DOSSIER RGPD 2020

Tout ce qu'il faut savoir

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
RGPD (source CNIL) (lien vers le règlement intégral)

Pour garantir une meilleure maîtrise des données personnelles et renforcer le droit des personnes, le **Règlement Général sur la Protection des Données** (RGPD) entre en application à partir du 25 mai 2018. Tout organisme (public et privé) traitant des données personnelles est tenu de se conformer au RGPD.

Qu'est-ce qu'une donnée personnelle (CNIL) ?

Toute information, identifiant directement ou indirectement une personne physique (ex. nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale, adresse IP, ADN, numéro de sécurité sociale, donnée biométrique, ensemble d'informations permettant de discriminer une personne au sein d'une population tels que, donnée physique, physiologique, génétique, psychique, économique, culturelle, sociale, la voix, une photo, lieu de résidence, profession, sexe, âge…).

Qu'est-ce qu'un traitement de données à caractère personnel (CNIL) ?

Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...)

Un traitement de données personnelles **n'est pas nécessairement informatisé :** les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Qui est concerné ?

Le RGPD s'applique à toute organisation (entreprise, association, collectivité, **publique et privée) qui traite des données personnelles pour son compte ou non.** Le RGPD **concerne aussi les sous-traitants** qui traitent des données personnelles pour le compte d'autres organismes.

Ainsi, si vous traitez ou collectez des données pour le compte de vos clients, vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées. Vous devez permettre aux personnes dont les données personnelles font l'objet d'un traitement, de maîtriser leurs données en leur conférant des droits d'accès, de rectification, d'effacement, d'opposition, etc.

Exemple : Votre expert-comptable collecte et traite certaines de vos données personnelles ainsi que les données personnelles de ses salariés, il est concerné à double titre.

https://www.youtube.com/watch?v=62xV4JKn_HA (cliquez pour voir la vidéo)

Améliorer la sécurité des données de votre entreprise.

L'actualité témoigne d'un nombre de plus en plus important de failles de sécurité et d'attaques informatiques. Ces dernières peuvent avoir des conséquences désastreuses sur l'activité des entreprises. Le niveau de sécurité de l'entreprise dans sa globalité se pose, ainsi **les données personnelles doivent faire l'objet de mesures de sécurité particulières,** informatiques et physiques.

Rassurer vos clients et donneurs d'ordre et ainsi développer votre activité.

Dans tous les secteurs d'activité, les clients seront très attentifs à la mise en œuvre du RGPD par leurs prestataires. Il s'agit donc d'un sujet crucial pour les sous-traitants qui traitent des données personnelles pour le compte d'entreprises, à la fois pour maintenir leurs relations commerciales existantes mais également pour éventuellement en conquérir de nouvelles. Si vous respectez le RGPD, vous aurez un **avantage concurrentiel !**

Quelles sont les actions à mener pour une mise en conformité RGPD ?

(Ces actions doivent perdurer dans le temps pour être efficaces).

1-Registre de traitement

Le registre listant vos traitements de données vous permettra d'avoir une vision d'ensemble.

Identifiez ou cartographiez les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données (exemples : recrutement, gestion de la paye, formation, gestion des badges et des accès, statistiques de ventes, gestion des clients prospects, etc.).

Dans votre registre, créez une fiche (sous-registre) pour chaque activité ou traitement recensés, en précisant :

- **Les acteurs :** le(s) responsable de traitement (l'entreprise), les sous-traitants.
- **Les catégories de données utilisées** (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.).
- **Descriptif du risque** : (vol, piratage, pertes de données).
- **L'objectif poursuivi ou** la finalité (exemple : Gestion du personnel, obligations légales, paiement des salaires).
- **Déterminer le flux de données** : (exemples : PC, disques dur externes, cloud, supports papier).
- **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** (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).
- **Données nécessitant** la mise en place d'une analyse d'impact (PIA).
- **Mesures de sécurité** : Mises en œuvre et préventions pour protéger les données à caractère personnel.
- **Identification et priorisation des actions à mener**.

