L'employeur peut-il surveiller les outils collaboratifs comme Slack, Teams ou Microsoft 365 ?

Réponse courte

L'employeur peut activer un **niveau minimal de journalisation** sur les outils collaboratifs (Slack, Teams, Microsoft 365) pour des raisons de sécurité informatique et de conservation légale, mais l'utilisation des **fonctions analytiques avancées** (Viva Insights, Workplace Analytics, dashboards de productivité individuels) est presque toujours **disproportionnée** au regard du RGPD applicable en entreprise. Le contenu des conversations privées entre salariés ne peut jamais faire l'objet d'une analyse systématique.

Avant tout déploiement, l'employeur doit réaliser une analyse d'impact sur la protection des données, consulter la **délégation du personnel** (L.414-9), informer chaque salarié des modalités précises de la journalisation et préférer les **agrégations anonymisées** aux indicateurs nominatifs. Toute analyse comportementale individualisée constitue un traitement à risque élevé, susceptible de sanctions CNPD jusqu'à 4 % du chiffre d'affaires mondial.

Définition

La **surveillance des outils collaboratifs** désigne l'usage des fonctions natives ou tierces de journalisation, d'analyse ou de dashboard intégrées aux plateformes Slack, Microsoft Teams, Microsoft 365 et équivalents. Elle inclut les **logs techniques** (connexions, partages, créations de canaux), les **analytics de productivité** (temps de focus, réunions, messages envoyés) et les **rapports administrateurs**.

Ces fonctions, fournies par défaut par les éditeurs, créent un **traitement de données à caractère personnel** dès lors qu'elles permettent d'identifier ou d'individualiser un salarié.

Questions fréquentes

Combien de temps conserver les logs techniques des outils collaboratifs ?

Strictement le temps nécessaire à la finalité, généralement 6 mois maximum pour les logs. Toute durée supérieure exige une justification documentée au regard du principe de minimisation (article 5 RGPD).

Faut-il informer les salariés des fonctions analytiques actives sur Teams ou Slack ?

Oui, une notice détaillée doit lister les indicateurs collectés, leur usage, les destinataires et la durée de conservation. Cette obligation découle des articles 13 RGPD et L.261-1 du Code du travail luxembourgeois.

Faut-il une AIPD avant d'activer les analytics Microsoft 365 ou Slack ?

Oui, l'AIPD est presque systématiquement obligatoire dès qu'une fonction analytique est activée (risque élevé). Elle doit être accompagnée de la consultation de la délégation (L.414-9) pour les entreprises ? 150 salariés.

L'employeur peut-il analyser l'activité Slack ou Teams des salariés ?

Une journalisation technique minimale pour la sécurité et la conservation légale est admise, mais les analytics avancés (Viva Insights, Workplace Analytics, dashboards de productivité individuels) sont presque toujours disproportionnés au regard du RGPD.

Les conversations privées entre salariés sur Teams peuvent-elles être analysées ?

Non, le contenu des conversations privées entre salariés ne peut jamais faire l'objet d'une analyse systématique. Cette pratique constitue un traitement à risque élevé, susceptible de sanctions CNPD jusqu'à 4 % du chiffre d'affaires mondial.

Qui peut accéder aux logs des outils collaboratifs dans l'entreprise ?

L'accès doit être restreint aux administrateurs IT et au DPO, avec journalisation des consultations. Les managers ne doivent pas avoir d'accès direct aux dashboards individuels, qui doivent être désactivés par défaut au niveau du tenant.

Viva Insights peut-il être utilisé pour évaluer la productivité individuelle ?

Non, l'analyse individualisée du temps de focus, du nombre de messages ou de la fréquence des réunions est jugée disproportionnée. Seules les vues agrégées par équipe (? 5 personnes) sont admises pour des finalités managériales générales.

Conditions d’exercice

L'analyse individualisée du temps de focus, du nombre de messages envoyés ou de la fréquence des réunions est jugée disproportionnée par les autorités européennes ; seules les vues agrégées ou anonymisées par équipe sont admises pour des finalités managériales générales.

Condition	Exigence
Finalité limitée	Sécurité informatique, conservation légale, gestion technique — exclu : évaluation individuelle de productivité
Niveau minimal	Journalisation technique uniquement ; pas d'activation des dashboards individuels par défaut
Anonymisation	Vues agrégées par équipe (? 5 personnes) plutôt que par salarié
AIPD obligatoire	Risque élevé presque systématique dès qu'une fonction analytique est activée
Consultation délégation	Co-décision L.414-9 pour les entreprises ? 150 salariés ; information sinon
Information individuelle	Notice détaillant les indicateurs collectés, leur usage et les destinataires

Modalités pratiques

La désactivation par défaut des dashboards individuels (Viva Insights manager view, Workplace Analytics) est la mesure la plus efficace pour respecter la proportionnalité ; l'activation au cas par cas exige une justification documentée.

Démarche	Précision
Inventaire des fonctions actives	Cartographier toutes les options analytiques activées sur le tenant
Désactivation par défaut	Décocher les fonctions de productivité individualisée à l'échelle du tenant
AIPD ciblée	Réaliser une analyse d'impact pour chaque fonction conservée
Consultation délégation	Présenter les fonctions retenues et leur finalité, recueillir l'accord ou les avis
Notice salariés	Liste des données journalisées et durées de conservation
Habilitation des accès	Restriction aux administrateurs IT et au DPO ; pas d'accès managérial direct
Durée de conservation	Strictement nécessaire à la finalité (généralement 6 mois maximum pour les logs)

Pratiques et recommandations

Désactiver systématiquement les dashboards de productivité individuels (Viva Insights manager view) qui ne sont presque jamais proportionnés.

Préférer les agrégations par équipe ou département aux indicateurs nominatifs pour les finalités managériales générales.

Documenter chaque fonction analytique conservée par une AIPD spécifique justifiant la nécessité et la proportionnalité.

Informer les salariés via une notice détaillée listant les indicateurs collectés, le rythme et les destinataires.

Restreindre les accès aux logs techniques aux seuls administrateurs et DPO, avec journalisation des consultations.

Réexaminer annuellement l'utilité réelle de chaque fonction et désactiver celles qui ne servent pas à la finalité initiale.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Traitement des données pour surveillance des salariés
Art. L.414-9 du Code du travail	Consultation/co-décision de la délégation du personnel
Règlement (UE) 2016/679 (RGPD)	Articles 5, 6, 25 (protection by design), 35 (AIPD)
Loi modifiée du 1er août 2018	Cadre national luxembourgeois
Lignes directrices CEPD 8/2020	Réseaux sociaux et plateformes collaboratives
Recommandations CNPD	Cybersurveillance sur le lieu de travail

L'activation par défaut des dashboards de productivité individuels sans AIPD ni consultation est presque toujours qualifiée de manquement par la CNPD. Les sanctions atteignent 4 % du chiffre d'affaires mondial et toute évaluation individuelle fondée sur ces données est inopposable.