

# Les audits RGPD sont-ils mutualisables entre plusieurs pays frontaliers ?

## Réponse courte

Les audits RGPD peuvent être **mutualisés** pour les aspects communs à tous les postes de télétravail transfrontalier : mesures techniques de sécurité (VPN, chiffrement, authentification multifacteur), politique de sécurité interne, registre des traitements et formation des salariés. L'employeur peut définir un **socle commun** d'exigences applicable quel que soit le pays de résidence du télétravailleur, réduisant ainsi les coûts de conformité, comme précisé dans la fiche sur [audit RGPD pour les postes de télétravail transfrontalier](#).

En revanche, certains aspects nécessitent une **évaluation par pays** : la coopération avec l'autorité de protection des données locale, les exigences spécifiques de la CNIL (France), de l'APD (Belgique) ou du BfDI (Allemagne), les règles locales de notification des violations et les éventuelles obligations de langue pour la documentation destinée aux salariés.

## Définition

La **mutualisation des audits RGPD** consiste à regrouper les vérifications de conformité applicables aux postes de télétravail situés dans différents pays frontaliers en un seul processus d'audit. Cette approche permet de réduire les coûts et d'harmoniser les pratiques tout en respectant les exigences spécifiques de chaque juridiction, comme précisé dans la fiche sur [protection des données en télétravail frontalier](#).

## Conditions d'exercice

La mutualisation est possible dans un cadre défini.

Mutualisable	Non mutualisable
Mesures techniques (VPN, chiffrement)	Coopération avec l'autorité locale
Politique de sécurité	Exigences réglementaires nationales
Formation des salariés	Analyse d'impact spécifique au pays
Registre des traitements	Procédure de notification locale
Checklist ergonomique	Langue de la documentation

## Modalités pratiques

L'employeur structure l'audit RGPD en deux niveaux.

Niveau	Détail
Socle commun	Mesures techniques, politique de sécurité, formation
Volet national	Exigences locales de chaque autorité de contrôle
Fréquence	Audit du socle commun annuel, volet national selon besoin
Prestataire	Cabinet spécialisé en droit européen de la donnée
Documentation	Rapport unique avec annexes par pays

## Pratiques et recommandations

**Définir** un socle commun de sécurité RGPD applicable à tous les postes de télétravail, incluant VPN, chiffrement, authentification multifacteur et formation cybersécurité.

**Compléter** le socle commun par des vérifications spécifiques aux exigences de la CNIL, de l'APD et du BfDI pour les salariés résidant respectivement en France, Belgique et Allemagne.

**Mandater** un prestataire unique spécialisé en protection des données transfrontalières pour réaliser l'audit mutualisé et réduire les coûts.

**Mettre à jour** le rapport d'audit en cas d'évolution des exigences d'une autorité de contrôle nationale, sans remettre en cause l'intégralité du dispositif.

## Cadre juridique

Le cadre juridique applicable repose sur les textes suivants.

Référence	Objet
Règlement (UE) 2016/679 (RGPD)	Cadre commun de protection des données
Art. 56-60 du RGPD	Mécanisme de coopération entre autorités
Art. L.261-1 du Code du travail	Surveillance des salariés
Loi du 1er août 2018	Organisation de la CNPD

La mutualisation ne dispense pas l'employeur de ses **obligations individuelles** envers chaque salarié. Chaque télétravailleur doit recevoir une information personnalisée sur les traitements de données le concernant, dans la langue qu'il comprend. Le DPO de l'entreprise coordonne la démarche d'audit mutualisé.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.