Le registre est placé sous la responsabilité du dirigeant de l'entreprise. Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'entreprise susceptibles de traiter des données personnelles.

En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données.

2-Documentation

Vous devez constituer une documentation attestant de la conformité au RGPD.

Pour prouver la conformité au règlement, il est nécessaire de constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

LA DOCUMENTATION SUR VOS TRAITEMENTS DE DONNÉES PERSONNELLES

- **Le registre des traitements** (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants).
- **Les analyses d'impact sur la protection des données** (PIA) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes.
- **L'encadrement des transferts** de données hors de l'Union européenne (notamment, les clauses contractuelles types, les BCR et certifications)

L'INFORMATION DES PERSONNES

- **Les mentions d'information**
- Les modèles de **recueil du consentement des personnes concernées**,
- Les procédures mises en place pour **l'exercice des droits**

LES CONTRATS QUI DÉFINISSENT LES RÔLES ET LES RESPONSABILITÉS DES ACTEURS

- **Les contrats avec les sous-traitants**
- Les procédures internes **en cas de violations de données**
- Les preuves que les personnes concernées **ont donné leur consentement** lorsque le traitement de leurs données repose sur cette base.

3-Registre sous-traitant

En tant que sous-traitant, vous devez tenir un registre des catégories d'activités de traitement que vous effectuez pour le compte de vos clients. Ce registre doit être tenu par écrit et contenir :

- Le nom et les coordonnées de chaque client pour le compte duquel vous traitez des données.
- Le nom et les coordonnées de chaque sous-traitant ultérieur, le cas échéant.
- Le nom et les coordonnées du délégué à la protection des données, le cas échéant.
- Les catégories de traitements effectués pour le compte de chaque client.

- Les transferts de données hors UE que vous effectuez pour le compte de vos clients, le cas échéant.

- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles que vous mettez en place.

Tri des données collectées et stockées

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).

- Que vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter.

- Que seules les personnes habilitées ont accès aux données dont elles ont besoin.

- Que vous ne conservez pas vos données au-delà de ce qui est nécessaire.

À cette occasion, améliorez vos pratiques !

Minimisez la collecte de données, en éliminant de vos formulaires de collecte et vos bases de données toutes les informations inutiles.

Redéfinissez qui doit pouvoir accéder à quelles données dans votre entreprise.

Pensez à poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

Respecter les droits des personnes

Informez les personnes À 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 notamment 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'Union européenne** (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

- Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à **une politique de confidentialité sur votre site internet.**

À l'issue de cette étape, vous avez répondu à votre obligation de transparence.

Permettre aux personnes d'exercer facilement leurs droits

Les personnes dont vous traitez les données (clients, collaborateurs, prestataires, etc.) ont des droits sur leurs données, qui sont d'ailleurs renforcés par le RGPD : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.

Vous devez leur donner les moyens d'exercer effectivement leurs droits.

Si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée. Si vous proposez un compte en ligne, donnez à vos clients la possibilité d'exercer leurs droits à partir de leur compte.

Mettez en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

Bonne pratique : La réactivité !

Bien traiter les demandes des consommateurs quant à leurs données personnelles, c'est :

- Renforcer la confiance qui sécurise la relation-client.

- Vous mettre à l'abri de critiques sur les réseaux sociaux, ou de **réclamations auprès de la CNIL.**

Sécurisation des données
(Vous êtes tenu d'assurer la sécurité des données personnelles que vous détenez)

Garantissez-vous contre 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 d'incident.

Différentes actions doivent être mises 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.

Les failles de sécurité ont également des conséquences pour ceux qui vous ont confié des données personnelles. Ayez à l'esprit les conséquences pour les personnes de la perte, la divulgation, la modification non souhaitée de leurs données, et prenez les mesures nécessaires pour minimiser ces risques.

