La protection des données personnelles

L'essentiel à connaître sur le GDPR / RGPD : définition, périmètre, principes et mesures

Le **GDPR** (ou **RGPD**) est le **nouveau règlement européen sur la protection des données**. Il entrera en application en 2018 et impactera toutes les entreprises opérant du traitement de données à caractère personnel sur des résidents européens.

Le GDPR poursuit plusieurs objectifs ambitieux :

- **Uniformiser** au niveau européen la réglementation sur la protection des données.
- **Responsabiliser** davantage les entreprises en développant l'auto-contrôle.
- **Renforcer le droit des personnes** (droit à l'accès, droit à l'oubli, droit à la portabilité, etc.).

En raison de l'importance du sujet, nous avons décidé de consacrer une série d'articles sur la RGPD. Dans le premier article de cette série, nous allons définir le GDPR (de quoi s'agit-il ?), préciser son périmètre (qui est concerné ?), sa date d'entrée en vigueur (quand ?) et les principaux changements qu'elle apporte par rapport à la loi Informatique et Libertés.

Cabinet de conseil en Relation Clients, en CRM et en Centre de Contacts, CustUp vous accompagne dans la compréhension du GDPR et de ses enjeux pour votre organisation.

Définition et périmètre du GDPR

Le GDPR (*General Data Protection Regulation*), aussi désignée sous son acronyme français RGPD (*Règlement général de protection des données*) est le **nouveau texte de référence en matière de protection des données au niveau européen**. Le règlement a été publié en mai 2016, après de longues années d'élaboration. La version finale du texte, qui fait plus de 88 pages, est accessible à cette adresse (en français).

Le GDPR entrera en vigueur le 25 mai 2018. Dans la mesure où il s'agit d'un **règlement européen**, et non pas d'une directive, le texte entrera en application directement et en même temps dans tous les Etats membres de l'Union européenne, sans transposition.

La RGPD, le règlement 679/2016, remplacera la directive 95/46/CE (publiée en 1995). Cette directive a servi, en France, de fondement à la loi Informatique & Libertés. Mais il est évident que depuis le milieu des années 1990, le paysage technologique et numérique a beaucoup évolué. La RGPD a été conçue pour **adapter et moderniser le cadre juridique** en matière de protection des données à ces évolutions.

Plus largement, la RGPD a pour ambition de « **redonner aux citoyens le contrôle de leurs données personnelles, tout en simplifiant l'environnement réglementaire des entreprises**« .

A l'heure où ces lignes sont rédigées, les entreprises disposent d'une petite année encore pour opérer leur mise en conformité GDPR.

Quelles sont les entreprises concernées par le GDPR ?

Les règles du GDPR s'appliqueront, à compter de mai 2018, **à toutes les entreprises privées ou publiques des 28 Etats membres** de l'Union européenne. Plus précisément, aux entreprises :

- Proposant des **biens et services** sur le marché de l'UE.
- **Collectant et traitant des données à caractère personnel sur les résidents de l'UE**.

A noter que le règlement s'appliquera également aux entreprises non implantées en UE, dès lors qu'elles collectent et traitent des données personnelles sur des résidents de l'UE.

Le périmètre d'application du GDPR

Les règles et obligations du GDPR s'appliquent au traitement – automatisé ou non – des données à caractère personnel. L'objectif du GDPR est de renforcer l'encadrement des pratiques en matière de collecte et d'utilisation des données à caractère personnel.

La RGPD donne une définition précise des « données à caractère personnel » (DCP) : il s'agit de « **toute information se rapportant à une personne physique identifiée ou identifiable** ». Par personne physique identifiable, il faut comprendre « une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Le GDPR concerne uniquement la protection des données personnelles rattachées à des personnes physiques. Ce qui signifie que la RGPD **ne s'applique pas aux entreprises** ne traitant que des données relatives à des personnes morales, sauf si celles-ci sont amenées à collecter des données sur des représentants des personnes morales (ce qui, dans les faits, est presque toujours le cas…).

Pour bien comprendre : la collecte de données sur des représentants d'une entreprise (à partir de cartes de visite par exemple) entre dans le champ d'application du GDPR. En revanche, la collecte d'informations sur l'entreprise (dénomination sociale, objet social, numéro de TVA, SIRET, etc.) en est exclue.

Le « traitement des données », au sens du GDPR, fait référence à la collecte, à l'accès, au stockage, à la manipulation, à la destruction et à la consultation à distance des données. Concrètement, une entreprise qui délègue à un prestataire la collecte et le stockage des données fait néanmoins du traitement de données dans la mesure où elle les consulte.

