## Texte RGPD : <https://www.cnil.fr/reglement-europeen-protection-donnees> <https://www.cnil.fr/fr/rgpd-par-ou-commencer> 1. Constituez un registre de vos traitements de données

**Dans votre registre, créez une fiche pour chaque activité recensée**, en précisant :

* **L’objectif poursuivi** (la finalité - exemple : la fidélisation client) ;
* **Les catégories de données utilisées** (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;
* **Qui a accès aux données** (le destinataire - exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
* [La durée de conservation de ces données](https://www.cnil.fr/fr/limiter-la-conservation-des-donnees) (durée durant laquelle les données sont utiles d’un point de vue opérationnel, et durée de conservation en archive).

Les données personnelles ne peuvent être conservées de façon indéfinie dans les fichiers informatiques : une durée de conservation doit donc être déterminée en fonction de l’objectif ayant conduit à la collecte de ces données. Une fois cet objectif atteint, ces données devraient être archivées, supprimées ou anonymisées (afin notamment de produire des statistiques)

[Informer](https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation) représentants légaux et élèves des conditions dans lesquelles vous traitez leurs données  
Prévoir des mesures de sécurité adaptées au regard des risques.

Informer = L’obligation d’information existe déjà dans la loi Informatique et Libertés. Elle est renforcée par le RGPD : l’information doit être plus complète et plus précise. Elle est par ailleurs assouplie sur les modalités de fourniture et de présentation de cette information.

La transparence permet aux personnes concernées :

* de connaître la raison de la collecte des différentes données les concernant ;
* de comprendre le traitement qui sera fait de leurs données ;
* d’assurer la maîtrise de leurs données, en facilitant l’exercice de leurs droits.

Pour les responsables de traitement, elle contribue à un traitement loyal des données et permet d’instaurer une relation de confiance avec les personnes concernées.  
<https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence>  
<https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles>  
<https://www.cnil.fr/fr/limiter-la-conservation-des-donnees>

1. **Faites le tri dans vos données**

**La constitution du registre vous permet de vous interroger sur les données dont votre entreprise a réellement besoin.**

Pour chaque fiche de registre créée, vérifiez que :

* les données que vous traitez sont nécessaires à vos activités (par exemple, il n’est pas utile de savoir si vos salariés ont des enfants, si vous n’offrez aucun service ou rémunération attachée à cette caractéristique) ;
* vous ne traitez aucune donnée dite « sensible » ou, si c’est le cas, que vous avez bien le droit de les traiter (voir la fiche « Traitements de données à risque : êtes-vous concerné ? ») ;
* seules les personnes habilitées ont accès aux données dont elles ont besoin ;
* vous ne conservez pas vos données au-delà de ce qui est nécessaire.

1. **Respectez les droits des personnes**

Le RGPD renforce l’obligation d’information et de transparence à l’égard des personnes dont vous traitez les données (clients, collaborateurs, etc.).

**Informez les personnes**

A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d’information.

Vérifiez que l’information comporte les éléments suivants :

* pourquoi vous collectez les données (« la finalité » ; par exemple pour gérer l’achat en ligne du consommateur) ;
* ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s’agir du consentement de la personne concernée, de l’exécution d’un contrat, du respect d’une obligation légale qui s’impose à vous, de votre « intérêt légitime ») ;
* Qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.) ;
* Combien de temps vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle ») ;
* Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;
* Si vous transférez des données hors de l’UE (précisez le pays et l’encadrement juridique qui maintient le niveau de protection des données).

Droit des personnes détails : <https://www.cnil.fr/fr/respecter-les-droits-des-personnes>

## Sécurisez vos données

Si le risque zéro n’existe pas en informatique, vous devez prendre les mesures nécessaires pour garantir au mieux la sécurité des données. Vous êtes en effet tenu à une obligation légale d’assurer la sécurité des données personnelles que vous détenez.

Vous garantissez ainsi l’intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas de d’incident.

**Des réflexes doivent être mis en place** : mises à jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement de vos données dans certaines situations. En cas de perte ou vol d’un outil informatique, il sera plus difficile pour un tiers d’y accéder