Sensibiliser les utilisateurs travaillant avec des données à caractère personnel :

Les informer des mesures prises pour traiter les risques et des conséquences potentielles en cas de manquement. Organiser une séance de sensibilisation, envoyer régulièrement les mises à jour des procédures pertinentes pour les fonctions des personnes, faire des rappels par messagerie électronique, etc.

Documenter les procédures d'exploitation, les tenir à jour et les rendre disponibles à tous les utilisateurs concernés. Concrètement, toute action sur un traitement de données à caractère personnel, qu'il s'agisse d'opérations d'administration ou de la simple utilisation d'une application, doit être expliquée dans un langage clair et adapté à chaque catégorie d'utilisateurs, dans des documents auxquels ces derniers peuvent se référer.

Rédiger une charte informatique et lui donner une force contraignante (ex. annexion au règlement intérieur).

Cette charte devrait au moins comporter les éléments suivants :

- Le rappel des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci.
- Le champ d'application de la charte, qui inclut notamment :
- Les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de l'organisme.
- Les moyens d'authentification utilisés par l'organisme.

Les règles de sécurité auxquelles les utilisateurs doivent se conformer, ce qui doit inclure de :

- Signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement.
- Ne jamais confier son identifiant/mot de passe à un tiers.
- Ne pas installer, copier, modifier, détruire des logiciels sans autorisation.
- Verrouiller son ordinateur dès que l'on quitte son poste de travail.
- Ne pas accéder, tenter d'accéder, ou supprimer des informations si cela ne relève pas des tâches incombant à l'utilisateur.
- Respecter les procédures préalablement définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité.

Les modalités d'utilisation des moyens informatiques/télécommunications mis à disposition comme :

- Le poste de travail.
- Les équipements nomades (notamment dans le cadre du télétravail).
- Les espaces de stockage individuel.
- Les réseaux locaux.

- Les conditions d'utilisation des dispositifs personnels.
- L'Internet.
- La messagerie électronique.
- La téléphonie.

Exemple

Vous êtes restaurateur et vous livrez à domicile. Vos clients vous communiquent leur adresse précise et le code d'entrée de leur immeuble. Si ces informations sont piratées ou perdues, elles peuvent être utilisées pour s'introduire frauduleusement au domicile de votre client.

Conséquence désastreuse pour **vos clients**, mais aussi **pour vous !**

Bonne pratique

Pour évaluer le niveau de sécurité des données personnelles dans votre entreprise, voici quelques questions à se poser :

- Les comptes utilisateurs internes et externes sont-ils protégés par des mots de passe d'une complexité suffisante ?
- Les accès aux locaux sont-ils sécurisés ?
- Des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?
- Avez-vous mis en place une procédure de sauvegarde et de récupération des données en cas d'incident ?

Signalez à la CNIL les violations de données personnelles

Votre entreprise a subi une violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou vous avez constaté un accès non autorisé à des données) ?

Vous devez **la signaler à la CNIL** dans les 72 heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Cette notification s'effectue en ligne sur le site internet de la CNIL.

Si ces risques sont élevés pour ces personnes, **vous devrez les en informer**.

À l'issue de cette étape, vous serez en capacité d'assurer une protection des données personnelles en continu et de faire face aux incidents.

Sous-traitants

Le RGPD reconnaît le rôle des sous-traitants dans le traitement de données personnelles, et leur impose des obligations particulières.

Qui est concerné ?

Le sous-traitant est la personne physique ou morale qui traite des données personnelles pour le compte d'une autre société ou d'un organisme (le « responsable de traitement »), dans le cadre d'un service ou d'une prestation.

Vous êtes concerné, en qualité de **responsable de traitement,** si vous choisissez de confier la gestion de vos données personnelles à des prestataires qui seront vos sous-traitants (exemple : SSII, intégrateurs de logiciels, hébergeurs de données, experts-comptables, toute entreprise qui dans le cadre de sa mission traite pour votre compte ou celui de vos clients des données personnelles).

Vous êtes concerné, **en qualité de sous-traitant,** si votre entreprise traite des données personnelles sur instruction et pour le compte d'une autre société ou organisme dans le cadre d'un service ou d'une prestation (exemple : vous effectuez des opérations de comptabilité, de prospection commerciale pour le compte de vos clients).

