Quelles sont les obligations en matière de RGPD concernant les logs de connexion des salariés au Luxembourg ?

Réponse courte

Les logs de connexion des salariés au Luxembourg sont considérés comme des données à caractère personnel et leur traitement doit respecter le RGPD ainsi que la législation nationale. L'employeur doit définir une finalité précise, informer individuellement les salariés par écrit, limiter la collecte aux données strictement nécessaires, restreindre l'accès aux personnes habilitées, et conserver les logs pour une durée maximale de six mois, sauf justification particulière. Toute utilisation à des fins disciplinaires doit avoir été expressément portée à la connaissance des salariés.

Une analyse d'impact est requise en cas de risque élevé, et toute surveillance généralisée ou disproportionnée est interdite. L'ensemble du traitement doit être documenté dans le registre des activités, sécurisé par des mesures techniques et organisationnelles, et faire l'objet d'audits réguliers. Toute violation de données doit être notifiée à la CNPD dans les 72 heures.

Définition

Les logs de connexion correspondent aux enregistrements informatiques retraçant l'accès d'un utilisateur à un système d'information, incluant notamment les dates, heures, adresses IP, identifiants et actions réalisées. Au Luxembourg, ces logs sont considérés comme des **données à caractère personnel** dès lors qu'ils permettent d'identifier, directement ou indirectement, un salarié.

Leur traitement relève du **Règlement (UE) 2016/679 (RGPD)** et de la législation nationale, notamment la loi du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. La CNPD encadre strictement leur utilisation, en particulier dans le contexte professionnel.

Conditions d'exercice

La collecte et le traitement des logs de connexion doivent répondre à une **finalité déterminée, explicite et légitime**, telle que la sécurité du système d'information, la prévention des accès non autorisés ou la gestion des incidents. Le traitement doit reposer sur une **base légale** appropriée, généralement l'intérêt légitime de l'employeur (article 6, RGPD), sous réserve que cet intérêt ne porte pas atteinte aux droits et libertés des salariés.

L'information préalable des salariés sur la nature, la finalité et la durée de conservation des logs est **obligatoire** (articles L.261-1 et suivants du Code du travail, article 13 RGPD). Une **analyse d'impact relative à la protection des données (AIPD)** est requise si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées (article 35 RGPD).

Toute surveillance généralisée, systématique ou disproportionnée est interdite. L'égalité de traitement et la non-discrimination doivent être garanties (article L.241-1 du Code du travail).

Modalités pratiques

L'employeur doit limiter la collecte des logs aux **données strictement nécessaires** à la finalité poursuivie (principe de minimisation, article 5 RGPD). La durée de conservation ne peut excéder **six mois**, sauf nécessité particulière dûment justifiée et documentée, par exemple en cas d'enquête interne ou d'obligation légale spécifique (avis CNPD, article 5 RGPD).

L'accès aux logs doit être restreint aux seules personnes habilitées, telles que les administrateurs systèmes ou le service informatique, dans le cadre de leurs missions. Toute consultation des logs doit être **tracée et justifiée**.

Les salariés doivent être informés individuellement, par écrit, des modalités de traitement des logs, notamment via une politique informatique ou une note de service (article L.261-1 du Code du travail, article 13 RGPD). Les logs ne peuvent être utilisés à des fins disciplinaires que si cette possibilité a été **expressément portée à la connaissance des salariés** (article L.261-1(2) du Code du travail).

Pratiques et recommandations

Il est recommandé de formaliser une **politique interne** détaillant les conditions de collecte, d'accès, de conservation et de suppression des logs de connexion. Cette politique doit être validée par le **délégué à la protection des données (DPO)** et communiquée à l'ensemble du personnel.

L'employeur doit assurer la **sécurité des logs** par des mesures techniques et organisationnelles appropriées, telles que le chiffrement et le contrôle d'accès (article 32 RGPD). Toute violation de données doit être notifiée à la CNPD dans les 72 heures et, le cas échéant, aux personnes concernées (articles 33 et 34 RGPD).

L'ensemble des traitements doit être documenté dans le **registre des activités de traitement** (article 30 RGPD), en précisant la finalité, la base légale, les catégories de données, les destinataires et la durée de conservation. Un **audit régulier** des pratiques de gestion des logs est conseillé pour garantir la conformité continue.

Cadre juridique

- **Code du travail luxembourgeois** :
  - Article L.261-1 et suivants (surveillance sur le lieu de travail, information préalable, consultation des représentants du personnel)
  - Article L.241-1 (égalité de traitement)
- **Règlement (UE) 2016/679 (RGPD)** :
  - Article 5 (principes relatifs au traitement)
  - Article 6 (licéité du traitement)
  - Article 13 (information des personnes concernées)
  - Article 30 (registre des activités de traitement)
  - Article 32 (sécurité du traitement)
  - Articles 33 et 34 (notification des violations de données)
  - Article 35 (analyse d'impact)
- **Loi du 1er août 2018** relative à la protection des personnes à l'égard du traitement des données à caractère personnel
- **Lignes directrices et décisions de la CNPD**

L'absence d'information préalable des salariés, la conservation excessive des logs ou l'absence de consultation des représentants du personnel exposent l'employeur à des sanctions administratives de la CNPD et à des actions en responsabilité civile. Toute surveillance doit être encadrée par une intervention humaine et respecter le principe de proportionnalité.