Au final, l'immense majorité des entreprises est concernée par les dispositions du GDPR.

Les 4 principes clés du GDPR et les mesures qui en découlent

Les dispositions du GDPR s'articulent autour de 4 principes clés : le consentement, le droit des personnes, la transparence et la responsabilité.

Le consentement

Le GDPR renforce la notion de consentement. A partir du 25 mai 2018, **le consentement des individus quant à la collecte et au traitement des données à caractère personnel les concernant devra être explicite et « positif »**. Ce consentement pourra être retiré à tout moment par les individus le demandant. Les entreprises faisant du traitement de données devront, par ailleurs, être en mesure de **prouver le recueil de ce consentement** le cas échéant (en cas de contrôle de la CNIL).

Une distinction doit être faite entre le B2B et le B2C concernant les règles du consentement relatif aux sollicitations email. **Pour les entreprises B2B**, la **collecte du consentement n'est pas obligatoire** si la finalité de la collecte est bien respectée. Dans ce cas, les cases pré-cochées sont autorisées. En revanche, le consentement est obligatoire (case à cocher) pour des sollicitations par des tiers (filiales, partenaires…).

Les entreprises B2B collectant de la donnée B2C devront veiller à bien séparer les modes de collecte suivant qu'il s'agit de données B2B ou de données B2C. Cela pourra par exemple se traduire par la mise en place de deux entrées différentes sur le site afin d'adapter les règles de consentement en fonction du type de clients (B2C/ B2B).

Le GDPR emporte aussi des conséquences dans le **mode de gestion des cookies**. La nouvelle réglementation impose la mention des informations suivantes : la **finalité** du cookie, le **droit d'opposition** de l'utilisateur et l'acceptation implicite de l'utilisateur si celui-ci décide de poursuivre sa navigation. Le **bandeau d'information** ne devra pas disparaître tant que l'utilisateur n'aura pas poursuivi sa navigation (en ouvrant une nouvelle page par exemple).

Autre conséquence : à compter de mai 2018, **aucun cookie ne pourra être déposé si l'utilisateur rebondit sur la page** – sauf les cookies nécessaires au bon fonctionnement du site. Cela devra être pris en compte dans les projets de DMP ou de mutualisation des données clients.

Toujours sur le thème du consentement, le GDPR prévoit une autre évolution majeure : **l'encadrement du profilage**. Le règlement n'interdit pas cette pratique, mais renforce son encadrement. Il impose notamment le recueil d'un consentement explicite de la part des personnes (case à cocher). Le profilage sera par ailleurs soumis à compter de mai 2018 au droit d'opposition.

La transparence

La transparence est le deuxième grand principe mis en avant par la RGPD. Il s'articule au consentement, dans la mesure où la transparence est la condition de possibilité d'un **consentement explicite et éclairé**.

Les entreprises devront – et ce dès la phase de collecte – fournir aux individus des informations claires et sans ambiguïté sur **la manière dont leurs données seront traitées**. Ces informations devront être fournies de façon concise, compréhensive et accessible par tous (par exemple, sur les formulaires de collecte, dans les documents contractuels, sur la page du site relative à la politique de « privacy », etc.).

Le droit des personnes

Un des principaux objectifs du GDPR est de renforcer les droits des personnes physiques. Les résidents européens se voient attribuer de nouveaux droits :

- **Un droit d'accès facilité pour tous les utilisateurs**. Le responsable du traitement devra faciliter l'exercice de ce droit, par la mise en place de process et d'outils adaptés. Si la collecte s'opère sur le site internet par exemple, une solution électronique devra être prévue, si possible avec un accès à distance sécurisé. En cas de demande d'accès de la part d'un utilisateur, l'entreprise disposera d'un délai d'un mois maximum pour la satisfaire.
- **Un droit l'oubli pour tous les utilisateurs**. L'apport majeur de la réglementation réside dans l'extension de conditions d'exercice de ce droit. Les entreprises disposeront d'un délai réduit d'un mois, et non plus de deux mois, pour supprimer les données à la suite d'une demande. Toutes les copies et toutes les reproduction des données devront aussi être effacées.
- **Un droit à la limitation du traitement**, applicable dans quelques cas précis.
- **Un droit à la portabilité des données**. Il s'agit d'un nouveau droit qui permet à une personne de récupérer les données qu'elle a fournies, sous une forme aisément réutilisable et, le cas échéant, de les transférer à un tiers (en cas de changement de fournisseur de services par exemple).

Il revient aux entreprises de garantir le droit des personnes par la **mise en place de mesures, d'outils et de process appropriés**. Ce qui nous amène au quatrième principe du GDPR : la responsabilité.