Que doivent faire les sous-traitants ?

Les sous-traitants sont tenus de respecter des **obligations spécifiques** en matière de sécurité, de confidentialité et de documentation de leur activité.

Ils doivent prendre en compte l'objectif de protection des données personnelles et de la vie privée dès la conception de leur service (principe du « *privacy by design* ») ou de leur produit, et ils doivent mettre en place des mesures permettant de garantir une protection optimale des données.

Les sous-traitants ont également une **obligation de conseil** auprès de leurs clients (exemple : insister auprès de ses clients pour les mises à jour de logiciel). Ils doivent les aider dans la mise en œuvre de certaines obligations du règlement (exemple : étude d'impact sur la vie privée, notification de violation de données, sécurité, etc.).

Les sous-traitants doivent enfin **tenir un registre des activités de traitement effectuées pour le compte de leurs clients** en complément de leurs propres traitements !

Pour déterminer les obligations respectives des responsables de traitements et de leurs sous-traitants, il est nécessaire de rédiger un contrat.

Ce contrat doit prévoir une clause spécifique sur la protection des données personnelles.

Bonne pratique

Vous pouvez prévoir et anticiper le recours à la médiation pour gérer un potentiel conflit.

Etes-vous concerné par les traitements de données à risques ou traitez-vous des données sensibles ?

Certaines données ou certains types de traitements nécessitent une vigilance particulière :

Lorsque vous traitez certains types de données à risque, sont notamment concernées les données dites « sensibles » :

- Révélant l'origine prétendument raciale ou ethnique.
- Portant sur les opinions politiques, philosophiques ou religieuses.

- Relatives à l'appartenance syndicale.
- Concernant la santé ou l'orientation sexuelle.
- Génétiques ou biométriques.
- Condamnations pénales ou infractions
- Numéro d'identification national unique

Les données d'infraction ou de condamnation pénale font également l'objet de règles particulières. Ces données ne peuvent être utilisées que sous certaines conditions strictement encadrées par la loi Informatique et libertés et par le RGPD.

PIA (analyse d'impact)

Lorsque votre traitement a pour objet ou pour effet :

- **L**'évaluation d'aspects personnels ou notation d'une personne (exemple : scoring financier).
- **U**ne prise de décision automatisée.
- **L**a surveillance systématique de personnes (exemple : télésurveillance).
- **L**e traitement de données sensibles (exemple : santé, biométrie, etc.).
- **L**e traitement de données concernant des personnes vulnérables (exemple : mineurs).
- **L**e traitement à grande échelle de données personnelles.
- **L**e croisement d'ensembles de données.
- **D**es usages innovants ou l'application de nouvelles technologies (exemple : objet connecté).
- **L**'exclusion du bénéfice d'un droit, d'un service ou contrat (exemple : liste noire).

Si vos traitements de données répondent à au moins 1 de ces 9 critères, vous devez, *a priori*, conduire une analyse d'impact sur la protection des données (**PIA** : Privacy Impact Assesment), avant de commencer les opérations de traitement.

Dans le cas ou vos traitements répondent à au moins 2 des 9 critères, l'analyse d'impact doit être réalisée de façon quasi systématique.

En complément de l'établissement du registre et de la description du traitement, cette analyse de l'impact sur la vie privée vous permettra d'identifier les risques associés à ces données personnelles. Il ne s'agit donc pas du même travail.

Lorsque vous transférez des données en dehors de l'Union européenne

Vérifiez si le pays hors Union européenne vers lequel vous transférez les données dispose d'une législation de protection des données et si elle est reconnue adéquate par la Commission européenne.
Une carte du monde présentant les législations de protection des données est à votre disposition sur le site de la CNIL.

Sinon, vous devrez encadrer juridiquement vos transferts pour assurer la protection des données à l'étranger.

