startup

RGPD

Recommandations et conseils pour votre mise en conformité

CHER CLIENT

Le **Règlement Général de Protection des Données**, présenté sous l'appellation **RGPD**, est un texte de loi adopté le 27 avril 2016 par l'Union Européenne.

Sa **mise en application** est prévue **le 25 mai 2018**.

Ce texte encadre la collecte, le traitement et la circulation des données personnelles pour tous les ressortissants de l'Union Européenne.

Toutes les entreprises, organismes et collectivités sont concernés : Vous aussi.

Des contrôles seront exercés et les sanctions prévues en cas de non-respect peuvent être lourdes. Il ne faut donc pas prendre cette obligation à la légère et oeuvrer à la mise en conformité.

Dans ce contexte, Startup vous diffuse ce document d'information qui, nous l'espérons, vous aidera dans votre démarche de mise en conformité.

L'équipe Startup

Focus sur le RGPD

Qu'est-ce que le RGPD ?

Approuvé par 29 pays signataires de l'UE, c'est un texte qui structure et impose de **nouvelles règles sur la collecte et l'utilisation des données personnelles**.

Mise en application : le 25 mai 2018

La réforme poursuit 4 objectifs :

- Renforcer les droits des personnes et la protection des données
- Rendre aux individus la maîtrise de leurs informations personnelles
- Responsabiliser les acteurs traitant les données
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données (CEPD)

Vous pouvez consulter le règlement intégral sur le site de la CNIL :
https://www.cnil.fr/fr/reglement-europeen-protection-donnees

à savoir que …

De nombreuses formalités auprès de la CNIL vont être supprimées. En contrepartie, la responsabilité des entreprises sera renforcée.

L'objectif est de faire un transfert de responsabilités de la CNIL vers les entreprises ou les organismes.

Les entreprises ont donc la responsabilité des données qu'elles collectent et stockent.

Ainsi, elles doivent les sécuriser, documenter et justifier tout le processus de collecte des données.

En cas de contrôle, **ce n'est plus à la CNIL de prouver qu'il y a un manquement, mais à l'entreprise ou à l'organisation de démontrer sa bonne pratique.**

Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle selon l'article 2 :

« Constitue une donnée à caractère personnel, ***toute information relative à une personne physique*** *identifiée ou qui peut être identifiée,* ***directement*** *ou* ***indirectement****, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres .... ».*

Exemples

Date de naissance	N° de Téléphone	E-mail
Immatriculation	Localisation	Etc.

La loi distingue certaines **données personnelles** comme **sensibles** qui font l'objet de dispositions particulières (selon l'article 9) :
Données génétiques ou biométriques, données médicales, sanctions administratives, opinions politiques, orientations sexuelles ...

Enfin en France, la loi de 1978 encadre particulièrement la collecte de certaines données :
Origine raciale et ethnique, appartenance religieuse, appartenance syndicale ...

à savoir que ...

Les informations relatives aux sociétés (personnes morales) ne sont pas considérées comme des données personnelles.

Par contre, les informations relatives aux contacts (personnes physiques) de ces mêmes sociétés sont considérées comme des données personnelles.

Une donnée personnelle est une donnée qui concerne une personne physique dont on peut identifier l'identité. Ainsi, les données personnelles anonymisées ne sont pas concernées.

Qui est concerné ?

Sont concernés par le RGPD :

« Toutes les entreprises ou organismes qui collectent, traitent et stockent des données personnelles relatives à des ressortissants européens. ».

Nous pouvons considérer que
toutes les entreprises sont concernées,
sans distinction de taille ou de volume de données personnelles collectées ou traitées.

à savoir que …

Dès lors qu'une société détient des données personnelles, elle est concernée par le RGPD.

Ainsi, l'utilisation de base de données ou de fichiers clients ou prospects (ex: CRM, ERP…) avec des noms, prénoms, adresses email… entrent dans le champ d'application, de même que les données relatives aux salariés de l'entreprise ou de l'organisme.

Toutes les collectes d'informations relatives à des personnes physiques sont concernées. ex :

- sites internet via les formulaires, comptes utilisateurs …
- sur supports-papier ou digitaux pour des questionnaires, sondages, jeux-concours …
- en point de vente pour des cartes de fidélité …
- Etc.

Quels sont les droits renforcés par le RGPD ?

