GDPR CARPA

CNPD

Certification RGPD

Renforcez la confiance, démontrez votre conformité

Conformité *Transparence* *Confiance*

cnpd.lu
certification@cnpd.lu

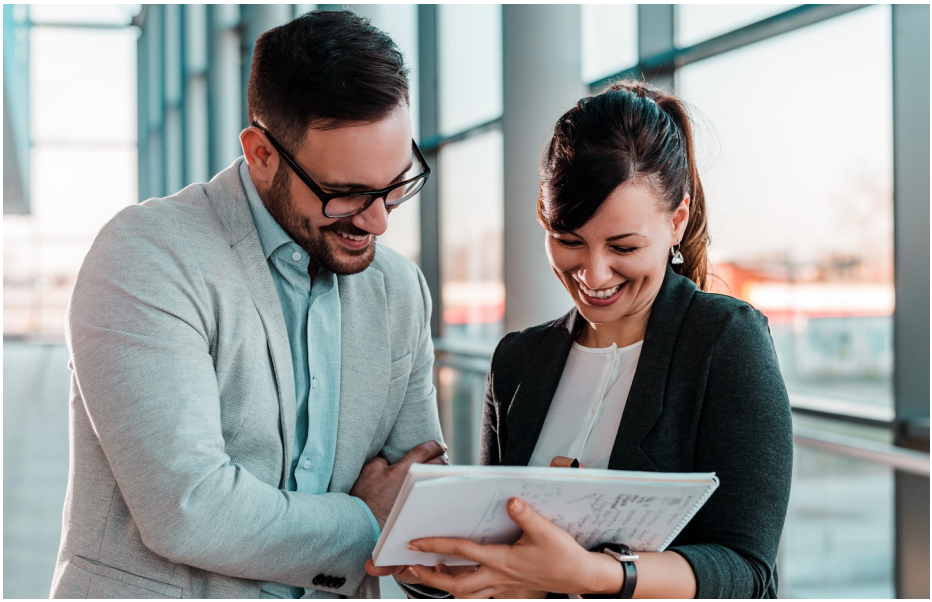
GDPR
CARPA
CNPD

Qu’est-ce que la certification RGPD ?

La certification est un outil de conformité prévu par le Règlement général sur la protection des données (RGPD), s’adressant aux professionnels qui souhaitent démontrer le niveau de protection des données de leurs opérations de traitement.

Elle atteste qu’un traitement de données à caractère personnel est conforme aux critères d’un schéma de certification, approuvé soit par la CNPD au niveau national, soit par le Comité européen de la protection des données (CEPD/EDPB) au niveau européen. Cette conformité est vérifiée par un organisme de certification agréé.

La certification est valorisée par le règlement comme un gage de conformité et de confiance.



Que vous apporte la certification ?

En intégrant la protection des données dès la phase de conception des services et des processus, conformément à l'article 25.3 du RGPD, l'organisation renforce sa cohérence et améliore son efficacité globale. La certification accompagne cette démarche en structurant les pratiques, en clarifiant les responsabilités et en inscrivant la protection des données dans la durée.

Elle représente à la fois un levier d'efficacité opérationnelle et un gage de bonne gouvernance des données personnelles. Elle permet aussi de réduire les risques, de faciliter les audits internes comme externes et de renforcer la confiance des clients et partenaires.

Enfin, la certification valorise les parties prenantes, notamment l'organisation et le délégué à la protection des données. Elle reconnaît leur engagement en matière de protection des données, dans un environnement où la conformité devient un facteur croissant de différentiation.

