

DONNEES PERSONNELLES ET RGPD : COMMENT FAIRE ?



MARS 2018

Chaque entreprise dispose de données personnelles. Les règles qui s'appliquent à leur gestion sont régies par la loi 78-17 dite loi Informatique et libertés jusqu'au 25 mai 2018.

A cette date, le Règlement (européen) général de protection des données (RGPD) entre en application. Il fixe de nouvelles règles qui auront un impact sur votre entreprise, parmi lesquelles des sanctions pouvant aller jusqu'à 4% du chiffre d'affaires annuel.

Ainsi, chaque entreprise, chaque association, quelle que soit sa taille et son secteur d'activité, devra modifier nombre de réflexes existants sur le recueil, le traitement et la conservation des données personnelles, qu'elles soient numériques ou sous format papier.

Pour ce faire, la CPME avec le concours de la CNIL, vous transmet les étapes-clés du passage à une meilleure sécurité des données que vous collectez et/ou traitez, pour vous conformer aux exigences du RGPD.

Ces étapes-clés sont au nombre de 9 et détaillées dans le présent document.

Si vous ne connaissez pas encore le RGPD ou que vous souhaitez un rappel de la définition d'une donnée personnelle ou des principaux changements issus du RGPD, reportez-vous d'abord à la [fiche de la CPME sur le RGPD](#)
[www.cpme.fr/onglet économie-fiscalité/guides et fiches pratiques](http://www.cpme.fr/onglet-economie-fiscalite/guides-et-fiches-pratiques)

Notez que le RGPD n'impose quasiment plus de formalités préalables à effectuer concernant les fichiers de données personnelles, mais repose sur le **principe d'accountability** : l'obligation pour les entreprises de mettre en place des procédures internes permettant de démontrer le respect des règles issues du RGPD. Les contrôles de la CNIL viseront à vérifier le respect, dans les faits, du cadre de protection des données et les preuves de la mise en place de telles procédures internes.

Les 9 étapes à suivre pour se conformer aux exigences du RGPD :

- Etape 1. Désigner une personne référente pour l'entreprise**
- Etape 2. Etablir un registre des données personnelles utilisées dans l'entreprise**
- Etape 3. Analyser les données du registre**
- Etape 4. Mettre en place des mesures pour sécuriser les données et sensibiliser tous les salariés de l'entreprise**
- Etape 5. Permettre le droit à la portabilité**
- Etape 6. Informer du droit à la portabilité**
- Etape 7. Mener une analyse d'impact relative à la protection des données (DPIA) pour certains traitements strictement définis**
- Etape 8. Programmer la suppression des données**
- Etape 9. Réagir immédiatement en cas d'atteinte/de risque d'atteinte aux données personnelles**

Annexe 1 : exemple de courrier papier/électronique à adresser aux salariés pour leur mentionner les démarches en cours dans l'entreprise pour se conformer au RGPD

Etape 1. Désigner une personne référente des données pour l'entreprise

Pourquoi ?

Le RGPD fait référence à un Délégué à la protection des données (DPO), qui est la personne en charge de tout ce qui a trait aux données personnelles pour l'entreprise.

Il n'est obligatoire que dans 2 situations :

- Lorsque vos activités de base vous amènent à réaliser un suivi à grande échelle¹, régulier et systématique des personnes,

- Lorsque vos activités de base vous amènent à traiter à grande échelle des données dites « sensibles » (orientation sexuelle, convictions religieuses, données biométriques, génétiques ou de santé, origine raciale ou ethnique, etc.), ou relatives à des condamnations pénales et infractions.

Toutefois, même lorsque vous n'êtes pas dans une de ces deux situations, il est recommandé de désigner un DPO, ou tout au moins une personne dédiée au sujet des données personnelles dans l'entreprise, qui sera la personne référente.

Comment ?

Lorsque la désignation est obligatoire, l'entreprise peut désigner un membre de son personnel en déterminant le temps alloué à sa mission, ou une personne extérieure

Pour les autres, il est recommandé d'avoir une personne qui sera celle, pour l'entreprise, référente sur le sujet. Elle peut être ou non membre du personnel.