Une extension des droits individuels

1. **Droit à une information complète** sur le traitement des données, exprimée de façon claire et simple **avant de donner son consentement**

2. **Droit d'être informé en cas de violation** de ses données personnelles

3. **Droit à l'oubli**

4. **Droit à la limitation** du traitement

5. **Droit à la portabilité** des données (changement de fournisseur)

6. **Droit d'opposition** (encadrement du profilage)

7. **Dispositions** propres aux **personnes mineures**

à savoir que …

1. Pour chaque collecte de données, expliquer l'utilisation, traitement et durée de conservation et recueillir une preuve de consentement

2. Le délai est de 72h pour déclarer une violation de données à la CNIL

3.Pour demander la suppression de ses données

4. Pour stopper des traitements y compris par une action en justice

5. Pour récupérer ses données et les confier à un autre fournisseur

6. Pour se soustraire à certains traitements élaborés à partir de profilage

7. La collecte de données personnelles de mineurs est interdite.

Qui est responsable devant la loi ?

Selon l'article 4 les responsabilités sont partagées entre :

Le **responsable de traitement**
*« Toute personne physique, morale, l'autorité publique, le service ou un autre organisme, **qui détermine les finalités et les moyens** du traitement de données à caractère personnel. »*
En d'autres termes, **vous, client de Startup**.

Le **sous-traitant**
*« Toute personne physique, morale, l'autorité publique, le service ou un autre organisme, **qui traite des données** à caractère personnel **pour le compte d'un responsable de traitement**. »*
Exemples :
- *Votre prestataire informatique qui a accès à vos données*
- *Votre cabinet comptable qui a accès à vos données*
- *Votre agence web qui héberge vos données*

En d'autres termes, **Startup** fait parti de cette catégorie.

Notre rôle, en tant que sous-traitant co-responsable, au-delà de notre propre conformité au RGPD, **est de conseiller le responsable de traitement (vous)** en vous incitant **à vous mettre en conformité,** ce qui est **de votre obligation**.

à savoir que …

Le RGPD utilise son propre vocabulaire :

- Le responsable de traitement est la personne (morale ou physique), c'est à dire vous propriétaire du site qui recueillez les données et les exploitez sous votre propre responsabilité.

- Lorsqu'on parle de sous-traitant, il s'agit de toutes les entreprises qui traitent vos données. En l'occurrence, nous, qui hébergeons les données que vous collectez via votre site.

- Pour les entreprises de taille importante (qui utilisent massivement les données), le RGPD impose de désigner un DPO (délégué à la protection des données) au sein de l'entreprise, pour piloter et contrôler les traitements pour le compte du responsable de traitement.

Quelles sont les sanctions ?

La loi introduit des sanctions pour la première fois :

Le législateur l'annonce : **des contrôles seront menés**
Et prévoit **des sanctions encadrées, graduées et renforcées**

La CNIL peut notamment :

- *Prononcer un avertissement*
- *Mettre en demeure l'entreprise*
- *Limiter temporairement ou définitivement un traitement*
- *Suspendre les flux de données*
- *Ordonner de satisfaire aux demandes d'exercice des droits des personnes*
- *Ordonner la rectification, la limitation ou l'effacement des données.*

S'agissant des **amendes administratives**, elles peuvent s'élever selon la catégorie de l'infraction :
De 10 à 20 millions d'euros (pour les très grandes sociétés)
De 2% à 4% du CA annuel (pour les entreprises)

à savoir que …

Les amendes sont assez lourdes dans le cas du non-respect du RGPD.

Le signal que le législateur envoie, c'est que **tout le monde est concerné** et qu'**il ne faut pas prendre ces nouvelles obligations à la légère**.

Cependant, à la date de mise en application de la loi au 25 mai 2018, on estime à un peu plus d'un quart, le nombre d'entreprises en conformité.

Si l'autorité de contrôle prévoit un « démarrage pédagogique » en évitant les sanctions dans un premier temps, il est très important de montrer que cette mise en conformité est un sujet de préoccupation central, en étant en mesure de **prouver que des démarches sont en cours**.

Comment se mettre en conformité ?

5 conditions indispensables à respecter

Pour vous conformer au RGPD, vous devez à minima respecter les conditions suivantes :

1 - **Obtenir un consentement** pour chaque collecte de données et le conserver pour pouvoir en justifier.

2 - Pour chaque collecte de données, **informer préalablement** sur la finalité, l'utilisation et la durée de conservation.

- *Si ces données sont utilisées pour des traitements de profilage, vous devez l'indiquer au moment de la prise de consentement.*
- *Vous avez également l'**obligation de minimiser la collecte des données**, en la **limitant strictement aux données indispensables** au traitement dont elles doivent faire l'objet.*

3 - Donner **les moyens de faire valoir leurs droits** aux personnes pour lesquelles vous détenez des données personnelles.

4 - Être en mesure de **justifier via la tenue d'un registre** de l'ensemble des types de collectes et de traitements réalisés.