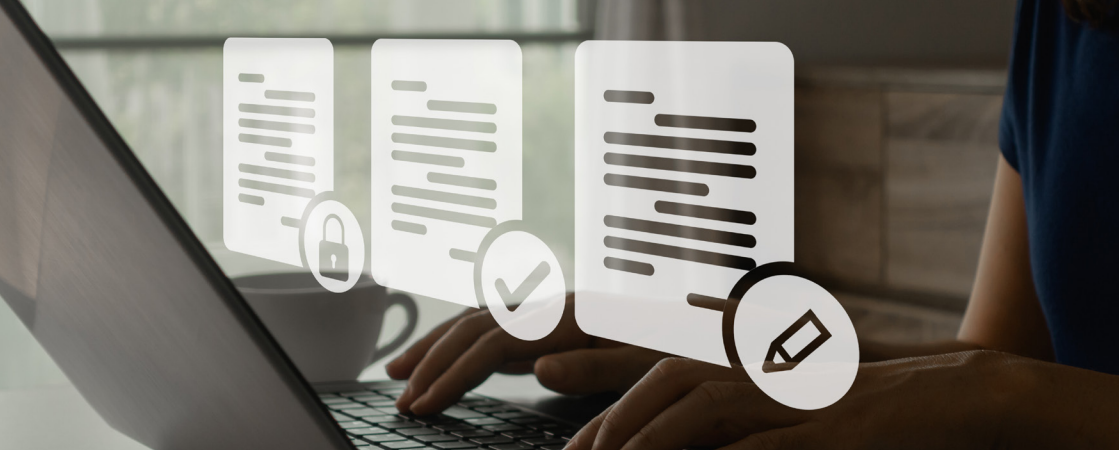
Bon à savoir :

Prise en compte de la certification dans la décision d'imposer une amende administrative (art. 83 du RGPD) :

- Elle peut être considérée comme une preuve de bonne foi, en démontrant la volonté de respecter le règlement, et de diligence, en attestant de la mise en œuvre effective des mesures techniques et organisationnelles.
- Elle peut également atténuer la sévérité d'une sanction, dès lors que l'organisme est en mesure de démontrer concrètement les mesures techniques et organisationnelles qu'il a mises en place.

Attention :

Cela ne garantit pas l'absence de sanction.



Que contiennent les critères d'une certification RGPD ?

Conformément à l'article 42 et au considérant 100 du RGPD, les critères visent à évaluer la conformité aux principes et obligations du règlement. Dans ce cadre, ils peuvent couvrir différents aspects de la protection des données, tels que : la gouvernance des données (privacy by design, rôle du DPO, etc.), le respect des principes fondamentaux du traitement (licéité, minimisation, limitation des finalités, etc.), la prise en compte des droits des personnes concernées (accès, rectification, effacement, etc.) ou encore la tenue du registre des traitements.

Votre organisation est-elle concernée par une démarche de certification ?

Toute entité, publique ou privée, qui traite des données personnelles peut demander une certification RGPD.

La certification peut porter sur différents aspects des opérations de traitement de données à caractère personnel, tels que le traitement des données personnelles par un site web ou un service en ligne, les services de stockage, la gestion des données clients, les ressources humaines ou encore le traitement de données médicales.

Dans ce cadre, l'organisme de certification peut être amené à évaluer à la fois les systèmes techniques utilisés pour les traitements (infrastructures, matériel, logiciels) et les processus ou procédures liés aux opérations de traitement.

Comment obtenir une certification RGPD au Luxembourg ?

1 Choisir un schéma de certification reconnu

Exemples:

- GDPR-CARPA (Luxembourg)
- Europrivacy (EU SEAL)

2 Contacter un organisme de certification agrée

Organismes de certification agréés et établis au Luxembourg

3 Préparer son dossier de conformité

Preuves, politiques internes, mesures mises en place

4 Se soumettre à une évaluation indépendante

L'organisme de certification vérifie la conformité et délivre la certification

5 Maintenir sa conformité

- Certification valable 3 ans (en pratique)
- Surveillance périodique
- Conformité à maintenir en continu

Quel est le coût d'une certification ?

Les tarifs sont fixés directement par l'organisme de certification en fonction de plusieurs éléments, tels que la complexité des traitements à évaluer, la taille de l'organisation concernée et le périmètre du schéma de certification choisi. Le coût couvre généralement l'analyse du dossier, la délivrance du certificat et les audits de surveillance.

