



Aide-mémoire RGPD

L'essentiel du Règlement Général sur la Protection des Données en un document — obligations, registre, droits des personnes, sous-traitants, incidents.

À qui s'adresse ce document ? Dirigeants, gérants, responsables et agents non-techniques. Ce guide ne remplace pas un audit complet mais permet une consultation rapide des obligations essentielles.

BLOC 1 — C'EST QUOI LE RGPD EN 30 SECONDES ?

Le RGPD (Règlement Général sur la Protection des Données, règlement UE 2016/679) est la loi européenne qui encadre la collecte, le traitement et la conservation des données personnelles.

Il s'applique à VOTRE structure si vous :

- Collectez des données clients (nom, email, téléphone, adresse...)
- Gérez des fichiers RH (salariés, bénévoles, agents)
- Utilisez la vidéosurveillance ou des badges d'accès
- Envoyez des newsletters ou utilisez un CRM
- Traitez des données de mineurs, de santé ou d'opinions politiques/religieuses

■ **Sanctions possibles :** jusqu'à 20 M€ ou 4 % du chiffre d'affaires mondial annuel (le montant le plus élevé). La CNIL prononce des amendes croissantes depuis 2021.

BLOC 2 — LES 5 OBLIGATIONS ESSENTIELLES

OBL. 1 — Tenir un Registre des Traitements (art. 30)

Pour chaque traitement de données, documenter :

- Finalité (pourquoi on collecte ces données)
- Catégories de données (lesquelles)
- Qui y a accès (destinataires internes et externes)
- Durée de conservation (et critères de suppression)
- Mesures de sécurité appliquées

Outil gratuit : modèle de registre → cnil.fr · *Temps estimé : 2-4h pour une petite structure*



OBL. 2 — Informer les personnes (art. 13 & 14)

Toute personne dont vous collectez des données DOIT être informée de :

- Qui collecte (votre structure)
- Pourquoi (la finalité précise)
- Combien de temps les données sont conservées
- Ses droits (accès, rectification, suppression, portabilité)

Concrètement : mentions légales sur votre site, clauses dans vos contrats, information orale ou écrite lors de collecte.

OBL. 3 — Obtenir un consentement valide (art. 6 & 7)

Le consentement doit être :

- Libre (pas de case pré-cochée, pas de condition à l'accès d'un service)
- Éclairé (la personne sait exactement à quoi elle consent)
- Univoque (action positive claire)
- Retirable à tout moment

Attention : le consentement n'est pas la seule base légale — l'exécution d'un contrat ou l'obligation légale peuvent suffire selon les cas.

OBL. 4 — Sécuriser les données (art. 32)

Mesures minimales attendues par la CNIL :

- Mots de passe complexes + authentification à deux facteurs (MFA)
- Chiffrement des données sensibles (au repos et en transit)
- Sauvegardes régulières et testées (règle 3-2-1)
- Contrôle des accès (principe du moindre privilège)
- Journalisation des accès aux données sensibles

OBL. 5 — Encadrer les sous-traitants (art. 28)

Si vous confiez des données à un prestataire (logiciel SaaS, comptable, hébergeur, DRH externalisée...) :

- Signer un **DPA (Data Processing Agreement)** incluant les clauses RGPD obligatoires
- Vérifier que le prestataire offre des garanties suffisantes
- S'assurer que les données ne sont pas transférées hors UE sans garanties adéquates

Action pratique : demandez à chaque prestataire numérique sa politique de traitement des données.



BLOC 3 — EN CAS D'INCIDENT : QUE FAIRE DANS LES 72 HEURES ?

■ **Obligation légale** : Tout incident affectant des données personnelles doit être notifié à la CNIL dans les 72h (art. 33). Si les personnes concernées sont à risque élevé, elles doivent également être informées (art. 34).

H+0	Confinement Isoler les systèmes compromis, couper les accès suspects, sauvegarder les logs.
H+4	Évaluation Identifier les données touchées, le nombre de personnes concernées, la nature de l'incident.
H+24	Notification interne Informer le DPO (si vous en avez un), la direction, le service juridique.
H+72	Notification CNIL Via notifications.cnil.fr — même partielle si l'enquête est incomplète.
Après	Communication Si risque élevé pour les personnes : les informer par email, courrier ou communiqué.

BLOC 4 — DROITS DES PERSONNES : VOS OBLIGATIONS DE RÉPONSE

Droit	Description	Délai max
Droit d'accès (art. 15)	La personne peut demander une copie de toutes les données que vous détenez sur elle.	1 mois
Droit de rectification (art. 16)	Corriger des données inexactes ou incomplètes.	1 mois
Droit à l'effacement (art. 17)	Supprimer les données si elles ne sont plus nécessaires ou si le consentement est retiré.	1 mois
Droit à la portabilité (art. 20)	Fournir les données dans un format structuré et lisible (CSV, JSON...).	1 mois
Droit d'opposition (art. 21)	Permettre à la personne de s'opposer au traitement à des fins de prospection.	Immédiat

Un diagnostic Wilizé couvre l'ensemble de ces obligations et vous remet un plan d'action priorisé avec délais et responsables. Contact : infos.wilize@gmail.com · wilize.com