Qu'est-ce que le RGPD et à qui s'applique-t-il en entreprise ?

Réponse courte

Le **RGPD** (Règlement (UE) 2016/679) est un règlement européen directement applicable au Luxembourg depuis le **25 mai 2018**. Il encadre tout **traitement de données à caractère personnel** et s'impose à toute entreprise, quelle que soit sa taille, qui collecte ou utilise des informations sur des personnes physiques identifiées ou identifiables.

En pratique, il s'applique à toute **entreprise établie au Luxembourg** ainsi qu'à celles qui, sans y être établies, proposent des biens ou services ou surveillent le comportement de personnes situées sur le territoire. Les **sous-traitants** sont également soumis au règlement. Seuls les traitements à des fins purement **personnelles ou domestiques** sont exclus du champ d'application.

Définition

Le **RGPD** est un texte européen directement applicable qui établit un cadre harmonisé pour la protection des données à caractère personnel au sein de l'Union européenne. Une **donnée à caractère personnel** est toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement (nom, numéro de matricule, adresse IP, données de géolocalisation, etc.).

Au Luxembourg, le RGPD est complété par la **loi du 1er août 2018** portant organisation de la Commission nationale pour la protection des données (CNPD) et du régime général sur la protection des données.

Questions fréquentes

Qu'est-ce qu'une donnée à caractère personnel selon le RGPD ?

Une donnée à caractère personnel est toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement : nom, numéro de matricule, adresse IP, données de géolocalisation. La définition figure à l'article 4 du RGPD.

Qu'est-ce que le RGPD et quand s'applique-t-il au Luxembourg ?

Le RGPD (Règlement UE 2016/679) est un règlement européen directement applicable au Luxembourg depuis le 25 mai 2018. Il encadre tout traitement de données personnelles et s'impose à toute entreprise, quelle que soit sa taille, qui collecte ou utilise des informations sur des personnes physiques.

Quelle loi luxembourgeoise complète le RGPD ?

Au Luxembourg, le RGPD est complété par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données (CNPD) et du régime général sur la protection des données personnelles.

Quelles entreprises sont soumises au RGPD au Luxembourg ?

Toute entreprise établie au Luxembourg est soumise au RGPD, ainsi que celles hors UE qui proposent des biens ou services ou surveillent le comportement de personnes situées sur le territoire. Les sous-traitants sont également concernés (article 3 RGPD).

Quelles sanctions encourt une entreprise en cas de non-respect du RGPD au Luxembourg ?

Le non-respect du RGPD expose l'entreprise à des sanctions administratives pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial, selon le montant le plus élevé. La CNPD est l'autorité de contrôle compétente.

Quelles sont les principales obligations imposées par le RGPD aux entreprises ?

L'entreprise doit recenser ses traitements, définir une base légale pour chacun (article 6), informer les personnes concernées, tenir un registre des activités (article 30), sécuriser les données et notifier toute violation à la CNPD dans les 72 heures.

Quels traitements de données sont exclus du RGPD ?

Seuls les traitements à des fins purement personnelles ou domestiques sont exclus du champ d'application du RGPD, ainsi que ceux relevant de la sécurité nationale. Tous les autres traitements automatisés ou fichiers structurés manuels relèvent du règlement.

Conditions d’exercice

L'article 3 du RGPD définit un champ d'application large reposant sur trois critères alternatifs : l'établissement de l'entreprise dans l'UE, le ciblage de personnes situées dans l'UE et la surveillance de leur comportement, avec des exclusions limitées aux activités purement personnelles ou domestiques.

Critère	Détail
Établissement	Entreprise établie au Luxembourg, traitement effectué dans le cadre de ses activités
Ciblage	Entreprise hors UE proposant des biens ou services à des personnes au Luxembourg
Surveillance	Suivi du comportement de personnes situées sur le territoire de l'UE
Sous-traitance	Prestataire agissant pour le compte d'un responsable de traitement soumis au RGPD
Nature du traitement	Traitement automatisé ou fichier structuré manuel
Exclusions	Activités purement personnelles, domestiques ou de sécurité nationale

Modalités pratiques

La conformité RGPD impose au responsable de traitement de recenser ses traitements, de définir une base légale pour chacun et de tenir un registre conforme à l'article 30 du RGPD.

Étape	Détail
Identification	Recensement de tous les traitements de données (RH, clients, fournisseurs)
Base légale	Détermination d'une base légale valable (art. 6 RGPD) pour chaque traitement
Information	Notice d'information claire remise aux personnes concernées
Registre	Tenue du registre des activités de traitement (art. 30 RGPD)
Sécurité	Mesures techniques et organisationnelles adaptées aux risques
Droits	Procédure pour répondre aux demandes d'accès, rectification, effacement

Pratiques et recommandations

Cartographier l'ensemble des traitements de données dès la création de l'entreprise et mettre à jour cette cartographie à chaque nouveau projet RH ou commercial.

Former les collaborateurs qui accèdent à des données personnelles (RH, IT, commerciaux) à leurs obligations RGPD et aux procédures internes de sécurité.

Documenter chaque décision relative à la protection des données pour démontrer la conformité en cas de contrôle de la **CNPD** (principe d'accountability).

Consulter la délégation du personnel avant la mise en place de tout traitement de données des salariés, conformément à l'article L.261-1 du Code du travail.

Anticiper les violations de données par une procédure interne de détection et de notification à la CNPD dans les 72 heures.

Cadre juridique

Le cadre juridique applicable repose sur les textes européens et luxembourgeois suivants.

Référence	Objet
Règlement (UE) 2016/679 (RGPD)	Cadre général de la protection des données personnelles
Loi du 1er août 2018	Organisation de la CNPD et régime général au Luxembourg
Art. L.261-1 Code du travail	Surveillance des salariés et protection dans la relation de travail
Art. L.414-9 Code du travail	Consultation de la délégation du personnel sur les traitements
Art. 4 RGPD	Définitions (données personnelles, traitement, responsable)
Art. 3 RGPD	Champ d'application territorial

Le non-respect du RGPD expose l'entreprise à des sanctions administratives pouvant atteindre **20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial**, selon le montant le plus élevé. La CNPD est l'autorité de contrôle compétente au Luxembourg.