MANDIL AVOCATS

Comprendre le RGPD en 10 grands principes

Fiche n°02 - Janvier 2020

Le RGPD prévoit 10 grands principes permettant de s'assurer que les traitements de données personnelles réalisés sont nécessaires, proportionnés et réalisés de manière sécurisée. Contrairement à l'ancien régime de formalités préalables auprès de la CNIL, il repose sur une logique de responsabilisation et de transparence des responsables de traitements et des sous-traitants qui doivent documenter leur conformité tout au long du traitement.

I. Licéité du traitement

Le traitement doit se fonder sur **une des 6 bases légales** suivantes : Cf. Fiche n°03

Consentement de la personne concernée

Exécution d'un contrat auquel la personne concernée est partie

Respect d'une obligation légale

Exécution d'une mission d'intérêt public

Sauvegarde des intérêts vitaux

Intérêt légitime du responsable du traitement

II. Limitation des finalités

Les données doivent être collectées pour des finalités :

- **Déterminées** : précisément identifiées en amont de la collecte ;
- **Explicites** : clairement exprimées de façon intelligible dès la collecte des données ;
- **Légitimes** : fondées sur l'une des 6 bases légales et conformes à la loi.

Elles ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités (**le détournement de finalité est une infraction pénale**).

SAUF si le traitement ultérieur :

- A obtenu le consentement de la personne concernée ;
- Repose sur une finalité « compatible » avec la finalité initiale ;
- Est réalisé à des fins archivistiques dans l'intérêt public, de recherche scientifique ou historique, ou statistiques.

III. Minimisation

Seules doivent être traitées les données personnelles **adéquates, pertinentes et limitées à ce qui est nécessaire** au regard des finalités pour lesquelles elles sont traitées.

Exemple : un site internet non marchand n'a pas a priori pas besoin de collecter le numéro de carte bancaire d'un internaute.

IV. Exactitude

Le responsable du traitement doit veiller à ce que les données soient **exactes et, si nécessaire, tenues à jour, effacées ou rectifiées** sans tarder.

V. Limitation de la conservation

Les données doivent être **conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités** pour lesquelles elles sont traitées.

A terme, elles doivent être **supprimées ou anonymisées**.

Cf. Fiche n°09

Comprendre le RGPD en 10 grands principes

VI. Intégrité & confidentialité

Des **mesures de sécurité techniques, physiques et organisationnelles** appropriées doivent être prise pour limiter les risques d'accès, de modification et de suppression non autorisés des données.

Recours à des méthodes de chiffrement ou de pseudonymisation

Limitation des accès aux seuls destinataires (internes et externes) **nécessaires et légitimes**

Principe d'interdiction des transferts de données hors de l'EEE

Cf. Fiche n°10

VII. Transparence

Le responsable du traitement doit préalablement informer la personne concernée par le traitement des :

Mentions légales obligatoires (identité du responsable du traitement, finalité du traitement, durée de conservation des données…)

+

Droits de la personne concernée et de sa possibilité d'adresser une réclamation à la CNIL

Cf. Fiche n°07

VIII. Loyauté et droits des personnes concernées

La personne concernée bénéficie de nombreux droits garantis par le **Chapitre III du RGPD et la Loi de 1978** : Cf. Fiche n°07

Accès | **Portabilité** | **Rectification** | **Effacement / oubli** | **Opposition** | **Limitation** | **Mort numérique** (Loi de 78)

IX. Responsabilité (accountability)

Le responsable du traitement doit **documenter le traitement pour être en mesure de démontrer** sa conformité au RGPD.

Tenue du registre des traitements

Cf. Fiche n°05

Désignation d'un délégué à la protection des données

Cf. Fiche n°06

Accountability

Réalisation des analyses d'impact sur la vie privée

Obtention de certifications et conformité à des codes de conduite

Détection et notification des violations de données

Cf. Fiche n°08

X. Protection dès la conception & par défaut

La conformité aux dispositions du RGPD doit être anticipée par des mesures appropriées **dès la conception d'un produit ou d'un service**

+

Par défaut, des mesures doivent être prises pour limiter le traitement à ce qui est strictement nécessaire

Cf. Fiche n°04

MANDIL AVOCATS