L'IMPACT DU RGPD SUR LES CGV ET LES CGU DES SITES INTERNET

Les objectifs du législateur européen exprimés à travers le Règlement Général pour la Protection des Données (RGPD) sont multiples. Il s'agit de créer un cadre renforcé et harmonisé de la protection des données tenant compte des récentes évolutions technologiques (Big Data, objets connectés, Intelligence Artificielle) et des nouveaux modes de consommations induits par le phénomène de « *plateformisation* » de l'économie de marché. L'individu est placé au cœur du dispositif légal et voit ainsi ses droits renforcés : consolidation des obligations d'information, clarification de l'acte de consentement, droit à la portabilité des données, droit à l'effacement... etc.

Aussi, dans le cadre de leur activité commerciale, les cybermarchands sont amenés à collecter, conserver et traiter nombre de données sur les utilisateurs de leur site ayant pour finalité la vente des produits ou la fourniture de services proposés sur le site : nom, adresse, mail, numéro de téléphone, données de paiement. A ce titre, ils endossent la qualité de responsable de traitement et devront d'ici le 25 mai 2018 respecter les obligations issues du Règlement général sur la protection des données personnelles (RGPD).

RETOUR SUR LES PRINCIPES CLÉS DU RGPD

Les devoirs et responsabilités de toute la chaîne d'acteurs ont évolué à l'aune du RGPD. Du responsable de traitement aux partenaires commerciaux, en passant par les sous-traitants fournisseurs de services chacun sera concerné. Les nouvelles obligations sont notamment issues des principes de « Privacy by Design »[1] et « d'accountability »[2]. L'accountability signifie que le responsable du traitement et le sous-traitant doivent mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. Le Privacy by Design implique une conformité ab initio afin que toutes les mesures techniques

Me Gérard HAAS

Me Rachel RUIMY

et organisationnelles soient mises en œuvre par le responsable du traitement et le sous-traitant dès le moment de la détermination des moyens du traitement puis au moment du traitement lui-même. A défaut, les exigences du Privacy by default s'appliqueront et le responsable du traitement devra mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir que seules sont traitées les données à caractère personnel nécessaires, au regard de chaque finalité spécifique du traitement.

Il en résulte que chaque cybermarchand devra se doter d'une politique de protection des données globale en s'assurant que le service qu'il s'apprête à lancer sur le marché et par le biais duquel il va collecter des données est conforme à la réglementation.

Dans cet objectif, le RGPD prescrit notamment la désignation d'un Délégué à la Protection des Données (DPO ou Data protection officer en anglais) pour tout responsable de traitement ou sous-traitant dont l'activité de base consiste en des opérations de traitement ou un suivi régulier et systématique à grand échelle des personnes concernées[3]. Chaque responsable de traitement devra donc faire du DPO l'allié central de leur politique de « data governance ». Afin d'atteindre ces objectifs, il conviendra de tenir un registre de l'ensemble des activités de traitement et de mener des études d'impact (PIA) régulières qui dans l'hypothèse d'un contrôle de la CNIL attesteront de la régularité des traitements.

Il s'agit de responsabiliser chaque maillon de la chaine d'acteurs et de l'obliger à s'engager dans une démarche globale vertueuse pour la vie privée de ses clients. Pour atteindre cet objectif et inciter les responsables de traitement à se conformer à la réglementation au plus vite, la CNIL dispose d'un panel de sanctions élevées.

UN ÉLARGISSEMENT DU CHAMP D'APPLICATION

On observe un net élargissement du champ d'application des règles en matière de protection des données, tout d'abord, au regard du nombre de personnes concernées puisque chaque citoyen européen aura la possibilité de se prévaloir des garanties offertes par le RGPD face aux entreprises qui collectent ses données[4]. Concernant le champ d'application territorial, la nouvelle réglementation sera opposable à n'importe quelle entreprise ou administration, sur le territoire européen ou en dehors, dès lors que les données traitées sont celles de citoyens européens[5].

En résulte un strict encadrement des transferts de données à caractère

1 - Article 25 du RGPD
2 - Article 5 du RGPD
3 - Articles 37 et suivants du RGPD
4 - Article 2 du RGPD
5 - Article 3 du RGPD

personnel vers les États tiers au Règlement[6]. Désormais, tout transfert de données personnelles hors de l'Union Européenne est prohibé sauf à ce qu'un État tiers au Règlement soit reconnu par la Commission européenne comme offrant un niveau de sécurité équivalent au niveau de sécurité requis. A défaut, un transfert demeure envisageable s'il est encadré par des règles internes d'entreprise (Binding Corporate Rules - BCR) ou par des clauses contractuelles types sur le modèle de celles édictées par la Commission, ou bien encore si des accords internationaux tel que le Privacy Shield pour les entreprises américaines le permettent.