Pour les chefs d'entreprise souhaitant faire appel à un DPO externe, il faut penser à faire jouer la concurrence. Attention aux démarchages abusifs. Rapprochez-vous de votre fédération ou syndicat professionnel qui pourra vous apporter des conseils pratiques.

Son rôle : conseiller et informer en interne, recenser les fichiers dont l'entreprise dispose (« registre des données personnelles »), gérer la mise en place des procédures internes visant à assurer la confidentialité et la protection des données ; constituer le lien avec la CNIL le cas échéant.

 A chaque étape, n'oubliez pas le principe d'accountability qui vous oblige à conserver les preuves de vos actions de mise en conformité !

¹ La notion de « traitement à grande échelle » n'a pas été définie au sein du Règlement, mais la CNIL a publié une FAQ sur le sujet : www.cnil.fr/professionnel, « besoin d'aide » puis rubrique « Règlement européen » et elle fournit des exemples.

La gestion des données des voyageurs utilisant des transports en commun sont considérés comme des traitements de données à grande échelle, comme ceux de gestion clients des banques, assurances, opérateurs téléphoniques ou les fournisseurs d'accès internet, à l'inverse des traitements de données d'un médecin ou d'un avocat.

Etape 2. Etablir un registre des données personnelles utilisées dans l'entreprise

Pourquoi ?

Utiliser un tel registre permet à l'entreprise :

- de réaliser une « photographie » des données personnelles collectées et traitées par l'entreprise, qu'elles le soient par voie informatique ou papier.
- de savoir quelles données sont utilisées et par quels services. C'est ainsi que l'entreprise sera en mesure d'évaluer l'impact du RGPD dans sa structure.

Comment ?

Ce registre se fait avec un fichier informatique ou un document manuscrit, ce qui vous convient le mieux. Il existe un modèle sous format Excel sur le site de la CNIL, pour le télécharger, [cliquez ici](#)² puis cliquez « modèle de registre règlement européen ». La CNIL prépare par ailleurs une version allégée destinée aux PME.

Ce registre doit vous permettre de réaliser une « photographie » des données que vous avez collectées et de la manière dont elles sont traitées dans l'entreprise.



A chaque étape, n'oubliez pas le principe d'accountability qui vous oblige à conserver les preuves de vos actions de mise en conformité !

² Le lien est : www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

Etape 3. Analyser les données du registre

Pourquoi ?

Une fois l'ensemble des données collectées et traitées dans l'entreprise réunies au sein du registre, il faut analyser l'ensemble de ces données afin de vérifier dans quelle mesure les traitements sont conformes au RGPD.

Comment ?

Il faut vérifier, pour chaque traitement :

- les circonstances de collecte des données : consentement obtenu ? Sans consentement, la collecte répondait-elle à d'autres obligations (collecte nécessaire au contrat, obligation légale du responsable du traitement, sauvegarde des intérêts vitaux de la personne, exécution d'une mission d'intérêt public ou poursuite d'intérêt légitime par le responsable) ?
- l'information délivrée aux personnes faisant l'objet de la collecte et du traitement : les personnes ont-elles été informées, lors de la collecte, de la finalité du traitement de celles-ci et de leurs droits ? La CNIL prépare des modèles de mentions d'informations qui pourront être utilisées par les PME.
- la nature des données collectées au regard de la finalité : seules les données strictement nécessaires au traitement et à la finalité recherchées peuvent être collectées et traitées.

Précision de la CNIL :

Pour les fichiers existants, les entreprises qui ont accompli une déclaration de conformité à la Norme CNIL relative aux fichiers clients-prospects et vente en ligne (dite [Norme NS-048](#)) ou autres normes relatives à la gestion des salariés (gestion administrative, badgeuse, gestion de flottes de véhicules, ...) n'auront pas, pendant 3 ans, à réaliser une étude d'impact.



A chaque étape, n'oubliez pas le principe d'accountability qui vous oblige à conserver les preuves de vos actions de mise en conformité !

Etape 4. Mettre en place des mesures pour sécuriser les données et sensibiliser tous les salariés de l'entreprise

Pourquoi ?

Une fois le registre complété avec les éléments ci-dessus, permettant de faire une « photographie » des données qui sont collectées et traitées par l'entreprise, il convient de prendre des mesures pour se conformer au RGPD et faire un point pour les futures données qui seront collectées.