Si votre situation correspond à l'un ou à plusieurs de ces points de vigilance, une analyse approfondie du RGPD et de la loi Informatique et Libertés est nécessaire pour déterminer les mesures à mettre en œuvre.

DPO (délégué à la protection des données)

Dans certains cas, vous pourrez être conduits à désigner un délégué à la protection des données.

Cette désignation est obligatoire pour certaines **entreprises opérant des traitements à grande échelle présentant des risques particuliers**.

Dans les autres cas, la désignation d'un délégué (DPO) est recommandée notamment si votre activité vous impose de mener une analyse approfondie du RGPD.

Le délégué peut être désigné en interne parmi vos collaborateurs ou en externe. Il peut aussi être mutualisé entre plusieurs organismes ou au sein d'associations ou fédérations professionnelles.

Si vos traitements de données sont susceptibles d'engendrer des risques spécifiques ou des problématiques nouvelles au regard de la protection des données, n'hésitez pas à vous informer auprès de la CNIL (modalités de contact sur la page « CONTACT » du site internet de la CNIL).

Par ailleurs, vos sous-traitants ont une obligation d'alerte et de conseil en matière de protection des données. N'hésitez-pas à les solliciter.

En résumé :

1 Ne collectez que les données vraiment nécessaires.

Posez-vous les bonnes questions : Quel est mon objectif ?
Quelles données sont indispensables pour atteindre cet objectif ? Ai-je le droit de collecter ces données ? Est-ce pertinent ? Les personnes concernées sont-elles d'accord ?

2 Soyez transparent.

Une information claire et complète constitue le socle du contrat de confiance qui vous lie avec les personnes dont vous traitez les données.

3 Pensez aux droits des personnes.

Vous devez répondre dans les meilleurs délais, aux demandes de consultation, de rectification ou de suppression des données.

4 Gardez la maîtrise de vos données.

Le partage et la circulation des données personnelles doivent être encadrées et contractualisées, afin de leur assurer une protection à tout moment.

5 Identifiez les risques.

Vous traitez énormément de données, ou bien des données sensibles ou avez des activités ayant des conséquences particulières pour les personnes, des mesures spécifiques peuvent s'appliquer.

6 Sécurisez vos données.

Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

Quel est le rôle de la CNIL ?

La Commission nationale de l'informatique et des libertés, (CNIL) est le régulateur français des données personnelles.

La CNIL informe et conseille les acteurs privés et publics dans la mise en œuvre de leur conformité en matière de protection des données personnelles.

Elle reçoit et traite les réclamations des personnes physiques. **Elle dispose des pouvoirs de contrôles sur place ou en ligne.**

Elle peut imposer à un acteur de régulariser son traitement **(mise en demeure)** ou **prononcer des sanctions (amende, etc.).**

Articles et informations divers

RGPD : des sanctions possibles pour TOUTES les entreprises, TPE/PME comprises.

D'une manière générale, ce sont les petites entreprises qui risquent de négliger le RGPD car elles ne se sentent pas vraiment concernées. Pourtant, comme les autres, les TPE/PME disposent de données, plus ou moins sensibles, se rapportant à des personnes physiques identifiées ou identifiables (ne serait-ce que celles de leurs salariés !). **Le RGPD concerne en effet les entreprises de toute taille**, localisées ou non en Europe, du moment qu'elles possèdent et traitent des données personnelles relatives à un citoyen européen…

Pour toutes, **le risque de sanction est bien réel** : si un de vos clients, prospects ou concurrents adresse une plainte à la CNIL, cette dernière aura l'obligation d'effectuer un contrôle. Cela peut donc arriver plus vite qu'on ne le croit ! Et les sanctions liées à une exploitation illégale des données seront sévères : les amendes prévues peuvent atteindre **4% du chiffre d'affaires annuel**.

Il est préférable de **se mettre en conformité le plus rapidement possible** ! Car au-delà de la sanction financière, une non-conformité peut tout de même vous nuire si une personne porte plainte …

Ne pas se mettre en conformité, c'est nuire à mon image.

