

Règlement général de protection des données (RGPD)

Textes réglementaires :

- ✓ *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.*
- ✓ *Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (NOR: JUSC1732261L).*
- ✓ *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite Loi Informatique et Libertés.*
- ✓ *Article 1240 du Code Civil.*
- ✓ *Articles L226-16 à L226-24 et articles R625-10 à R625-13 du Code Pénal.*
- ✓ *Article L. 211-2 du Code du Patrimoine.*

I. Le contexte

Le règlement général de protection des données (RGPD) est un texte réglementaire européen qui encadre le traitement¹ des données à caractère personnel² relatives aux personnes vivantes³, papier ou numériques, de manière égalitaire sur tout le territoire de l'Union Européenne. Il est entré en application le 25 mai 2018.

La transposition nationale de ce texte est dictée par la loi 2018-493 du 20 juin 2018, qui porte modification de la loi 78-17 « Informatique et Libertés » du 6 janvier 1978. Si, depuis 1978, le traitement de données personnelles était soumis à l'avis en amont de la CNIL⁴, avec l'application de la loi 2018-793 aujourd'hui la commission est chargée davantage de l'accompagnement des organismes à la bonne mise en place de la RGPD ainsi qu'au contrôle en aval et à la sanction des mauvaises pratiques.

¹ Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement).

² Les données à caractère personnel sont celles dont les informations se rapportent à des personnes physiques identifiées ou identifiables, directement ou indirectement.

³ Sauf extension par les États membres aux données relatives aux personnes décédées. La France ne fait usage de cette dérogation à la règle que dans le domaine des données médicales.

⁴ Commission nationale informatique et libertés (CNIL).

II. Le cadre général

Le RGPD :

- **S'applique à toutes les collectivités territoriales et à tous les établissements publics.**
- S'applique aux sous-traitants qui traitent des données à caractère personnel pour le compte de la collectivité.
- S'applique aux **traitements de "données à caractère personnel"**, c'est-à-dire aux informations se rapportant à des personnes physiques identifiées ou identifiables, directement ou indirectement.
- Concerne **aussi bien le numérique que le papier** : les bases de données, les listes de contacts, les listes d'invités à des manifestations, les dossiers de personnel, les données générées par les outils de contrôle d'accès, les registres, fichiers ou applications de gestion des usagers.
- **S'applique aux données sensibles.** Il s'agit des données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la vie sexuelle ou à l'orientation sexuelle et à la santé, ainsi que des données génétiques et biométriques.
- S'applique seulement aux données relatives aux **personnes vivantes**, sauf extension par les États membres aux données relatives aux personnes décédées (*considérant n° 27 du RGPD*). La France n'a fait usage de cette option que dans le champ des données de santé.

III. Les principes

- La **co-responsabilité**, selon laquelle l'entité responsable du traitement des données doit prouver à tout moment qu'elle agit en conformité avec la loi.
- La **licéité, la loyauté et la transparence**, principes promus pour assurer le consentement explicite des personnes physiques.
- La **minimisation des données**, pour garantir qu'on ne collecte que les données strictement nécessaires au regard des finalités visées.
- L'**exactitude**. Les données doivent être justes et à jour. Les fichiers doivent être modifiés suivant les éventuelles demandes de modification ou de contrôle des personnes physiques concernées par ceux-ci⁵.
- La **limitation de la conservation** des données dans le temps (**sauf dérogations**).

IV. L'application du RGPD dans les collectivités territoriales

La loi prévoit que chaque collectivité ou établissement public soit doté d'un **délégué à la protection des données** (DPD). Celui-ci, dont la désignation est obligatoire, est chargé de conseiller et d'assister le responsable de traitement à garantir la conformité avec la réglementation sur la protection des données.

⁵ Les personnes physiques ayant fait l'objet d'une collecte de données personnelles bénéficient de plusieurs droits qui leur assurent l'accès et la rectification des données. Elles peuvent également porter opposition ou faire valoir le droit à l'oubli ou à la limitation des données collectées. Elles peuvent enfin engager des recours pour des procédures de collecte estimées abusives ou frauduleuses.

Les responsabilités du DPD :

- Cartographier les traitements de données, établir un registre des traitements et réaliser un bilan annuel des activités.
- Mener des actions pour sécuriser les traitements de données : boîtes mail sécurisées, implantation de mots de passe complexes et uniques, cloisonner le serveur et limiter le droit d'accès aux fichiers sensibles.
- Sensibiliser les collègues, la direction et les élus.
- Être l'interlocuteur de la CNIL et l'informer sous 72h en cas de failles de sécurité ou de perte de données. ([Lien vers les notifications de violation de données personnelles à la CNIL](#))
- Assister et conseiller pour la réalisation des études d'impact menées par le responsable du traitement.

Les bons réflexes :

- Ne collectez que les données vraiment nécessaires : dans un but précis.
- Soyez transparent : l'utilisateur doit être clairement informé des données collectées.
- Assurez l'exercice du droit des administrés : accès aisé à la rectification ou suppression des données.
- Avec l'aide de votre DPD, créez un registre des activités de traitement et tenez-le à jour.
- Avec l'aide de votre DPD, vérifiez la conformité au RGPD des sous-traitants qui traitent des données à caractère personnel pour votre compte.
- Fixez des durées de conservation en accord avec les circulaires de tri des archives relatives aux collectivités territoriales.
- Soumettez toute destruction de données à l'avis du conservateur des Archives départementales. Consultez un archiviste pour déterminer le sort final de vos données.
- Sécurisez les données et identifiez les risques.
- Pour les archives sur support papier, mettez en place une procédure d'archivage pour sécuriser l'accès physique aux données.
- Veillez à la mise en conformité de vos fichiers dans une démarche continue.

V. Et qu'en est-il pour les archives

Le RGPD prévoit un régime dérogatoire au régime de droit commun pour les « traitements archivistiques dans l'intérêt public » et les traitements à des fins de recherche scientifique ou historique ou à des fins statistiques.

Les archives définitives dérogent :

- À l'obligation de destruction à l'issue de la durée de conservation dans le traitement initial (art. 5 du RGPD et art. 36 de la LIL),
- Au droit à l'effacement (art. 17 du RGPD),
- Aux droits de rectification, d'opposition, à la limitation du traitement, à la portabilité et aux droits d'accès et de notification.

Les archives courantes et intermédiaires : relèvent du droit commun en matière de protection des données.

Cependant, ces droits sont limités dans certains cas : le droit d'effacement, par exemple, ne s'applique pas lorsque le traitement est nécessaire pour respecter une obligation légale ou pour exécuter « une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement » (art. 17 du RGPD).

Notons également que l'**élimination d'archives publiques** (papier ou numérique) doit être réalisée en fonction des durées de conservation et du sort final fixés par les circulaires de tri des archives et après l'obtention du visa des Archives départementales.

Se référer aux circulaires de tri des archives :

- ❑ **Instruction DPACI/RES/2004/001 du 5 janvier 2004** relative au traitement et à la conservation des archives relatives aux élections politiques postérieures à 1945.
- ❑ **Instruction DAF/DPACI/RES/2009/018 du 28 août 2009** pour le tri et la conservation des archives produites par les services communs à l'ensemble des collectivités territoriales et structures intercommunales.
- ❑ **Préconisations DGP/SIAF/2014/006 du 22 septembre 2014** pour le tri et la conservation des archives produites par les communes et structures intercommunales dans leurs domaines d'activité spécifiques.

Pour aller plus loin :

[RGPD : passer à l'action](#)

Note d'information réalisée par le service archives du Centre de gestion de l'Ain :
archives@cdg01.fr