

# Quelles sont les sanctions en cas de non-respect du RGPD par l'employeur ?

## Réponse courte

En cas de manquement au RGPD, l'employeur luxembourgeois s'expose à un éventail de **sanctions administratives** prononcées par la **CNPD** : avertissement, mise en demeure, limitation ou suspension du traitement, ordre de mise en conformité, retrait de certification, et surtout des **amendes administratives** pouvant atteindre **20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial**, selon le montant le plus élevé.

S'ajoutent des **sanctions pénales** prévues par le Code pénal luxembourgeois (art. 457-1 et suivants) en cas d'atteinte grave à la vie privée, ainsi que la **responsabilité civile** de l'employeur vis-à-vis des personnes concernées, qui peuvent réclamer des **dommages et intérêts** pour le préjudice matériel ou moral subi. Enfin, l'**atteinte à la réputation** et la perte de confiance peuvent avoir des conséquences commerciales et sociales majeures.

## Définition

Les **sanctions** en matière de RGPD regroupent les mesures correctrices et pécuniaires prévues par le chapitre VIII du règlement et par la loi luxembourgeoise du 1er août 2018. Elles visent à garantir l'effectivité de la protection des données et à dissuader les manquements.

## Conditions d'exercice

L'article 83 du RGPD prévoit deux plafonds d'amende (10 M€ ou 2 % du CA mondial pour le niveau 1 ; 20 M€ ou 4 % pour le niveau 2), cumulables avec des mesures correctrices, des sanctions pénales (art. 457-1 Code pénal) et la responsabilité civile vis-à-vis des personnes concernées.

| Niveau de sanction       | Montant maximal  |
|--------------------------|--|
| Manquements de niveau 1  | 10 millions d'euros ou 2 % du CA mondial               |
| Manquements de niveau 2  | 20 millions d'euros ou 4 % du CA mondial               |
| Mesures correctrices     | Avertissement, mise en demeure, suspension, effacement |
| Sanctions pénales        | Peines d'emprisonnement et amendes (Code pénal)        |
| Responsabilité civile    | Dommmages et intérêts aux personnes concernées         |
| Publicité de la sanction | Publication possible de la décision par la CNPD        |

## Modalités pratiques

La procédure CNPD se déroule en sept étapes : contrôle (plainte, signalement ou d'initiative), procès-verbal de constatation, contradictoire écrit, décision motivée, recours devant le tribunal administratif, publication éventuelle et exécution de la sanction (art. 58 RGPD).

| Étape                    | Détail  |
|--------------------------|---|
| Contrôle CNPD            | Investigation sur plainte, signalement ou contrôle d'initiative |
| Procès-verbal            | Constatation des manquements                                    |
| Procédure contradictoire | Observations écrites de l'employeur                             |
| Décision motivée         | Choix de la mesure correctrice et/ou amende                     |
| Recours                  | Tribunal administratif dans les délais légaux                   |
| Publication              | Possible affichage public de la décision                        |
| Exécution                | Paiement de l'amende et mise en conformité                      |

## Pratiques et recommandations

**Documenter** rigoureusement l'ensemble des mesures de conformité mises en œuvre (registre, AIPD, formation, contrats) pour démontrer la diligence de l'entreprise.

**Coopérer** activement avec la CNPD en cas de contrôle : la coopération est un facteur atténuant pris en compte dans la détermination du montant de l'amende.

**Corriger** rapidement les manquements identifiés et notifier les mesures prises, pour limiter l'impact de la sanction.

**Souscrire** une assurance cyber ou RGPD pour couvrir les conséquences financières des violations et des amendes (sous réserve des clauses d'exclusion).

**Former** régulièrement les équipes aux obligations RGPD et aux procédures internes de gestion des risques et des incidents.

## Cadre juridique

Le cadre juridique des sanctions repose sur le RGPD et la loi luxembourgeoise.

| Référence                           | Objet  |
|-------------------------------------|--|
| Art. 83 RGPD                        | Conditions générales des amendes administratives |
| Art. 84 RGPD                        | Sanctions pénales prévues par le droit national  |
| Art. 58 RGPD                        | Pouvoirs de l'autorité de contrôle               |
| Art. 82 RGPD                        | Droit à réparation et responsabilité             |
| Loi du 1er août 2018                | Régime général et sanctions au Luxembourg        |
| Art. 457-1 Code pénal               | Atteinte à la vie privée                         |
| Art. <u>L.261-1</u> Code du travail | Surveillance des salariés                        |

Le montant des amendes tient compte de plusieurs facteurs : **gravité, durée, caractère intentionnel, mesures prises, coopération** avec la CNPD, **antécédents** et **catégories de données concernées**. Une politique de conformité active est le meilleur moyen de limiter le risque.

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.