L'INFORMATION DE LA PERSONNE CONCERNÉE

Le Règlement fait la part belle à l'information de l'utilisateur, condition sine qua non de l'exercice des droits qui lui sont conférés. Outre les informations quant aux finalités du traitement, à la durée de conservation des données, aux destinataires éventuels et aux transferts des données hors de l'Union européenne, la personne concernée devra être informée de son droit de retirer son consentement , des modalités d'exercice de ses droits, des finalités spécifiques du traitement (exécution d'un contrat, obligation légale ou réglementaire, intérêt légitime du responsable), des coordonnées du responsable de traitement et du délégué à la protection des données (DPD), de l'existence ou non d'une prise de décision automatisée fondée sur le traitement, et enfin de la possibilité qui s'offre à elle d'introduire une réclamation auprès de la CNIL[7].

LA MINIMISATION DES DONNÉES

La minimisation des données est un autre principe directeur du RGPD, au nom duquel les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Ce principe concerne la quantité de données à caractère personnel collectées, l'étendue de leur traitement, mais aussi leur durée de conservation et leur accessibilité. En vertu de ce principe, les données doivent n'être accessibles qu'aux personnes qui en ont strictement besoin en fonction de la finalité du traitement.

La responsabilisation des acteurs

La nouvelle politique des traitements repose sur deux piliers :

- La responsabilisation des acteurs du traitement
- La transparence

La directive du 23 novembre 1995 exigeait l'accomplissement de formalités préalables, désormais le RGPD repose sur un nouveau paradigme : la conformité. Les acteurs du traitement seront responsables des ajustements et mesures de consolidation à mettre en œuvre, sous le contrôle et avec l'accompagnement du régulateur. Le 25 mai 2018 nous passerons donc d'une logique plutôt verticale dans laquelle le responsable du traitement endossait une part quasi-totale du risque juridique, à une logique de responsabilité plus horizontale où les responsables de traitements et leurs sous-traitants sont placés sur un même pied d'égalité face à la règlementation et aux sanctions.

Néanmoins, les obligations déclaratives demeurent dès lors que les traitements concernés constituent un risque pour la vie privée des personnes. En outre, le régime d'autorisation pourra être maintenu par le droit national dans certains domaines, notamment en matière de données de santé, ou pourra être remplacé par une nouvelle procédure centrée sur la réalisation d'études d'impact sur la vie privée.

De nouveaux droits pour les utilisateurs

L'objectif principal de ce nouveau règlement est de renforcer les droits des personnes. Ce renforcement passe par la réaffirmation de droits anciens, mais aussi et surtout, par la consécration de nouveaux droits. Si la règlementation ancienne exigeait déjà le recueil d'un consentement explicite de la personne concernée reposant sur une information claire, intelligible et aisément accessible, désormais les acteurs du traitement devront garantir le respect de nouveaux droits : la portabilité des données[8] (déjà prévu dans le cadre des relations BtoC par la loi pour une République Numérique), le droit à l'effacement qui comprend le droit au déréférencement des données personnelles indexées par un moteur de recherche ainsi que le droit à l'effacement des données après une durée déterminée à l'avance par l'entreprise[9], le droit à la limitation du traitement[10] ou encore le droit d'opposition à la prise de décisions individuelles automatisées[11]. En vertu de ces nouveaux droits, les utilisateurs sont réputés avoir un contrôle global et efficient sur l'utilisation de leurs données. En outre, il incombera aux responsables de traitement d'apporter la preuve de la mise en œuvre de ces droits.

Les nouvelles obligations pour les (co)responsables de traitement et leurs sous-traitants : l'exemple de la marketplace[12]

L'activité d'une marketplace implique une relation commerciale entre trois principaux acteurs que sont l'opérateur de la plateforme, le vendeur, et l'acheteur.

L'opérateur de plateforme en ligne qui édite la marketplace définit les modalités et les finalités du traitement, raison pour laquelle il endosse la qualité de responsable de traitement. Ainsi, chaque opérateur de plateforme en ligne sera tenu au respect des différentes obligations prévues par le RGPD dans le cadre de la mise en relation entre les acheteurs et les vendeurs référencés sur la marketplace.

Dans le cadre de certains traitements tels que la vente et la livraison des produits, l'opérateur de la marketplace et chaque vendeur pourront être qualifiés de co-responsables de traitement lorsqu'ils déterminent ensemble les moyens (recueil des informations via la marketplace) et la finalité du traitement (vente et livraison des produits).

