Quelles sont les règles de protection des données lors du télétravail frontalier ?

Réponse courte

Le télétravail frontalier implique le **transfert de données professionnelles** vers le domicile du salarié situé dans un autre pays. L'employeur reste le **responsable du traitement** au sens du RGPD et doit garantir un niveau de sécurité équivalent à celui du bureau, conformément à l'article L.261-1 du **Code du travail** et au **Règlement (UE) 2016/679**, comme précisé dans la fiche sur audit RGPD pour les postes de télétravail.

Définition

La **protection des données** en contexte de télétravail frontalier désigne l'ensemble des mesures techniques et organisationnelles que l'employeur doit mettre en place pour sécuriser les données à caractère personnel traitées par le salarié depuis son domicile à l'étranger, dans le respect du RGPD et de la loi luxembourgeoise du 1er août 2018, comme précisé dans la fiche sur information de la CNPD en cas de télétravail transfrontalier.

Conditions d’exercice

L'employeur doit respecter plusieurs obligations cumulatives.

Obligation	Description
Analyse d'impact (DPIA)	Réaliser une analyse d'impact si le télétravail implique un traitement à grande échelle
Mesures techniques	Fournir un VPN, chiffrement des données, authentification forte
Politique d'utilisation	Définir les règles d'usage des équipements professionnels à domicile
Notification CNPD	Notifier la CNPD en cas de traitement de surveillance des salariés
Information du salarié	Informer le salarié des traitements et de ses droits (Art. 13-14 RGPD)

Modalités pratiques

L'employeur met en place les mesures suivantes.

Élément	Détail
Charte informatique	Rédiger une charte spécifique au télétravail transfrontalier
Équipements sécurisés	Fournir des équipements professionnels configurés et mis à jour
Formation	Former les télétravailleurs aux bonnes pratiques de cybersécurité
Procédure de violation	Établir une procédure de notification des violations de données (72 heures)
Audit régulier	Réaliser des audits de conformité RGPD périodiques

Pratiques et recommandations

Il est recommandé de **séparer** strictement les usages professionnels et personnels sur les équipements de télétravail. L'employeur doit **former** régulièrement les salariés frontaliers aux risques cyber spécifiques au travail à domicile et **documenter** l'ensemble des mesures de sécurité dans un registre de traitements. La désignation d'un **délégué à la protection des données** (DPO) facilite la coordination des obligations RGPD en contexte transfrontalier.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Surveillance des salariés et protection des données
Art. L.261-2 du Code du travail	Limites du pouvoir de direction en matière de données
Règlement (UE) 2016/679 (RGPD)	Protection des données à caractère personnel
Loi du 1er août 2018	Organisation de la CNPD et protection des données
Convention du 20 octobre 2020	Cadre du télétravail, obligations de sécurité informatique

Le transfert de données vers le domicile du salarié dans un pays de l'UE ne constitue pas un transfert international au sens du RGPD, les pays frontaliers (France, Belgique, Allemagne) étant soumis au même règlement européen. Le risque principal réside dans la sécurisation physique et logique du poste distant.