Une des grandes lignes du RGPD est que la protection des données qui sont confiées à une entreprise concerne toutes les personnes de l'entreprise qui ont à utiliser ou à connaître, à un moment, ces données. La sécurité des données personnelles est l'affaire de tous et il faut donc prendre des mesures et sensibiliser les protagonistes.

Notez que, désormais, avec le RGPD, il n'y a plus, sauf exception, de formalités préalables à effectuer auprès de la CNIL. C'est au chef d'entreprise (avec l'aide de la personne référente (cf. étape 1) de mesurer et estimer le risque que fait peser une collecte ou un traitement de données sur les personnes concernées et prendre ainsi les mesures de sécurité appropriées.

Comment ?

- Informer l'ensemble des salariés de la mise en application, dans l'entreprise, du RGPD en en fournissant les grandes lignes et ce qui est attendu des entreprises³ ;
- Indiquer dans les documents de collecte notamment, la finalité de cette collecte et du traitement prévu⁴ et les droits des personnes ; des mentions d'informations seront prochainement proposées par la CNIL ;
- Laisser à la personne la possibilité de s'opposer au traitement indiqué⁵ ;
- Indiquer les coordonnées de la personne à contacter pour que la personne puisse faire valoir ses droits de modification et de suppression ;
- Prévoir un lien de désinscription à chaque newsletter envoyée ;
- Prévoir la sécurisation des locaux dans lesquels les données sont conservées, une accessibilité restreinte aux bureaux/salles contenant des données personnelles, la protection de base pour la sécurité informatique : mot de passe robuste changé régulièrement, pare-feu et antivirus pour chaque ordinateur, mise à jour régulière des logiciels (en ce sens, [voir les 12 bonnes pratiques prodiguées par l'Agence nationale de sécurité des systèmes d'information de PME, en collaboration avec la CPME](#)⁶) ;
- Lorsqu'il est fait appel à un sous-traitant qui accède aux données personnelles de l'entreprise : un contrat entre l'entreprise donneur d'ordre et le sous-traitant est indispensable, contrat qui doit prévoir que ce dernier ne traite notamment que les données qui lui sont confiées au regard de la demande de l'entreprise, qu'il doit informer cette dernière en cas de faille de la sécurité et qu'il doit respecter les obligations indiquées précédemment, pour se conformer au RGPD.

💡 A chaque étape, n'oubliez pas le principe d'accountability !

³ Cf. document en Annexe 1

⁴ La CNIL proposera avant le 25 mai des mentions d'informations et de recueil du consentement

⁵ Sous réserve qu'aucun motif légitime n'y fasse obstacle sauf s'agissant de la prospection commerciale pour laquelle les personnes disposent toujours de la possibilité de refuser tout contact commercial de votre entreprise

⁶ Guide téléchargeable à partir de : www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/

Etape 5. Permettre le droit à la portabilité

Pourquoi ?

Le droit à la portabilité est la possibilité pour les personnes de récupérer une partie de leurs données dans un format ouvert et lisible par machine. Le droit à la portabilité est un droit issu du RGPD, il n'existait pas jusqu'alors. Il vise à offrir aux personnes la possibilité d'obtenir et de réutiliser leurs données personnelles pour répondre à leurs propres besoins, à travers différents services.

Ce nouveau droit s'applique si ces trois conditions sont toutes réunies :

- Le droit à la portabilité est limité aux données personnelles fournies par la personne concernée (pas celles ajoutées, en complément, par l'entreprise ni celles qui auraient été déduites de l'activité des personnes par une analyse par exemple⁷) ;
- Il ne s'applique que si les données sont traitées de manière automatisée (les fichiers papiers ne sont donc pas concernés) et sur la base du consentement préalable de la personne concernée ou de l'exécution d'un contrat conclu avec la personne concernée ;
- L'exercice du droit à la portabilité ne doit pas porter atteinte aux droits et libertés de tiers, dont les données se trouveraient dans celles transmises suite à une demande de portabilité.

Comment ?

Le RGPD impose aux organismes d'offrir aux personnes la possibilité de télécharger directement leurs données personnelles et de ne pas faire obstacle à la transmission de ces données à un autre responsable du traitement, soit par l'intermédiaire de la personne concernée, soit directement lorsque c'est techniquement possible.