Dans le cadre de la gestion du flux financier, le Prestataire de Service de Paiement (PSP) pourrait être qualifié de sous-traitant lorsqu'il agit directement sur instructions de l'Opérateur de la plateforme et du vendeur dans le cadre de la gestion des flux financiers de chaque transaction. Néanmoins, cette qualification du PSP se détermine au cas par cas. En effet, le PSP pourrait

6 - Chapitre V du RGPD
7 - Article 13 et 14 du RGPD
8 - Article 20 du RGPD
9 - Article 17 du RGPD
10 - Article 18 du RGPD
11 - Article 22 du RGPD
12 - Pour télécharger notre livre blanc « RGPD et Marketplace » réalisé avec UFMD, vous pouvez cliquer ici : https://www.hoche-avocats.com/livre-blanc-rgpd-et-marketplaces/

également être qualifié de responsable de traitement (s'il mandate l'Opérateur pour gérer certains aspects du paiement et qu'il impose la procédure de KYC (*Know Your Costumer*) au vendeur), ou de co-responsable si le PSP détermine conjointement avec l'Opérateur et le vendeur les moyens et finalités du traitement de données lié au paiement.

IMPLICATIONS CONTRACTUELLES POUR LES CYBERMARCHANDS

Le RGPD renforce les obligations des responsables de traitement amenant nécessairement à sécuriser les relations juridiques unissant les éditeurs de sites ou opérateurs de plateformes à leurs prestataires sous-traitants ou à leurs clients. Cette sécurisation nécessitera de procéder à la consolidation juridique des contrats avec les sous-traitants, des contrats avec le prestataire de service de paiement, etc. Parmi ces contrats, figurent les conditions Générales de Vente (CGV) cœur du cadre juridique de la transaction et les conditions générales d'utilisation (CGU) document contractuel régissant les modalités d'interaction entre le fournisseur du service et ses clients utilisateurs.

La consolidation de vos CGV

Les apports du RGPD se répercutent sur l'ensemble des relations contractuelles et notamment dans le cadre du contrat régissant les transactions conclues sur un site internet : les Conditions Générales de Vente. Les CGV sont le contrat en ligne par lequel le professionnel propose sur sa plateforme digitale la vente de biens ou la fourniture de services. Elles peuvent régir tant les relations entre un professionnel et un consommateur (BtoC), que les rapports entre deux professionnels (BtoB). A cet égard, disposer d'un cadre juridique conforme permet de se prémunir contre d'éventuels litiges avec des clients ou de prévenir des contrôles toujours plus fréquents de la DGCCRF. Il s'agit, pour le cybermarchand, d'assurer une exploitation sereine de son activité retail tout en renforçant la confiance de ses clients, de ses partenaires et de ses prospects.

Dans le cadre d'une marketplace, les CGV sont le contrat qui régit les transactions entre les vendeurs et les acheteurs, auquel l'opérateur n'est pas partie. Ainsi, l'obligation préalable d'information reposera sur les seuls vendeurs. Néanmoins, en application de l'article L.111-7 du Code de la consommation, l'Opérateur a l'obligation de mettre à disposition des vendeurs un espace leur permettant de communiquer leurs CGV à leurs clients consommateurs. En outre, l'opérateur pourra proposer aux vendeurs référencés un « modèle » de CGV afin d'établir des exigences minimales communes, conformes à la législation en vigueur. Les CGV ont déjà fait l'objet de nombreux renforcement à l'aune des évolutions du droit de la consommation: Loi Hamon, Loi Macron, Loi pour une République Numérique et désormais le RGPD.

Désormais, en application du principe d'information préalable qui prévaut en droit de la consommation, les CGV devront indiquer les bases juridiques du traitement lorsque celui-ci est fondé sur les « *intérêts légitimes poursuivis par le responsable de traitement ou par un tiers* », c'est-à-dire lorsque le traitement n'est pas simplement fondé sur le consentement du titulaire des données, ni sur un contrat ou une obligation légale.

En outre, si un transfert en dehors du territoire de l'Union européenne est envisagé, la décision d'adéquation prise par la Commission européenne ou les garanties de protections appropriées (data agreement, clauses contractuelles types) devront être renseignées dans les CGV. Le cas échéant, devront également être renseignées les finalités de traitement envisagées et l'existence de prises de décisions automatisées telles que le profilage.

Enfin, le cybermarchand devra accorder le plus grand soin à renseigner les droits opposables par les consommateurs dont les données sont traitées tel que le droit à la limitation du traitement, le droit à l'effacement des données, le droit d'accès aux données, le droit d'accès et de modification ou encore à la portabilité des données. Le consommateur devra également être dument informé de son droit à introduire une réclamation auprès de l'autorité de contrôle à savoir la CNIL.