5 - **Avertir en cas de « fuite »** ou de piratage de données personnelles.

à savoir que …

1 - Vous devez recueillir le consentement de chaque personne majeure vous confiant ses données pour pouvoir en justifier par la suite en cas de contrôle ou litige (une confirmation par mail suffit). Attention, un consentement n'est pas irrévocable.

2 - Sur le support de collecte (ex. un formulaire de contact), vous devez expliquer quelle utilisation sera faite des données collectées et combien de temps vous les conserverez. Il faudra également faire évoluer vos mentions légales et CGV.

3 - Vous devez indiquer clairement le moyen par lequel les personnes peuvent reprendre leur consentement ou faire valoir leurs droits.

4 - La tenue du registre de traitement des données est obligatoire. Il doit justifier des types de récoltes, types de données, utilisations, conservations, sous-traitance …

5 - En cas de fuite ou de piratage constaté, le responsable de traitement doit informer la CNIL dans les 72h. S'il s'agit de données à caractères sensibles, les personnes concernées doivent également en être informées.

7 étapes pour bien se préparer

Voici 7 étapes clés pour réussir votre mise en conformité au RGPD

1 - Cartographiez les données personnelles.

Recensez tous les types de données que vous collectez, stockez, et les types de traitements auxquels vous pouvez les soumettre.
Ce travail va vous permettre de classifier vos données et types de traitements pour faciliter la mise en oeuvre des étapes suivantes.

2 - Mettez en place un registre de traitement des données

Ce document doit recenser tous les types de collectes, tous les types de données personnelles et tous les traitements que vous mettez en oeuvre en indiquant **pour chaque traitement** ou **utilisation distincte** :
Le type de données personnelles collectées ; l'origine de la collecte ; l'utilisation prévue ; les conditions de stockage et de sécurité ; le partage avec un sous-traitant pour le traitement ou l'hébergement des données ; la durée de conservation des données ;

3 - Mettez en place un registre des sous-traitants

Ce document doit identifier tous les sous-traitants qui soit interviennent sur vos données pour votre compte, soit les stockent ou les hébergent.
De la même manière vous devez indiquer par sous-traitant, le type de données personnelles concernées ; l'origine de la collecte ; l'utilisation prévue ; les conditions de stockage et de sécurité ; le partage avec un autre éventuel sous-traitant ; la durée de conservation des données ;

à savoir que …

1 - Identifiez le type de données personnelles que vous collectez, stockez, les moyens de collecte et les utilisations que vous en faites. Ex. fichier de clients, fichier de prospects, fichier du personnel de l'entreprise, fichier d'abonnés à la newsletter, fichier de comptes d'utilisateurs, fichier de candidatures …

2 - Il n'y a pas de règle de formalisme exigée concernant le registre de traitement. Vous pouvez utiliser par exemple une feuille de calcul de Google Drive qui sera facile à partager, et isoler chaque type de données, de collecte, ou de traitement sur un onglet différent. Il ne s'agit pas de consigner les données à proprement parlé, mais les indications sur les caractéristiques demandées.

3 - De la même manière, vous pouvez utiliser le même principe, voir le même document, pour établir le registre des sous-traitants.

7 étapes pour bien se préparer

à savoir que …

4 - Définissez les procédures internes

Pour garantir une protection des données personnelles optimale, il faut élaborer des procédures internes qui prennent en considération l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement : *(ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire, etc.).*

4 - Ce document fait état des mesures à prendre et actions à mettre en oeuvre selon les différents cas de figure pouvant survenir et qui devront être appliquées par le responsable de traitement. Ce document doit figurer dans le dossier de conformité pour être présenté en cas de contrôle.

5 - Désignez un DPO (si nécessaire)

Le DPO (Délégué à la Protection des Données) est le chef d'orchestre qui va piloter la gouvernance des données personnelles au sein de votre entreprise. Il a pour missions d'informer et de conseiller le(s) responsable(s) du traitement et de contrôler en interne le respect du règlement européen.

Si vous êtes un organisme public, vous avez l'obligation de nommer un DPO.

Si vous êtes une PME vous pouvez vous en dispenser, sauf si vous pratiquez un traitement des données à grande échelle ou manipulez des données sensibles.

5 - Un DPO doit être obligatoirement nommé si le responsable de traitement est un organisme public.
C'est le cas également pour toutes les activités qui exigent un suivi régulier de traitements de données personnelles utilisés à grande échelle.
C'est aussi le cas si dans le cadre de votre activité vous manipulez des données sensibles (bancaires, médicales …) relatives à l'article 9 du texte du RGPD.

