Quelle est la durée légale de conservation des logs de connexion des salariés au Luxembourg ?

Réponse courte

Aucun **seuil légal unique** ne fixe la durée de conservation des journaux d'activité informatique : la durée doit être **strictement nécessaire** à la finalité poursuivie (article 5(1)(e) du RGPD). La CNPD recommande une approche par finalité, avec une durée généralement comprise entre **6 et 12 mois** pour les finalités de sécurité, plus courte pour le contrôle d'activité ordinaire.

L'employeur fixe la durée préalablement, l'inscrit au registre des traitements et la justifie au regard de la finalité. Une conservation prolongée n'est admise qu'en cas d'incident de sécurité documenté ou de procédure judiciaire en cours. La consultation préalable de la délégation du personnel (article L.414-9) et l'information individuelle des salariés sont impératives.

Définition

Les **logs de connexion** sont des enregistrements automatiques documentant les accès et activités des utilisateurs sur les systèmes d'information : identifiants, dates, heures, adresses IP, ressources consultées. Ils constituent des **données à caractère personnel** dès lors qu'ils permettent d'identifier un salarié.

Leur conservation est régie par le principe de **limitation de la conservation** (article 5(1)(e) RGPD) et par le principe d'**accountability** (article 5(2)) : aucune durée légale fixe n'est imposée, l'employeur doit justifier la durée retenue par finalité.

Questions fréquentes

Comment justifier la durée de conservation des logs auprès de la CNPD ?

L'employeur fixe la durée préalablement, l'inscrit au registre des traitements et la motive par finalité. Toute durée supérieure à 12 mois exige une motivation renforcée et documentée dans le registre.

Faut-il consulter la délégation pour définir la durée de conservation des logs ?

Oui, la consultation préalable de la délégation du personnel est impérative (article L.414-9). Un procès-verbal doit être dressé. L'information individuelle de chaque salarié sur la durée retenue est également obligatoire.

Peut-on appliquer la même durée pour tous les logs de l'entreprise ?

Non, la CNPD recommande une approche par finalité plutôt qu'un seuil unique. La sécurité, l'audit et les obligations légales appellent des durées différenciées, justifiées dans la politique de conservation et le registre.

Que faire en cas d'incident de sécurité justifiant une conservation prolongée ?

La conservation prolongée n'est admise qu'en cas d'incident documenté ou de procédure judiciaire en cours. Une justification écrite est obligatoire et l'exception est tracée dans le registre des traitements.

Quelle est la durée légale de conservation des logs de connexion au Luxembourg ?

Aucun seuil légal unique n'existe. La durée doit être strictement nécessaire à la finalité (article 5(1)(e) RGPD). La CNPD recommande 6 à 12 mois pour la sécurité informatique, plus courte pour le contrôle d'activité ordinaire.

Quels documents formaliser autour de la conservation des logs ?

L'employeur doit produire une politique de conservation, la charte informatique, le registre des traitements (article 30 RGPD), une notice individuelle aux salariés et un procès-verbal de consultation de la délégation du personnel.

Conditions d’exercice

La durée se détermine au cas par cas selon la finalité et doit être justifiée dans le registre ; toute durée supérieure à 12 mois exige une motivation renforcée et documentée.

Condition	Exigence
Pas de seuil fixe	Durée fixée par finalité, sans plafond légal unique
Sécurité informatique	Généralement 6 à 12 mois, justifiable au cas par cas
Contrôle d'activité	Durée plus courte, strictement limitée à la finalité
Justification	Durée motivée et inscrite au registre des traitements
Information préalable	Notice individuelle remise à chaque salarié
Consultation	Délégation du personnel (article L.414-9)

Modalités pratiques

La durée est définie dans la charte informatique et la politique de conservation, validée par le DPO et présentée à la délégation du personnel pour consultation.

Démarche	Précision
Politique de conservation	Grille des durées par finalité, validée par le DPO
Registre des traitements	Article 30 du RGPD, durée justifiée et tracée
Charte informatique	Mention de la durée et des conditions d'accès
Information individuelle	Notice écrite remise à chaque salarié
Suppression automatisée	Mécanisme technique de purge à l'échéance
Conservation prolongée	Justifiée par incident ou procédure judiciaire
Consultation de la délégation	Procès-verbal préalable (article L.414-9)

Pratiques et recommandations

Différencier les durées selon la finalité (sécurité, audit, obligation légale) plutôt qu'appliquer un seuil unique.

Automatiser la suppression des logs à l'échéance pour fiabiliser la conformité.

Documenter dans le registre la justification de chaque durée et de toute conservation prolongée.

Limiter l'accès aux logs aux personnes habilitées avec traçabilité des consultations.

Réévaluer annuellement la pertinence des durées retenues avec le DPO.

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)(e), 5(2), 6, 30, 32
Lignes directrices CNPD	Cybersurveillance et conservation des logs

La conservation au-delà de la durée nécessaire à la finalité expose l'employeur à des sanctions administratives jusqu'à 4 % du chiffre d'affaires mondial. La traçabilité des durées dans le registre conditionne la défense en cas de contrôle de la CNPD ou de l'ITM.