La consolidation des CGU

La loi pour une République numérique du 7 octobre 2016 a introduit à l'article L.111-7 du Code de la consommation, l'obligation pour tout opérateur de plateforme en ligne de délivrer une obligation claire, loyale et transparente sur « les conditions générales d'utilisation de sa plateforme », mais également sur les éléments suivants :

- Les modalités de référencement et de classement des contenus, des biens et des services.
- La qualité de l'annonceur et les droits et obligations des parties en matière civile et fiscale.
- En cas d'influence dudit classement et/ou référencement, l'existence d'une relation contractuelle, d'un lien capitalistique ou d'une rémunération à son profit.
- En cas d'activité dépassant un nombre de connexions de 5 millions de visiteurs uniques mensuel l'élaboration et la diffusion des « bonnes pratiques » (Article L.111-7-1 du Code de la consommation).
- En cas de collecte, de modération ou de diffusion d'avis en ligne, les informations relatives aux modalités de publication et de traitement des avis mis en ligne (date de l'avis, raisons justifiant la non-publication d'un avis...) tel que précisé par le décret du 29 septembre 2017[17]. (Article L.111-7-2 du Code de la consommation).

En outre, les CGU informent l'utilisateur quant au traitement des données personnelles et à l'utilisation qui en sera faite. Avec l'application du RGPD, les cybermarchands vont devoir principalement procéder à la consolidation des dispositions suivantes :

- La clause « données personnelles »
- La clause relative aux cookies et traceurs.

Il conviendra d'informer de manière claire et aisément accessible les utilisateurs du site sur les données collectées, les finalités pour lesquelles ces données sont collectées et le traitement qui en est fait. En toute hypothèse, l'utilisateur devra avoir explicitement consenti sur la base d'un acte positif univoque, au traitement de ses données : formulaire à compléter, case à cocher...etc. En outre, l'utilisateur devra être informé de moyens dont il dispose pour s'opposer au traitement de ses données.

Enfin, il conviendra pour le responsable de traitement de préciser ses instructions relatives aux traitements

17 - Décret n° 2017-1436 du 29 septembre 2017 relatif aux obligations d'information relatives aux avis en ligne de consommateurs ; Articles. D. 111-16 à D111-19 du Code de la consommation

des données en adéquation avec les informations renseignées dans les CGU.

LES SANCTIONS ENCOURUES EN CAS DE NON-RESPECT DU DEVOIR D'INFORMATION PRÉALABLE

Pour rappel, les CGV et CGU sont des dispositions contractuelles régies par le droit de la consommation et par le droit des contrats. Le cybermarchand ou l'opérateur pourra donc se voir appliquer les sanctions déjà prévues par le Code de la consommation, par le Code civil et par le Code de commerce, pour pratiques commerciales trompeuses ou pour manquement au devoir précontractuel d'information par exemple. Si le consentement est vicié, la nullité du contrat pourra être prononcée.

En outre, au regard du RGPD le défaut d'information de la personne concernée par le traitement sur les droits opposables au responsable de traitement est constitutif d'un manquement au droit des personnes faisant encourir une amende de la CNIL d'un montant pouvant désormais aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires.
Pour ce qui est des sanctions pénales, l'article R. 625-10 du code pénal prévoit une amende de 1500 euros par infraction constatée lorsqu'il est fait défaut à l'obligation d'information des personnes concernées par le traitement.

Enfin, les sanctions prononcées par la CNIL sous l'ère du RGPD seront rendues publiques. L'impact réputationnel n'est donc pas à négliger.

Le RGPD impose de nouvelles obligations aux responsables de traitements de données notamment en ce qui concerne l'information des utilisateurs concernant le recueil et les modalités de traitement de ses données à caractère personnel. Par conséquent, l'adaptation des conditions contractuelles, CGU et CGV est un enjeu fondamental de la mise en conformité des plateformes avec les nouvelles exigences de sécurisation juridique issues du RGPD. A ce titre, il conviendra de compléter vos clauses dédiées aux données personnelles avant le 25 mai 2018. Que vous opériez directement en BtoB, en BtoC, en CtoC ou que vous soyez opérateur de plateforme en ligne, la nouvelle règlementation impactera nécessairement vos relations contractuelles. A cet égard, le RGPD constitue une opportunité pour chaque plateforme de renforcer la confiance de ses clients et de ses prospects.

Me Gérard HAAS,
Associé fondateur du Cabinet HAAS Avocats
Auteur du livre « Le RGPD expliqué à mon Boss »

Me Rachel RUIMY
Responsable d'activité E-commerce du Cabinet HAAS Avocats

HAAS AVOCATS