AIDE-MÉMOIRE RGPD — GUIDE PRATIQUE RAPIDE

Pour les dirigeants, gérants, responsables et agents non-techniques

Version 1.0 **Siba KOIVOGUI** **OPSIE M2 Lyon 2**

NOTE D'UTILISATION

Ce document est conçu pour être imprimé (format A4 recto-verso) et affiché ou conservé à portée de main. Il ne remplace pas le rapport de diagnostic 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) est la loi européenne qui protège les données personnelles des individus.

- Il s'applique à VOTRE structure si vous collectez des données sur :
- des clients ou prospects
- des salariés ou bénévoles
- des adhérents, abonnés, donateurs
- des administrés (pour les collectivités)

→ "Données personnelles" = toute information qui permet d'identifier une personne : nom, email, téléphone, adresse IP, photo, etc.

→ Amende maximale : 20 millions € ou 4 % du chiffre d'affaires annuel. En pratique, la CNIL sanctionne aussi les petites structures. (Exemple : association condamnée à 5 000 € pour liste d'adhérents mal gérée)

BLOC 2 — VOS 5 OBLIGATIONS CLÉS

┌──┐

│ OBLIGATION 1 — TENIR UN REGISTRE DES TRAITEMENTS (Art. 30 RGPD) │ │ │ Vous devez lister tous les usages que vous faites des données personnelles. │ │ Un "traitement" = toute

utilisation de données (liste clients, fichier RH, │ │ vidéosurveillance, newsletter, etc.) │ │ │ │ Pour chaque traitement, noter : │ │ • Finalité (pourquoi on collecte) │ │ • Catégories de données (lesquelles) │ │ • Qui y a accès (destinataires) │ │ • Durée de conservation │ │ • Mesures de sécurité │ │ │ │ Outil gratuit : modèle de registre sur → cnil.fr │ │ Temps estimé : 2 à 4 heures pour une petite structure │
└──┘

┌──┐
│ OBLIGATION 2 — INFORMER LES PERSONNES (Art. 13 & 14 RGPD) │ │ │ │ Toute personne dont vous collectez des données DOIT être informée : │ │ • Qui collecte (vous) │ │ • Pourquoi (la finalité) │ │ • Combien de temps les données seront conservées │ │ • Ses droits (accès, rectification, effacement...) │ │ │ │ Concrètement : │ │ → Mention légale sur votre site web │ │ → Clause dans vos formulaires papier ou numériques │ │ → Contrat de travail pour les salariés │ │ → Bulletin d'adhésion pour les associations │ │ │ │ Outil gratuit : générateur de mentions légales → cnil.fr │
└──┘

┌──┐
│ OBLIGATION 3 — AVOIR UNE BASE LÉGALE (Art. 6 RGPD) │ │ │ │ Vous ne pouvez pas utiliser des données "parce que ça vous arrange". │ │ Chaque traitement doit reposer sur une base légale : │ │ │ │ ✔ CONTRAT : données nécessaires pour exécuter un contrat │ │ ex : adresse de livraison d'un client │ │ │ │ ✔ OBLIGATION LÉGALE : imposé par la loi │ │ ex : fiche de paie, déclaration URSSAF │ │ │ │ ✔ INTÉRÊT LÉGITIME : usage raisonnable sans impact sur les droits │ │ ex : prospection auprès de clients existants (sous conditions) │ │ │ │ ✔ CONSENTEMENT : accord explicite, libre, informé, révocable │ │ ex : newsletter marketing, cookies non essentiels │ │ → Le consentement doit être tracé (date, moyen, objet) │
└──┘