7 étapes pour bien se préparer

6 - Menez une analyse d'impact sur la protection (si nécessaire)

Si votre activité repose ou dépend du traitement de données personnelles, si vous utilisez des données personnelles à grande échelle, ou si vous manipulez des données personnelles sensibles, il est conseillé de mener préalablement une **analyse PIA** d'impact sur la protection que vous pouvez assurer sur ces informations.

Le PIA est une étude qui vous aide à mettre en place des traitements de données respectueux de la vie privée et qui permettent d'en démontrer la conformité auprès du RGPD.

7 - Prouvez votre conformité

Vous devez constituer un dossier qui regroupe toutes les actions et documents nécessaires pour prouver votre conformité au règlement. Ce dossier sera constitué de la documentation relative aux traitements des données personnelles :

Registre de traitement des données, registre des sous-traitants, procédures internes, journal des traitements, PIA, contrats avec les sous-traitants...)

à savoir que ...

6 - Particulièrement si vous collectez et stockez des données sensibles, vous devez démontrer à l'autorité de contrôle que vous avez pris les mesures nécessaires pour assurer cette collecte et le traitement de ces données dans le respect du RGPD. De même, l'analyse d'impact vous permet de déceler les procédures à mettre en place en cas de dysfonctionnements ou de failles pour assurer la protection de ces données.

7 - Le principe est que pour toute demande de l'autorité de contrôle, vous puissiez facilement extraire et fournir un dossier complet centralisant l'ensemble des pièces qui attestent de votre conformité.
Le responsable de traitement ou son DPO s'il y a lieu, doit veiller à maintenir cette documentation pour qu'elle soit à jour.

Quelques infos supplémentaires ...

À savoir ...

Consentement : Vous avez vu que vous devez justifier du consentement des personnes pour leurs données personnelles confiées que vous conservez. *Sachez que dans le cas d'un formulaire de collecte de votre site, le mail qui réceptionne les contenus est considéré comme preuve si le champ d'opt-in y figure, ainsi que la date et les mentions relatives aux objectifs de la collecte. Ces informations sont également accessibles depuis votre CMS dans l'onglet correspondances. Vous devez conserver ces consentements, pour tout contrôle ou demande de retrait du consentement de la personne concernée.*
Nous vous conseillons de pratiquer de la même manière avec toutes vos sources de collecte.

Cookies : Il faut savoir que la réglementation sur l'utilisation et l'acceptation des cookies n'est pas encore finalisée tant ce volet est complexe à traiter. *Il semblerait que le législateur soit enclin à confier la gestion des cookies directement aux logiciels de navigation (Chrome, Firefox, Safari, Microsoft Edge ...), laissant ainsi à chaque utilisateur la possibilité de contrôler les fichiers tiers via les paramètres de confidentialité. À suivre ...*

Données personnelles et vente : Les données personnelles relatives à vos clients, dans le cadre de la contractualisation d'une vente ou d'un service, ne sont pas concernées par la RGPD. *Par contre, si vous utilisez ces mêmes données pour le solliciter en dehors du contrat que constitue la vente, elles tombent sous le coup de la réglementation.*

Nos conseils

Nos conseils ...

Nos conseils pour aborder sereinement cette évolution

Ne prenez pas cette obligation à la légère

Toutes les entreprises et organismes sont concernés, ne croyez pas que vous n'y êtes pas. Les données personnelles sont au coeur de toutes les activités à commencer par vos fichiers de contacts ou les données qui concernent vos collaborateurs !

Le sanctions sont lourdes et l'autorité de contrôle prévoit de se donner les moyens de vérifier à grande échelle.

Ne paniquez pas pour autant !

Si vous n'avez rien entamé, il y a très peu de chances que vous soyez en conformité pour le 25 mai prochain, mais vous ne serez pas seul dans ce cas.
La CNIL envisage une période probatoire pendant laquelle elle se contentera de conseiller et informer. Cela vous laisse quelques mois pour vous organiser avant de recevoir un avertissement.

L'important à ce stade est d'entamer les démarches, et de pouvoir justifier que vous êtes entrés dans ce processus de mise en conformité.

Démarrez dès que possible

Mettez en oeuvre les différentes étapes énoncées au chapitre précédent.

Ne construisez pas d'usine à gaz ! Faites les choses simplement en répondant avec pragmatisme aux obligations demandées.

Nos conseils ...

Commencez par ce qui se voit !
La premier indicateur qui peut alerter sur votre non-respect du RGPD est votre site internet. C'est aussi l'élément le plus facile à contrôler :
Tous les sites collectent des données personnelles par le biais d'au moins un ou plusieurs formulaires. Un site est toujours accessible et il est facile de programmer des contrôles à grande échelle via des outils de crawl ...