Les répercussions d'une sanction publique auraient un impact extrêmement négatif sur **la confiance de vos clients, prospects et même de vos collaborateurs**… Mais même sans sanction, le simple fait de ne pas se mettre en conformité avec le RGPD, c'est prendre **un parti tranché**, qui pourrait entacher votre image. En effet, vos clients, partenaires et prospects risquent fort de **vous demander si vous êtes en conformité avec le RGPD, avant de collaborer avec vous**.

De même, si vous êtes fournisseur ou sous-traitant et que l'on vous demande de signer **les clauses « données personnelles » et « responsabilité » dans vos contrats** : vous serez bien embarrassé ! Et votre business en pâtirait sans aucun doute. Dommage, car en respectant le règlement sur les données personnelles, vous pourriez, au contraire, entrevoir de nouvelles opportunités...

Le RGPD peut être source de business supplémentaire.

Ceux qui ne se plieront pas aux règles imposées par le RGPD, **seront hors la loi**, mais en plus, ils passeront à côté d'une **belle opportunité de communication**. En effet, quitte à faire les efforts nécessaires pour se mettre en conformité avec la réglementation, autant que cela se sache !

Et pour cause, alors qu'il est souvent considéré comme une contrainte, le RGPD peut devenir **un véritable avantage concurrentiel**. Comment ? Tout simplement en mettant en avant vos démarches de mises en conformité dans votre communication. Un bon moyen de prendre l'avantage face à vos concurrents qui n'auraient pas encore entamé ces démarches ou qui n'auraient pas eu l'idée de communiquer dessus !

En conclusion, **les risques liés à une non-conformité avec le RGPD sont réels**. TPE, PME et grands groupes doivent tous commencer les démarches dès à présent pour respecter cette nouvelle loi et éviter de douloureuses conséquences.

La mise en conformité n'est pas seulement une contrainte

Certes, la mise en conformité permet d'éviter les sanctions de la CNIL qui sera plus sévère qu'auparavant. Jusqu'ici, si vous étiez loin de Paris et d'une ligne de TGV, ou dans des secteurs d'activité rarement contrôlés, les sanctions étaient plutôt rares. Mais la situation va changer et les contrôles vont se renforcer et se multiplier. Ceci étant, le RGPD est un règlement fort différent des lois françaises habituelles. **Il s'agit d'un règlement pragmatique où on ne demande pas aux entreprises d'être parfaites mais de s'améliorer tous les jours.**

RGPD : Comment gérer ses sous-traitants ?

Applicable à partir du 25 mai 2018 à l'ensemble de l'Union européenne, le règlement européen sur la protection des données (RGPD) responsabilise les responsables de traitement et sous-traitants qu'ils soient ou non établis au sein de l'Union européenne.

Le règlement impose désormais des obligations spécifiques aux sous-traitants dont la responsabilité peut être engagée.

Un organisme qui traite des données personnelles pour le compte d'un responsable de traitements est considéré comme un sous-traitant. Pour rappel, le responsable de traitements est celui « qui détermine les finalités et les moyens d'un traitement » (article 4). A noter que le présent article ne traite que des seuls sous-traitants, un régime distinct est applicable si le prestataire est responsable conjoint du traitement avec son client.

Les activités des sous-traitants peuvent être différentes avec des tâches précises ou plus générales.

Beaucoup de sous-traitants ne se considèrent pas impliqués dans la conformité au RGPD au seul titre qu'ils ne traitent pas de données pour leurs clients, ou n'y accèdent pas, notamment les prestataires de services informatiques, les éditeurs de logiciels ... Or le « traitement » a un sens extrêmement large puisqu'il constitue toute opération effectuée sur ou appliquée à une donnée ou un ensemble de données : collecte, transmission, stockage, modification, communication, enregistrement… (article 4).

Vos prestataires peuvent dans de nombreux cas, avoir accès aux données de leurs clients ou, sans avoir accès à leur contenu, les stocker, les héberger (hébergeur de bases de données clients, société d'archivage...). Ils doivent par conséquent se conformer au règlement.

