

### Fichiers informatisés

Le Règlement Général sur la Protection des Données, entré en vigueur le 25 mai 2018, implique avant tout un devoir d'information auprès des utilisateurs concernés par le traitement de leurs données personnelles. En tant que responsable du traitement de ces données, ou bien en tant que sous-traitant, il convient de prendre les mesures nécessaires pour garantir une utilisation respectueuse de ces données, permettant la protection de la vie privée des personnes concernées, mais aussi de leurs droits à cet égard.

On appelle donnée personnelle toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement.

On appelle traitement de données à caractère personnel toute opération portant sur des données personnelles, quel que soit le procédé utilisé. C'est le cas notamment de l'enregistrement, de l'organisation, de la conservation, de la transmission de fichiers tels que les fichiers d'inscription, qu'ils soient manuels ou informatisés.

Le RGPD distingue les données dites sensibles : Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. Cette interdiction ne s'applique pas dans un certain nombre de cas, notamment lorsque la personne a donné son consentement explicite ou lorsque le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées.

La CNIL (Commission nationale Informatique et Libertés) donne cinq grands principes en matière de protection des données personnelles :



Les 5 grands principes des règles de protection des données personnelles sont les suivants :

- Le principe de finalité : le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime ;
- Le principe de proportionnalité et de pertinence : les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier ;
- Le principe d'une durée de conservation limitée : il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. Une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité du fichier ;
- Le principe de sécurité et de confidentialité : le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations ;
- Les droits des personnes.

**Les collectes de données personnelles doivent être limitées à vos stricts besoins et bien préciser quel en est l'usage ainsi que la durée de conservation. Au-delà, elles doivent effectivement être détruites.**

Source : <https://donnees-rgpd.fr/> (Coheris) et [www.cnil.fr](http://www.cnil.fr) (CNIL)

