Premiers pas RGPD : la liste de vérification en 4 étapes

Usage : Faire un premier point sur vos données personnelles en suivant les quatre étapes proposées par la CNIL aux petites structures. Ressource offerte.

Repères : texte du document · [champ à remplir] · *note à supprimer avant utilisation* · exemple fictif

Le RGPD s'applique dès qu'une structure traite des données sur des personnes physiques : clients, prospects, salariés, candidats, bénévoles, fournisseurs personnes physiques. Cette liste vous aide à repérer où vous en êtes ; elle ne remplace pas la lecture des textes et des fiches de la CNIL citées à la fin.

Étape 1 — Recenser vos traitements

- ☐ j'ai listé les activités qui utilisent des données personnelles (gestion des clients, facturation, paie, recrutement, prospection, site internet…)
- ☐ pour chaque activité, je sais pourquoi les données sont utilisées, lesquelles, qui y a accès et combien de temps elles sont gardées
- ☐ ces informations sont réunies dans un registre des activités de traitement (article 30 du RGPD)
- ☐ je connais les outils et prestataires qui accèdent à ces données

Note — à supprimer avant utilisation : la CNIL propose un modèle de registre simplifié ; les ressources R-01 (registre commenté) et R-02 (inventaire des outils) du catalogue LexDigita vont plus loin.

Étape 2 — Faire le tri dans vos données

- ☐ je ne collecte que les données utiles à l'objectif poursuivi (article 5.1.c)
- ☐ je n'ai pas de données sensibles (santé, opinions, religion…) sans base juridique adaptée (article 9)
- ☐ seules les personnes qui en ont besoin peuvent consulter les données
- ☐ j'ai fixé une durée de conservation pour chaque catégorie de données et je supprime ou j'archive ce qui n'est plus utile (article 5.1.e)

Exemple fictif : un artisan conserve les devis non signés de prospects pendant [durée choisie], puis les supprime (structure et durée inventées : fixez la vôtre selon vos besoins et vos obligations).

Étape 3 — Respecter les droits des personnes

- ☐ les personnes sont informées au moment de la collecte : qui je suis, pourquoi je collecte, combien de temps je conserve, comment exercer leurs droits (articles 12 et 13)
- ☐ une adresse ou un formulaire permet de me contacter pour exercer ses droits
- ☐ je sais répondre à une demande dans un délai d'un mois (article 12.3)

Étape 4 — Sécuriser vos données

- ☐ les logiciels et antivirus sont à jour
- ☐ chaque personne a son propre compte et un mot de passe solide ; la double authentification est activée quand elle existe

- ☐ les données sont sauvegardées régulièrement et la restauration a été testée
- ☐ les ordinateurs portables et supports amovibles sont chiffrés
- ☐ l'équipe sait à qui signaler un incident ; une violation présentant un risque est notifiée à la CNIL dans les 72 heures (article 33)

Note — à supprimer avant utilisation : le guide de la sécurité des données personnelles de la CNIL (édition 2024) détaille ces mesures (article 32 du RGPD).

Et ensuite ?

Chaque case non cochée est un point à traiter. Commencez par le registre : il sert de base à tout le reste.

Sources utilisées

- Règlement (UE) 2016/679 (RGPD) — https://eur-lex.europa.eu/eli/reg/2016/679/oj (articles 5, 9, 12, 13, 30, 32 et 33)
- CNIL, « RGPD : les premières étapes » — https://www.cnil.fr/fr/rgpd-les-premieres-etapes
- CNIL, « Le registre des activités de traitement » (modèle de registre simplifié) — https://www.cnil.fr/fr/RGPD-le-registre-des-activites-de-traitement
- CNIL, « Guide de la sécurité des données personnelles », édition 2024 — https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles-nouvelle-edition-2024

Note — à supprimer avant utilisation : les sources ont été consultées le 5 octobre 2026 et revérifiées le 7 novembre 2026. Vérifiez qu'elles sont toujours à jour avant d'utiliser le document.

© Lex Digita – lexdigita.fr · Ressource à compléter · Version novembre 2026