La responsabilité (accountability)

Le GDPR vise à responsabiliser davantage les entreprises dans leur traitement des données à caractère personnel. Cela se traduit par :

- **L'obligation faite aux entreprises de documenter toutes les mesures et procédures en matière de sécurité des DCP.** Les entreprises devront être en mesure de démontrer leur conformité avec la réglementation en cas de contrôle de la CNIL. Cette mesure se traduit par l'obligation de tenue d'un registre des traitements. Ce registre permettra de constituer une base de données des traitements, mais pourra aussi servir à centraliser et à suivre toutes les démarches de conformité mises en œuvre par l'entreprise.
- **Le renforcement des mesures de sécurité**. Les entreprises sont responsables de la sécurité des données qu'elles traitent et doivent mettre en place les mesures adéquates pour la garantir (pseudonymisation des données, analyses d'impact, tests d'intrusion…).
- **La mise en avant du principe de « Privacy By Design »**. Ce principe désigne toute la démarche visant à prendre toutes les mesures permettant de protéger les droits des personnes en amont (= dès la conception d'un produit ou d'un service) et tout au long du cycle de vie des données (de leur collecte à leur suppression).
- **L'encadrement des sous-traitants**. Les entreprises devront choisir des sous-traitants présentant des garanties suffisantes. En cas de faille de sécurité au niveau du sous-traitant, ce sera l'entreprise cliente (= le responsable des traitements) qui sera tenue pour responsable. En conséquence, les entreprises devront revoir les contrats signés avec les sous-traitants en intégrant des clauses concernant les DCP. Le GDPR instaure en fait un régime de co-responsabilité des sous-traitants.

- **La notification en cas de faille de sécurité** (data breach). Les entreprises auront pour obligation de mettre en place des actions en cas de violation de sécurité entraînant la destruction, la perte, l'altération ou la divulgation non autorisée de DCP. En cas de faille de sécurité, l'entreprise devra la notifier à l'autorité de régulation compétente (en France, la CNIL) dans un délai de 72h. Les personnes physiques concernées devront être informées « dans les meilleurs délais » si la faille ou la violation de données comporte un risque élevé pour les droits et libertés.
- **L'obligation de désignation d'un Data Protection Officer** (en français : « Délégué à la Protection des Données »). Doté d'un rôle très important, le DPO sera chargé de piloter la gouvernance des données, de contrôler la conformité de l'entreprise avec le GDPR et de conseiller le responsable des traitements. Cette obligation de désignation d'un DPO ne s'applique qu'aux entreprises réalisant des traitements **sur des données sensibles et/ou à grande échelle**.
- **La suppression de l'obligation de déclaration préalable à la CNIL**. Cette mesure traduit le principe qui gouverne le GDPR : responsabiliser les entreprises, en développant l'auto-contrôle.

Le GDPR opère de grands changements dans le paysage réglementaire relatif à la protection des données à caractère personnel. La conformité au GDPR sera demain la clé de réussite de la performance CRM. Dans un deuxième article, nous parlerons de l'impact de cette nouvelle réglementation sur les entreprises.

6 mots clefs pour comprendre le GDPR

Voici les définitions de quelques termes importants pour une bonne compréhension de le GDPR :

- **DPO – Data Protection Officer** : personne dont le rôle est de contrôler la conformité à la RGPD et de conseiller le responsable des traitements. Les entreprises traitant des données sensibles et/ou à grande échelle ont obligation de désigner un DPO.
- **DCP – Données à caractère personnel,** sensible : il s'agit, selon le GDPR, de « toute information se rapportant à une personne physique identifiée ou identifiable » : noms et prénoms, identifiants, numéros d'identification, téléphones, emails, données comportementales dès lors qu'elles peuvent être rattachées à un individu…
- **CNIL – Commission nationale de l'Informatique et des Libertés** : autorité de contrôle et de régulation française chargée de veiller à la bonne application par les acteurs économiques de la Loi Informatique et Libertés, et bientôt du GDPR.
- **Traitement des données** : désigne la collecte, l'accès, le stockage, la manipulation, la destruction et la consultation à distance des données. Le GDPR a une compréhension très large du traitement des données.
- **Profilage** : forme de traitement automatisé de DCP visant à évaluer certains aspects personnels relatifs à une personne physique (sa productivité au travail, son état de santé, etc.). La RGPD prévoit un encadrement renforcé de cette pratique.
- **Privacy by Design** : démarche consistant à prendre des mesures visant la protection des droits des personnes dès la phase de conception d'un produit ou d'un service. Démarche promue par le GDPR, liée au principe de responsabilisation des entreprises.