Mettez votre site en conformité ainsi que tous vos autres outils de collecte de données.

1 - **Modifiez tous vos formulaires** (contact, renseignement, abonnement newsletter, compte d'utilisateur ...) en ajoutant un bouton d'opt-in volontaire (pas de case pré-validée), une mention sur l'utilisation et la durée de conservation des données, ainsi qu'un lien pour faire valoir ses droits et notamment reprendre son consentement. *Vous devez également conserver la preuve de chaque consentement reçu (confirmation mail ou dans les correspondances du CMS).*

2 - **Créez une page « Faites valoir vos droits »**. Cette page doit donner la possibilité à une personne, de limiter l'utilisation de ses données en reprenant son consentement pour un traitement particulier, de demander la portabilité de ses données ou leur effacement complet. *Il s'agit d'un formulaire qui permettra d'engager un processus nécessitant une vérification de l'identité du demandeur.*

Nos conseils ...

Mettez votre site en conformité (suite) :

3 - **Proposez une page « Politique de confidentialité »** Cette page a pour objectif pédagogique, de démontrer votre respect de la gestion des données qui vous sont confiées, autant pour l'utilisateur que pour la CNIL. *Vous y présenterez les types de traitements que vous réservez aux données personnelles qui vous sont confiées, si vous les partagez, cédez ou non à des tiers, le soin que vous apportez à leur sécurité, et vous indiquerez comment chacun peut faire valoir ses droits sur ses données stockées.*

4 - **Modifiez votre page « Mentions légales »**. Les mentions légales de votre site devront proposer un paragraphe d'information sur votre démarche RGPD, en remplacement de celui de la CNIL qui n'a plus lieu de figurer. *Dans ce paragraphe nous vous conseillons de proposer un lien vers la page « Exercez vos droits » et d'indiquer les coordonnées du responsable de traitement. Vous procéderez de la même manière dans vos CGV si vous pratiquez le e-commerce.*

5 - **Informez sur votre utilisation des cookies**. Si votre site n'utilise que des cookies techniques et statistiques, vous n'avez rien à entreprendre. Par contre si vous utilisez des cookies publicitaires ou de géolocalisation, vous devez demander un consentement. *Dans ce cas vous devrez proposer une page d'opt-in pour ces cookies, dont un refus peut signifier l'inaccessibilité du service proposé. Ces consentements doivent être renouvelés tous les ans.*

6- **Passez votre site en HTTPS** si vous ne l'avez pas encore fait, c'est une **condition obligatoire**, dans le cadre de la sécurisation du flux des données.

Notre accompagnement ...

Comment Startup vous accompagne ...

☆ Nous vous conseillons à notre niveau d'approche

Partenaires de votre communication et votre activité web, nous intervenons à travers ce document pour **exercer notre devoir de conseil, afin de vous inciter et vous donner les moyens de respecter vos obligations** vis-à-vis de cette évolution réglementaire. Notre approche n'étant que « pratique » et non juridique, nous vous invitons à solliciter votre avocat si vous relevez d'un cas exigeant en matière de protection des données personnelles ou si vous éprouvez des difficultés dans la mise en oeuvre de vos obligations.

☆ Nous vous assurons de notre conformité au titre de sous-traitant

L'infrastructure que nous mettons à votre disposition via nos fournisseurs est **conforme aux exigences du RGPD** en proposant **un archivage et une circulation sécurisés des informations que nous hébergeons pour vous**.

Que ce soit pour l'hébergement de sites internet ou de celui des comptes mails, notre fournisseur OVH, met en oeuvre les sécurités physiques et informatiques qui s'imposent.

En ce qui concerne l'accès aux données, Medialibs, éditeur des CMS que nous déployons, garantit une mise en conformité et une maintenance logicielle systématique que nous répercutons sur les CMS, pour répondre aux exigences de sécurité des sites de nos clients.

Comment Startup vous accompagne …

☆ Nous vous accompagnons dans le cadre de votre mise en conformité

Si vous avez besoin d'aide pour réussir votre mise en conformité, **Startup est en mesure de vous proposer de manière personnalisée** :

- **des conseils**, relatifs à vos obligations dans le cadre de votre site,
- **un diagnostic opérationnel** de votre site, induisant **un plan d'actions**,
- une intervention pour **la mise en concordance de votre site** avec les exigences du RGPD.

Conformité au RGPD

Mise en application

25 mai 2018

Agence de communication • Print • Web • Digital

startup

Nous restons à votre écoute ...

contact@start-up.fr