A chaque étape, n'oubliez pas le principe d'accountability qui vous oblige à conserver les preuves de vos actions de mise en conformité !

⁷ Exemple de données ajoutées par l'entreprise : la fréquence d'achat de la personne pour un fichier client

Etape 6. Informer du droit à la portabilité

Pourquoi ?

Qui dit nouveau droit dit nécessité d'en informer les bénéficiaires.

Comment ?

Le G29 recommande aux responsables du traitement d'expliquer clairement la différence entre les données pouvant être transmises dans le cadre du droit à la portabilité et celles pouvant être communiquées au titre du droit d'accès.

A titre de rappel, le droit d'accès peut porter sur toutes les données personnelles concernant le demandeur alors que le droit à la portabilité ne concerne que les données personnelles fournies par la personne et traitées sur la base de son consentement ou de l'exécution d'un contrat.



A chaque étape, n'oubliez pas le principe d'accountability qui vous oblige à conserver les preuves de vos actions de mise en conformité !

Etape 7. Mener une analyse d'impact relative à la protection des données (DPIA) pour certains traitements strictement définis

Pourquoi ?

Le G29 ou groupe des CNIL européennes, prévoit l'obligation d'effectuer une analyse d'impact pour certains traitements, dès lors qu'il y a combinaison de deux des critères suivants :

- Evaluation ou notation ;
- Décision automatisée avec effet juridique ou effet similaire significatif ;
- Surveillance systématique ;
- Données sensibles ou données à caractère hautement personnel ;
- Données personnelles traitées à grande échelle ;
- Croisement d'ensembles de données ;
- Données concernant des personnes vulnérables ;
- Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
- Exclusion du bénéfice d'un droit, d'un service ou contrat.

Comment ?

L'analyse d'impact permet d'évaluer, en particulier, l'origine, la nature, la particularité et la gravité du risque pour les droits et libertés des personnes concernées.

Elle doit contenir :

- une description des opérations de traitement envisagées et des finalités du traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- la liste des mesures envisagées pour réduire les risques (les garanties, mesures et mécanismes de sécurité tels que le chiffrement et la pseudonymisation).

La CNIL met un logiciel dédié à disposition : www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Pour en savoir plus : reportez-vous à la page dédiée sur le site de la CNIL : www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-pia



A chaque étape, n'oubliez pas le principe d'accountability qui vous oblige à conserver les preuves de vos actions de mise en conformité !

Etape 8. Programmer la suppression des données

Pourquoi ?

Le RGPD impose de procéder à la suppression des données personnelles dès lors qu'elles ne sont plus nécessaires au regard de la finalité en application du principe de durée de conservation limitée.

Par ailleurs, les personnes disposent d'un droit à l'oubli et à l'effacement qu'elles peuvent exercer dans certains cas, par exemple :

- Collecte / traitement illégal (sans consentement ou lorsque la collecte ne répondait pas à d'autres obligations (cf. Etape 3)),
- Exercice du droit d'opposition sans qu'un motif légitime n'y fasse obstacle.

Comment ?

Il est nécessaire de prévoir des délais de suppression des données, en fonction de chaque fichier. Afin de ne pas oublier de procéder à la suppression, il est recommandé de programmer des mécanismes de suppression automatique ou alertes sur les outils utilisés pour la conservation des fichiers. Il en existe sur certains outils, par exemple, sur Excel.

Quant aux délais de conservation de ces données, la CNIL recommande par exemple de conserver :

- les données clients le temps de la relation commerciale (acte d'achat ou jusqu'à l'expiration d'une garantie par exemple),
- les données des prospects 3 ans à compter du dernier contact,
- les données des candidats à un poste 2 ans à compter de la réception de la candidature.

 A chaque étape, n'oubliez pas le principe d'accountability qui vous oblige à conserver les preuves de vos actions de mise en conformité !

Etape 9. Réagir immédiatement en cas d'atteinte/de risque d'atteinte aux données personnelles

Pourquoi ?

Le leitmotiv du RGPD est la protection des données personnelles recueillies. Aussi, dès lors qu'une violation de données (telle qu'une faille) est portée à la connaissance de l'entreprise et que celle-ci a un impact sur des données personnelles, la CNIL doit en être informée.