Gérer la sous-traitance constitue aussi une des obligations imposées par le RGPD au responsable de traitement.

Celui-ci doit en effet, ne faire appel qu'à des sous-traitants présentant des garanties suffisantes en termes techniques et organisationnels (article 28.1)

Le sous-traitant lui-même ne peut faire appel à d'autres sous-traitants que s'il est autorisé au cas par cas, par le responsable de traitement, soit, si ce dernier a consenti une autorisation générale, que s'il a notifié au responsable un changement de sous-traitant, lui permettant de refuser le choix proposé (article 28.2).

Les relations avec le sous-traitant doivent impérativement être encadrées soit par un contrat, soit par un autre acte juridique imposant des obligations minimales au sous-traitant (28.3).

De notre expérience, la communication avec ces sous-traitants n'est pas toujours aisée face à la conformité du règlement : Déni, absence de réponses concrètes ....

La difficulté peut s'allonger si l'organisation a plusieurs prestataires, comme on peut le voir par exemple dans les activités de logistiques et des sous-traitants en cascades, et si le sous-traitant est situé en dehors de l'Union européenne.

Pour ce faire, nous préconisons une démarche en 5 phases :

1°) Dans un premier temps, cartographiez tous les sous-traitants auxquels fait appel l'organisation et identifiez s'ils traitent, ou ont accès à des données personnelles pour le compte de leur client ; dans l'affirmative, analyser leur rôle exact au regard des données traitées (sous-traitant, responsable conjoint).

Auditer de façon approfondie chaque sous-traitant n'est pas réellement envisageable, parfois seules 4 questions permettent d'avoir un ressenti sur la maturité du sous-traitant.

1-Existe-t-il dans l'entreprise un cadre de gouvernance sur la sécurité informatique ?
2-Une politique de sécurité informatique est-elle diffusée aux utilisateurs ?
3-Les utilisateurs sont-ils sensibilisés au nouveau règlement ?
4-Quel type de mesure de protection sont implémentées dans l'entreprise, sont-elles documentées ?

Avec ces premières questions vous êtes en capacité de faire une première évaluation du sous-traitant. De manière générale, les réponses aux questionnaires doivent vous permettre d'évaluer le niveau de risque associé à chaque sous-traitant. Un sous-traitant qui a des réponses négatives devra mener un projet global et un changement de culture d'entreprise, or sans volonté de la direction, il n'a que très peu de chance de satisfaire aux exigences dans le temps.

2°) Une fois le prestataire audité, il faudra négocier avec votre prestataire, au moyen soit d'un avenant, soit d'un accord séparé, des clauses adaptées au niveau de risque, reprenant les obligations minimales du RGPD (mesures de sécurité, gestion de la sous-traitance ultérieure, transfert de données hors de l'Union européenne, assistance du responsable de traitement, notification des violations de données personnelles, etc.).

3°) Pour la sélection des futurs sous-traitants, vous devrez définir un référentiel d'exigences tenant compte des obligations liées au RGPD et adapter votre documentation de consultation.

5°) Comment en pratique, imposer à un sous-traitant de réaliser sa mise en conformité quand vous n'avez pas la possibilité de remplacer le sous-traitant ou de remplacer un logiciel métier qui ne serait pas conforme ?

Vous serez en mesure de démontrer en cas de contrôle que vous avez entamé des diligences. Cependant si le fournisseur persiste, une réponse juridique adaptée devra être faite : outre le fait que le fournisseur se met en risque face à son client (manquement contractuel) il pourra être tenu responsable et sanctionné par la CNIL ou une autre autorité de contrôle compétente ; sachez que désormais vous avez également la possibilité, à compter du 25 mai prochain, de diligenter des audits de fournisseurs même en l'absence de clause contractuelle à ce titre.

Extraits de : Les Avocats (conseil national des barreaux)

Qu'est-ce qu'un sous-traitant ?