┌──┐
│ OBLIGATION 4 — SÉCURISER LES DONNÉES (Art. 32 RGPD) │ │ │ │ Vous devez mettre en place des mesures "appropriées" pour protéger │ │ les données. Pour une petite structure, cela signifie au minimum : │ │ │ │ ✔ Mots de passe robustes et uniques (minimum 12 caractères) │ │ ✔ Antivirus et mises à jour activés sur tous les postes │ │ ✔ Sauvegardes régulières et testées (règle 3-2-1) │ │ ✔ Accès limités aux données selon les fonctions (principe du besoin) │ │ ✔ Chiffrement des données sensibles en transit et au repos │ │ │ │ La CNIL juge la "proportionnalité" : une PME de 5 personnes │ │ n'a pas les mêmes obligations qu'un hôpital, mais doit quand même │ │ démontrer des efforts sérieux. │
└──┘

┌──┐
│ OBLIGATION 5 — GÉRER LES SOUS-TRAITANTS (Art. 28 RGPD) │ │ │ │ Si vous confiez des

données à un prestataire (logiciel en ligne, comptable, │ │ hébergeur web, société de paie...), vous devez : │ │ │ │ ✔ Conclure un contrat ou avenant incluant des clauses RGPD spécifiques │ │ (DPA — Data Processing Agreement) │ │ ✔ S'assurer que le prestataire offre des garanties suffisantes │ │ ✔ Vérifier que les données ne sont pas transférées hors UE │ │ sans garanties (ex : serveurs aux USA sans Privacy Shield valide) │ │ │ │ Conseil pratique : demandez à chaque prestataire numérique sa │ │ "politique de traitement des données" et son DPA. │
└──┘

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

Un "incident" RGPD = toute violation pouvant affecter des données personnelles : → Piratage / ransomware touchant des données personnelles → Envoi de données par erreur à un mauvais destinataire → Perte ou vol d'un ordinateur ou téléphone contenant des données → Accès non autorisé à votre système → Divulgation accidentelle d'une liste de contacts

┌──┐ │ H+0 │ Identifier et contenir │ │ │ → Déconnecter le système │ │ │ → Alerter le responsable │
├────────┼───────────────────────────────┤ │ H+24 │ Évaluer la gravité │ │ │ → Quelles données touchées ? │ │ │ → Combien de personnes ? │ │ │ → Risque pour les personnes ? │
├────────┼───────────────────────────────┤ │ H+72 │ Notifier la CNIL si nécessaire│ │ │ → notifications.cnil.fr │ │ │ → (si risque pour les droits) │
├────────┼───────────────────────────────┤ │ Après │ Documenter dans le registre │ │ │ des violations de données │ │ │ → Obligatoire, même si pas │ │ │ de notification CNIL │
└────────┴───────────────────────────────┘

⚠ La notification est obligatoire si l'incident présente un RISQUE pour les droits des personnes. En cas de doute → notifier. L'omission volontaire aggrave les sanctions.

> Si les personnes concernées sont aussi en danger (ex : données de santé
> ou données financières exposées), elles doivent ÉGALEMENT être notifiées
> "dans les meilleurs délais".

BLOC 4 — LES DROITS DES PERSONNES : COMMENT RÉPONDRE ?

Toute personne peut exercer ses droits sur ses données. Vous avez en général UN MOIS pour répondre (prorogeable à 3 mois si complexe).

DROIT	CE QUE ÇA SIGNIFIE
Accès (Art. 15)	La personne veut savoir quelles données vous détenez → Fournir une copie gratuite des données
Rectification (Art. 16)	Corriger des données inexactes ou incomplètes → Effectuer la correction dans les meilleurs délais
Effacement (Art. 17)	"Droit à l'oubli" — supprimer les données → Pas absolu : ne s'applique pas si obligation légale
Opposition (Art. 21)	S'opposer à un traitement (ex : prospection) → Droit absolu pour la prospection commerciale
Portabilité (Art. 20)	Recevoir ses données dans un format réutilisable → S'applique si le traitement est basé sur contrat ou consentement, et réalisé automatiquement
Limitation (Art. 18)	Geler un traitement le temps du traitement d'un litige → Les données sont conservées mais plus utilisées