Comment ?

Que ce soit en cas de perte ou suppression par erreur de données dans des fichiers, ou en cas d'accès à un fichier par une personne non autorisée, ou encore en cas d'attaque informatique pouvant entraîner une divulgation de données personnelles, le RGPD vous impose d'avertir la CNIL au plus vite, idéalement dans les 72h suivant la découverte de l'incident.

Un téléservice sera disponible dès le mois de mai 2018 sur www.cnil.fr.

Attention, lorsque cette violation crée un risque élevé d'atteinte pour les personnes (ex. divulgation de résultats médicaux, de numéros de carte bancaire de profils issus d'un site de rencontre, etc.), l'entreprise doit les informer de la violation, des conséquences probables et des mesures qu'il convient d'adopter.



A chaque étape, n'oubliez pas le principe d'accountability qui vous oblige à conserver les preuves de vos actions de mise en conformité !

Annexe 1 : Exemple de courrier papier/électronique à adresser aux salariés pour leur mentionner les démarches en cours dans l'entreprise pour se conformer au RGPD

Il est recommandé d'informer l'ensemble des salariés de la mise en application, dans l'entreprise, du RGPD en en fournissant les grandes lignes et ce qui est attendu des entreprises et, ainsi, de leurs salariés. Il conviendra, également, de les sensibiliser au sujet.

Madame, Monsieur,

Le 25 mai 2018 entre en application un Règlement européen relatif à la protection des données personnelles (RGPD). Celui-ci oblige toutes les entreprises et associations à respecter de nouvelles règles concernant les données personnelles au risque de sanctions lourdes.

Dans notre structure, c'est Monsieur/Madame XXXXXX, la personne référente sur le sujet. Je vous invite à la/le contacter pour toute interrogation.

Je vous informe que pour nous conformer au RGPD, nous nous engageons :

- au recueil clair et non équivoque du consentement de la personne qui nous transmet ses données personnelles, à moins que la collecte des données soit nécessaire au contrat ou qu'elle fasse suite à une obligation légale à laquelle nous sommes soumis ou encore que cela soit justifié par la sauvegarde des intérêts vitaux de la personne ou encore par l'exécution d'une mission d'intérêt public ou la poursuite, par notre structure, d'intérêt légitime,*
- à une obligation d'information de l'utilisation qui sera faite par nous des données personnelles, qu'il s'agisse de vos données ou de celles de nos clients ou prospects, fournisseurs, ...*
- à une information sur les droits de ces personnes en ce qui concerne la possibilité, le cas échéant, de s'opposer ou de consentir à cette utilisation, ainsi que d'exercer un droit d'accès, de rectification ou suppression des données,*
- à fixer des durées de conservation pour toutes les catégories de données et fonction des règles de prescription et d'archivage légal,*
- à ne pas solliciter plus de données que nous en avons besoin pour notre activité (principe de proportionnalité).*

Je vous demande de bien vouloir respecter ces règles en vous conformant aux procédures et documents que nous avons mis à votre disposition à cette fin. → Joindre les nouveaux formulaires, nouveaux documents de procédures, etc.

De plus, désormais, pour respecter notre obligation de sécurisation des données en notre possession, et conformément à la nouvelle version du Règlement intérieur, je vous demande de bien vouloir fermer la porte de votre bureau et de verrouiller la session utilisateur dès lors que vous ne vous trouvez pas dans votre bureau/à votre poste de travail, de fermer à clé les tiroirs et meubles dans lesquels sont entreposées les données personnelles (de clients ou de salariés par exemple). Je vous demande également d'indiquer à la personne référente pour les données personnelles dans l'entreprise, impérativement et sans délai toute atteinte aux fichiers que vous constateriez. → Modifier le règlement intérieur en ce sens.

Sachez que pour vous, salariés de l'entreprise, nous nous engageons à supprimer l'ensemble des données personnelles vous concernant dans les délais imposés.

Ce guide a été réalisé par la CPME avec le concours de la CNIL.

En savoir plus :

www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_fr

Pour vous aider :

Service de la CNIL dédié aux professionnels

www.cnil.fr/fr/vous-souhaitez-contacter-la-cnil