A noter :

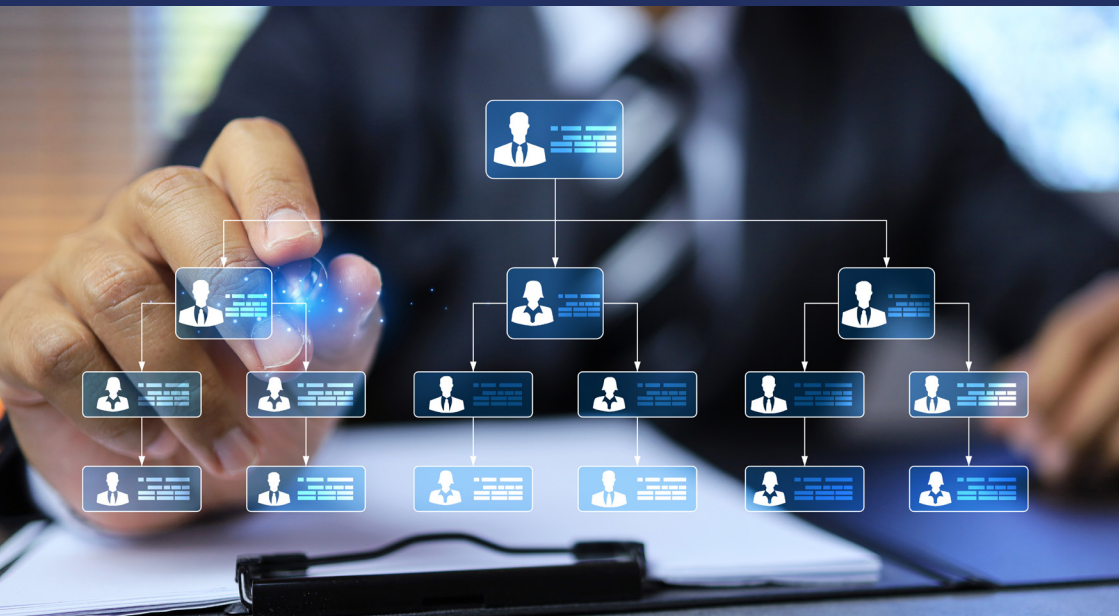
La CNPD ne délivre pas de certification et n'intervient pas dans la fixation des prix.

Quels organismes peuvent délivrer une certification RGPD au Luxembourg ?

La liste des organismes de certification agréés par la CNPD est disponible sur le site de l'autorité.

En ce qui concerne la certification européenne, également appelée label européen de protection des données (European Data ProtectionSseal), celle-ci pourra être délivrée par des organismes de certification établis dans l'EEE et sera valable dans toute l'Union européenne, y compris au Luxembourg.

Les informations détaillées sont accessibles sur les sites de chaque schéma de certification.



Quels sont les schémas de certification établis au Luxembourg ?

- **GDPR-CARPA**, un schéma national conçu pour refléter les spécificités du contexte luxembourgeois

La certification GDPR-CARPA est un schéma national destiné aux responsables de traitement et aux sous-traitants établis au Luxembourg, pour les opérations de traitement effectuées sur le territoire luxembourgeois. Développée par l'autorité de contrôle elle-même (CNPD), elle repose sur la norme ISAE 3000, garantissant ainsi un haut niveau d'exigence et renforçant la confiance des personnes concernées.

- **Europrivacy**, un schéma européen aligné sur les attentes du RGPD et reconnu au-delà des frontières

La certification Europrivacy est un label européen de protection des données reconnu par l'EDPB et s'adressant aussi bien aux responsables de traitement qu'aux sous-traitants. Elle est applicable aux opérations de traitement effectuées dans l'ensemble de l'Espace économique européen.

Consultez la liste des schémas de certification agréés par l'EDPB

DÉCOUVREZ UN AUTRE OUTIL DE CONFORMITÉ

Outre la certification, un groupement d'organisations d'un secteur spécifique peut élaborer son propre code de conduite RGPD ou choisir d'adhérer à un code déjà existant. Une fois approuvé par la CNPD, cet outil permet de démontrer la conformité au RGPD, tout en tenant compte des besoins opérationnels du secteur concerné. Les bénéfices sont comparables à ceux d'une certification, notamment en matière de gouvernance et de suivi.

Exemple de code de conduite au Luxembourg :

Le code de conduite du secteur du travail intérimaire, approuvé par la CNPD en 2024, est le premier à avoir été reconnu au niveau national.

À l'échelle européenne, vous pouvez également consulter la liste des codes de conduite approuvés par l'EDPB.

Pour découvrir l'ensemble des outils de conformité proposés par la CNPD, rendez-vous sur :

Pour en savoir plus

- **Explorez le cadre applicable aux critères de certification**
- **Identifiez les organismes de certification agréés**
- **Découvrez le schéma de certification GDPR-CARPA**