Procédure interne à suivre : 1. Vérifier l'identité du demandeur (copie pièce d'identité si doute) 2. Transmettre à **[RESPONSABLE RGPD / DPO]** 3. Traiter dans le délai d'un mois 4. Conserver une trace de la demande et de la réponse

---

BLOC 5 — CAS PARTICULIERS : CE QUI NÉCESSITE UNE ATTENTION SPÉCIALE

⚠ DONNÉES SENSIBLES (Art. 9 RGPD) — Interdites sauf exception explicite → Santé, origine ethnique, opinions politiques ou syndicales, données biométriques, orientation sexuelle, condamnations pénales → Traitement interdit sauf : consentement explicite + écrit, nécessité pour la médecine du travail, ou autre exception légale précise → Ne pas collecter si non strictement nécessaire

⚠ DONNÉES D'ENFANTS (Art. 8 RGPD) → En dessous de 15 ans en France : consentement parental obligatoire → Données d'enfants = protection renforcée obligatoire

⚠ VIDÉOSURVEILLANCE → Affichage obligatoire (panneau) à l'entrée des zones filmées → Durée de conservation limitée (généralement 30 jours max) → Accès aux images restreint à des personnes habilitées → Déclaration à la préfecture si établissement recevant du public

⚠ COOKIES ET TRACEURS SUR SITE WEB → Consentement préalable obligatoire pour les cookies non essentiels (analytics, publicité, réseaux sociaux embarqués) → Un bandeau cookie conforme est obligatoire → Les cookies strictement nécessaires ne nécessitent pas de consentement

⚠ TRANSFERTS HORS UE → Toute transmission de données à un prestataire hors Union Européenne (ex : serveurs USA, Inde, Chine) nécessite des garanties spécifiques → Vérifier que vos prestataires cloud ont leurs serveurs en Europe ou offrent des garanties contractuelles (Clauses Contractuelles Types)

BLOC 6 — CHECKLIST DE CONFORMITÉ MINIMALE

☐ Registre des traitements créé et tenu à jour ☐ Mentions légales présentes sur le site web ☐ Formulaires de collecte avec information RGPD ☐ Contrats DPA signés avec les prestataires numériques ☐ Procédure de réponse aux droits des personnes définie ☐ Procédure de notification des incidents documentée ☐ Registre des violations de données tenu (même si pas notifié CNIL) ☐ Politique de durée de conservation définie et appliquée ☐ Accès aux données limités selon les fonctions ☐ Charte informatique signée par tous les utilisateurs ☐ Sensibilisation RGPD des collaborateurs réalisée

---

BLOC 7 — CONTACTS ET RESSOURCES UTILES

Organisme | Pour quoi faire | Contact

CNIL | Registre, formulaires, plaintes | cnil.fr CNIL | Notifier une violation | notifications.cnil.fr CNIL | Téléphone information | 01 53 73 22 22

ANSSI | Sécurité informatique, guides | ssi.gouv.fr Cybermalveillance | Assistance en cas d'incident | cybermalveillance.gouv.fr MonAideCyber | Accompagnement gratuit ANSSI | monaidecyber.ssi.gouv.fr

BPI France | Financement diagnostic cyber PME | bpifrance.fr

VOTRE CONTACT RGPD / DPO :

Nom _____

Email _____

Tél _____

RÉFLEXES RGPD À ADOPTER AU QUOTIDIEN

- Avant de collecter des données → "En ai-je vraiment besoin ?"
- Avant de transmettre des données → "Ai-je le droit de le faire ?"
- Avant de supprimer des données → "Ai-je l'obligation de les garder ?"
- En cas de doute sur un incident → Signaler immédiatement en interne
- En cas de demande d'un client / agent → Transmettre au responsable RGPD

Le RGPD n'est pas une case à cocher — c'est une pratique quotidienne.

Document établi par Siba KOIVOGUI — OPSIE M2 — Université Lumière Lyon 2 Wilizé SASU — SNEE / Pépite Lyon Sous la supervision de M. Fouad BENJOUDAR