose sur l'intérêt légitime ou l'exécution du contrat (article 6 RGPD).

Pourquoi le consentement du salarié n'est-il jamais valable pour la cybersurveillance ?

Le lien de subordination empêche le salarié de donner un consentement libre. Le consentement obtenu sous lien de subordination n'est jamais valable et ne peut régulariser un dispositif illicite. La base correcte reste l'intérêt légitime de l'employeur.

Quelle base juridique invoquer pour la surveillance d'un poste informatique ?

L'intérêt légitime de l'employeur ou l'exécution du contrat de travail (article 6 RGPD). L'employeur doit documenter le test de mise en balance entre cet intérêt et les droits du salarié, à respecter les principes de nécessité et de proportionnalité.

Quelle durée de conservation pour les logs informatiques au Luxembourg ?

Strictement nécessaire à la finalité, généralement 6 à 12 mois pour les logs. La collecte doit être limitée aux métadonnées techniques avec exclusion de tout accès au contenu des messages identifiés comme privés.

Quelles obligations en pratique pour surveiller un poste informatique ?

Information préalable individuelle (articles 12-13 RGPD), consultation de la délégation du personnel (L.414-9), tenue du registre des traitements (article 30 RGPD), AIPD si risque élevé (article 35 RGPD), habilitation des accès et durée de conservation limitée.

Quelles sanctions pour une cybersurveillance sans information préalable ?

Le dispositif est nul, les preuves sont écartées par le tribunal du travail. L'employeur s'expose à des amendes administratives RGPD jusqu'à 4 % du chiffre d'affaires mondial et à des sanctions pénales L.261-2.

Conditions d’exercice

Le consentement du salarié n'est jamais valable comme base juridique en raison du lien de subordination ; la base correcte est l'intérêt légitime ou l'exécution du contrat (article 6 RGPD).

Condition	Exigence
Base juridique	Intérêt légitime ou exécution du contrat (article 6 RGPD) — pas le consentement
Finalité légitime	Sécurité du système d'information, prévention des intrusions, contrôle limité des obligations professionnelles
Proportionnalité	Limitation aux données techniques strictement nécessaires ; pas d'accès aux contenus identifiés comme privés
Information préalable	Notice individuelle écrite à chaque salarié avant la mise en service
Consultation	Délégation du personnel selon L.414-9 ou ITM à défaut

Modalités pratiques

L'information préalable conditionne la licéité : sans notice écrite remise individuellement, le dispositif est nul et les preuves issues du contrôle sont écartées par le tribunal du travail.

Démarche	Précision
Notice individuelle	Finalité, données collectées, durée de conservation, destinataires, droits (articles 12-13 RGPD)
Charte informatique	Annexée au règlement intérieur ou contrat ; rappel de la distinction usage privé/professionnel
Consultation délégation	Procès-verbal préalable obligatoire (L.414-9)
AIPD	Obligatoire si risque élevé (article 35 RGPD)
Registre des traitements	Article 30 RGPD — finalité, durée, destinataires, mesures de sécurité
Habilitation des accès	Liste nominative des personnes autorisées avec traçabilité
Durée de conservation	Strictement nécessaire à la finalité, généralement 6 à 12 mois pour les logs

Pratiques et recommandations

Limiter la collecte aux métadonnées techniques et exclure tout accès au contenu des messages identifiés comme privés.

Documenter la base juridique retenue (intérêt légitime) et le test de mise en balance avec les droits du salarié.

Sécuriser les accès aux journaux par authentification forte et journalisation des consultations.

Distinguer clairement, dans la charte, les usages professionnels et les usages privés tolérés.

Encadrer par contrat tout sous-traitant intervenant sur le SI conformément à l'article 28 du RGPD.

Réviser annuellement la pertinence et la proportionnalité du dispositif avec la délégation du personnel.

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.261-2 du Code du travail	Sanctions pénales en cas de violation
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel (? 150 salariés)
Loi modifiée du 1er août 2018	Protection des personnes à l'égard du traitement des données
Règlement (UE) 2016/679 (RGPD)	Articles 5, 6, 12-13, 28, 30, 32, 35
Lignes directrices CNPD	Surveillance sur le lieu de travail

Le consentement obtenu sous lien de subordination n'est jamais valable et ne peut régulariser un dispositif illicite. L'absence d'information préalable expose l'employeur à des amendes administratives jusqu'à 4 % du chiffre d'affaires mondial et à des sanctions pénales (L.261-2). Les preuves issues du dispositif sont irrecevables devant le tribunal du travail.