En vertu de l'article 4, al. 8, du RGPD, le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement ».
En pratique, il s'agit donc de la personne qui traite des données à caractère personnel pour le compte du cabinet d'avocats comme par exemple un comptable, un éditeur de logiciel, un hébergeur, etc.

Que faire en cas de sous-traitance ?

L'article 28, al. 3, du RGPD maintient l'obligation de souscrire un contrat liant le sous-traitant au responsable du traitement, tout en précisant ses contours et en fixant des exigences strictes et plus importantes. Ainsi, le contrat liant le cabinet au sous-traitant doit comporter :

- l'objet ;

- la durée ;
- la nature ;
- la finalité ;
- le type de données à caractère personnel ;
- les catégories de personnes concernées ;
- les droits et obligations du responsable de traitement ;
- les mesures de sécurité mises en œuvre concernant le traitement de données à caractère personnel qui sera réalisé.

L'acte juridique en question doit également définir les obligations du sous-traitant relatives à :

- la possibilité de ne traiter les données que sur instruction documentée du responsable du traitement, même en ce qui concerne les flux transfrontières ;
- la confidentialité des données ;
- l'exercice des droits des personnes concernées ;
- l'aide qu'il doit fournir au responsable de traitement par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, pour s'acquitter de l'obligation de donner suite aux demandes des personnes concernées ; l'aide fournie au responsable de traitement pour garantir le respect de ses obligations compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;
- la suppression des données concernées à l'issue du traitement, ou leur renvoi au responsable de traitement ou leur conservation s'il en est tenu par une disposition nationale ou européenne ;
- la mise à disposition du responsable du traitement de toutes les informations nécessaires pour démontrer le respect de ces obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;
- l'éventuel recrutement par le sous-traitant d'un sous-traitant ultérieur, d'un nouveau sous-traitant, et l'obtention de l'autorisation préalable écrite du responsable de traitement relative à ce recrutement qui doit être formalisé par un contrat mentionnant l'ensemble des obligations ci-dessus énumérées.

Les clauses contractuelles liant sous-traitants et responsables de traitement vont donc devoir être beaucoup plus précises tant sur les modalités de traitement que sur la gestion de leurs relations et l'échange d'informations entre eux.
En vertu de l'article 28, al.1, du RGPD, le responsable de traitement a l'obligation de ne recourir qu'à « des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée ».

L'avocat, lorsqu'il agit en qualité de responsable du traitement, a l'obligation, aux termes de l'article 28 du RGPD, de s'assurer que son prestataire informatique, en qualité de sous-traitant, a mis en place des mesures techniques et organisationnelles adaptées lui permettant de respecter la sécurité et la confidentialité des données. La conclusion d'un contrat est obligatoire entre l'avocat et ses sous-traitants et doit réserver une faculté d'audit pour permettre de vérifier la mise en œuvre conforme des mesures précitées.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Que faire avec les sous-traitants avec lesquels le cabinet est déjà en relation commerciale ?

Les cabinets d'avocats devront interroger leurs sous-traitants sur les garanties qu'ils ont mises en place afin de garantir leur conformité au RGPD.
Dans le cas où le cabinet d'avocats identifie des lacunes dans les mesures mises en place par le sous-traitant, ils devront conclure un avenant au contrat afin de combler lesdites lacunes.

Autorité de contrôle et sanctions

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du RGPD.

Les autorités de contrôle (en France, la CNIL) peuvent 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 nouveaux outils de conformité qui peuvent être utilisés par les entreprises, l'autorité peut retirer la certification délivrée ou ordonner à l'organisme de certification de retirer la certification.
S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de **2% jusqu'à 4% du chiffre d'affaires annuel mondial,** le montant le plus élevé étant retenu.
Ce montant doit être rapporté au fait que, pour les traitements transnationaux, la sanction sera conjointement adoptée entre l'ensemble des autorités concernées, donc potentiellement pour le territoire de toute l'Union européenne.
Dans ce cas, une seule et même décision de sanction décidée par plusieurs autorités de contrôle sera infligée à l'entreprise.