

FAQ réalisée avec le concours de la CNIL

1- Le professionnel est-il obligé de demander la date de naissance de tous ses clients lors de la conclusion du contrat pour éviter tout risque d'inexécution d'un jugement, en cas d'un litige ?

NON car ce serait disproportionné de demander la date de naissance de tous ses clients du fait du risque d'impayé/non-exécution de jugement ultérieur.

Faire exécuter la décision de justice rendue par le tribunal est subordonnée à 2 conditions :

- La notification au débiteur,
- L'existence des voies de recours - appel et opposition - purgées ou si le juge a assorti son jugement d'une exécution provisoire.

L'huissier mettra en œuvre des mesures d'exécution forcée - [saisie conservatoire](#), saisie exécution, [saisie attribution](#), saisie appréhension, [saisie vente](#)... - de nature à contraindre le débiteur à respecter ses obligations légales ou exécuter ses engagements contractuels.

2- Un référent « données personnelles » doit-il être nommé dans chaque entreprise ?

NON la désignation d'un délégué à la protection des données (DPO) est obligatoire pour :

- Les autorités et organismes publics,
- Les organismes dont les activités principales les amènent à réaliser un suivi régulier et systématique des personnes, à grande échelle. Exemple : compagnies d'assurance, banques, opérateurs téléphoniques, fournisseurs d'accès à Internet,
- Les organismes dont les activités principales les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Un délégué n'est donc pas obligatoire dans l'immense majorité des TPE PME. Un référent peut être utile pour disposer d'une expertise si la taille de l'entreprise le permet. Échanger avec d'autres entrepreneurs de votre secteur d'activité ou consulter votre fédération professionnelle vous aidera à mieux appréhender la mise en œuvre du RGPD.

3- Existe-t-il des outils/logiciels pour automatiser la suppression des fichiers à partir du moment où le délai de conservation est dépassé ?

La suppression automatique des données dont la durée de conservation est dépassée est une mesure fonctionnelle permettant de respecter la limitation de la durée de conservation.

La CNIL n'a pas encore de recommandations car il n'y a pas d'outil simple en la matière, cela dépend complètement de la nature du traitement et des conditions de mise en œuvre.

L'effacement sécurisé pour sa part consiste à supprimer des données d'un support physique sans que celles-ci soient récupérables. Cette mesure de sécurité permet d'éviter que les données puissent être récupérées en cas d'accès au support de stockage jeté par le responsable de traitement (ordinateur, téléphone, tablette, imprimantes...).

La CNIL recommande d'utiliser des logiciels dédiés à la suppression de données sans destruction physique qui ont été audités ou certifiés et l'ANSSI accorde des certifications de premier niveau à des logiciels de ce type.

Il existe des solutions gratuites quand il s'agit de supprimer <https://www.zdnet.fr/guide-achat/quels-sonr-les-outils-gratuits-pour-detruire-definitivement-des-documents-sur-votre-ordinateur-39844514.htm>.

4- Avec l'accord des salariés, est-il possible de déroger à certaines règles du RGPD ?

Non, il ne peut pas être dérogé au RGPD, il établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation des données, qui ne peuvent pas faire l'objet d'une dérogation, même avec l'accord des salariés.

5- Comment pouvoir communiquer simplement autour du RGPD vis-à-vis de ses salariés ?

Un salarié peut demander à son employeur l'accès et la communication des données personnelles qu'il a en sa possession, il a un droit d'accès à ses données. Le salarié est informé par son employeur de ce droit, par exemple par mail.

L'employeur peut également communiquer autour du RGPD en organisant des réunions de sensibilisation (lutte contre les cyberattaques, lois qui s'appliquent par exemple), en diffusant des fiches pratiques sur le RGPD, des guides sur les bonnes pratiques à adopter pour respecter le RGPD (verrouiller son ordinateur, changer de mot de passe régulièrement, etc...)

6- Comment pouvoir communiquer simplement autour du RGPD vis-à-vis des fonctions qui manipulent des données sensibles en entreprise ?

Organiser une réunion spécifique pour les personnes qui utilisent des données sensibles de l'entreprise, organiser des formations et mettre en place les mesures techniques permettant de garantir le respect de la confidentialité renforcée de ces données (habilitations, chiffrement ...).

7- En quoi consistent les données sensibles ?

Les données sensibles constituent une catégorie particulière de données à caractère personnel qui ne peuvent être traitées que par exceptions au principe d'interdiction qui s'applique.

Elles relèvent des informations qui représentent un risque important pour les droits et libertés des personnes concernées : l'origine ethnique ou raciale supposée ; les convictions religieuses ou philosophiques ; le traitement des données génétiques ; les opinions politiques ; l'appartenance syndicale ; la santé ; la vie sexuelle ou l'orientation sexuelle ; les données biométriques qui permettent l'identification d'une personne ; les données sur les infractions ou condamnations.

En France, le numéro de sécurité sociale fait aussi partie des informations bénéficiant d'une protection renforcée (nécessité d'une autorisation par décret pour le traiter).

8- Quelles sont les obligations pour les entreprises, en termes de RGPD, induites par une opération de prospection commerciale ?

La prospection commerciale est une activité légitime pour l'entreprise qui doit toutefois s'assurer que les personnes ont préalablement été informées et mises en mesure d'exercer leur droit d'opposition (courrier postal ou téléphone sauf automates d'appel ou encore mël en BtoB lié à l'objet social de l'entreprise) ou de consentement (mël, automates d'appel).

Attention en cas d'usage de listes pré établies à s'assurer auprès du prestataire que ces principes ont bien été respectés.

Le consentement doit être libre, spécifique, éclairé et univoque (par exemple, une case à cocher dédiée, qui ne soit pas pré-cochée). L'acceptation des conditions générales de vente ne peut pas suffire.

9- Quelles mesures doit prendre une entreprise qui subit une violation des données personnelles qu'elle détient ?

| Pour les personnes concernées, la violation engendre : | Aucun risque | Un risque | Un risque élevé |
|--|--------------|-----------|-----------------|
| Documentation interne , dans le « registre des violations » | X | X | X |
| Notification à la CNIL , dans un délai maximal de 72h | - | X | X |
| Information des personnes concernées dans les meilleurs délais, hors cas particuliers | - | - | X |

10- Où peut-on trouver des formules types RGPD à mettre en bas des mails ?

Sur le site de la Cnil : <https://www.cnil.fr/fr/exemples-de-formulaire-de-collecte-de-donnees-caractere-personnel> ou dans les guides professionnels qui sont réalisés par secteur d'activité

11- Que faire des feuilles d'épargne qui datent de plusieurs années, par exemple dix ans ?

Sauf obligation légale, les feuilles d'épargne doivent être supprimées.