RGPD : PREMIER COMPTE-RENDU

INTRODUCTION

Le traitement de données à caractère personnel est une nécessité et une obligation. En effet, le traitement de données vous permet, d'une part, d'assurer l'exécution de vos obligations contractuelles à l'égard de vos clients, et, d'autre part, d'améliorer et de proposer vos services ainsi que d'élaborer des stratégies de développement et de renforcer votre position sur le marché.

La matière connaît actuellement d'importantes évolutions législatives, particulièrement avec l'adoption du nouveau règlement européen sur la protection des données personnelles.

Ce règlement général sur la protection des données (ci-après le « RGPD ») poursuit deux objectifs principaux :

• d'une part, il renforce la protection des droits et libertés des personnes dont les données sont traitées ;

• d'autre part, il harmonise la matière et permet une meilleure circulation des données au sein de l'Union européenne.

Le RGPD sera obligatoire et applicable directement dans les Etats membres de l'Union à dater du 25 mai 2018. D'ici là, les autorités et les entreprises concernées doivent prendre toutes les mesures pour s'adapter et se conformer aux nouvelles exigences légales.

« Traitement » des « données à caractère personnel »

Une « donnée à caractère personnel » est toute information à partir de laquelle une personne physique peut être identifiée (ou identifiable), directement ou indirectement. Il s'agit d'un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale d'une personne, tels que, par exemple, un identifiant en ligne, un nom, une adresse postale, une adresse email, un numéro de téléphone, etc.

Il existe également ce que l'on appelle les « données sensibles », qui visent les données révélant, par exemple, les opinions politiques, les convictions religieuse et philosophique, l'origine raciale ou ethnique, l'appartenance à un syndicat, la vie sexuelle ou l'orientation sexuelle, les informations médicales ou encore les données biométriques (empreintes digitales, photographie).

Vous effectuez un « traitement de données » lorsque vous appliquez à des données personnelles une ou plusieurs des opérations suivantes (peu importe le procédé utilisé) : la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication ou la mise à disposition, la limitation ou encore l'effacement.

Le « responsable du traitement » est la personne qui détermine – seul ou conjointement avec d'autres – les finalités (c.-à-d. les objectifs poursuivis) et les moyens du traitement de données (c.-à-d. les méthodes de collecte et de traitement).

Il peut s'agir d'une personne physique (p. ex. un médecin), d'une personne morale (p. ex. une entreprise), d'une association (p. ex. une ASBL) ou même d'une administration publique (p. ex. une mairie ou une commune).

L'identification du (des) responsable(s) du traitement est essentielle. En effet, en tant que « responsable du traitement », vous êtes soumis à la réglementation en matière de protection des données. Vous êtes donc directement concerné par le nouveau règlement général sur la protection des données !

Pour être conforme à la réglementation, un traitement de données à caractère personnel doit répondre à certaines conditions strictes. Ainsi, les données à caractère personnel devront être :

• traitées de manière licite, loyale et transparente ;

• collectées pour des finalités déterminées, légitimes et explicites ;

• adéquates, pertinentes et nécessaires au regard des finalités poursuivies ;

• exactes, et le cas échéant, mises à jour ;

• conservées sous une forme qui permette l'identification de la personne concernée pendant une durée limitée, soit uniquement pendant la durée nécessaire à la réalisation des finalités du traitement.

Ainsi, une entreprise peut conserver les données de ses clients pendant la durée de leur contrat, à condition toutefois que la conservation de ces données soit réellement nécessaire à l'exécution du contrat. Le délai de conservation doit être raisonnable au regard des objectifs poursuivis, en fonction des circonstances et de la nature des données. Il s'agit d'une appréciation au cas par cas. Par exemple, les coordonnées d'un prospect qui ne réagit à aucune sollicitation durant trois années doivent être supprimées. Autre exemple : les images captées dans le cadre d'un dispositif de vidéosurveillance ne pourront être conservées plus d'un mois ;

• collectées et traitées de manière à garantir leur sécurité.

Devoir d'information

Le RGPD renforce le principe de transparence et le devoir d'information à l'égard des personnes dont les données sont collectées et traitées.

En tant que responsable du traitement, vous devez impérativement transmettre à ces personnes une information claire, précise, intelligible et accessible, portant notamment sur les modalités et les finalités du traitement ainsi que sur leurs droits et possibilités de recours.

Vous veillerez donc à insérer toutes ces informations dans votre Charte Vie Privée, laquelle doit par ailleurs être facilement accessible à tout moment.

Enfin, toute personne doit être en mesure de vous contacter, de manière effective, pour toute question et/ou réclamation (par courrier postal ou par email). Il s'agit d'une obligation légale.

Prenons l'exemple d'une campagne type jeux-concours que vous organisez sur votre Page Facebook ou sur un mini site. Les futurs participants sont généralement invités à s'enregistrer en ligne ou à remplir un formulaire de participation, contenant des données à caractère personnel que vous allez ensuite récolter et traiter. Dans ce contexte, vous effectuez un traitement de données à caractère personnel et vous êtes dès lors tenus de respecter le RGPD. Vous devez donc :

1. insérer une clause « protection des données personnelles et vie privée » dans le règlement du jeu concours, lequel doit être aisément accessible (notamment sur votre Page Facebook ou sur le site) ;

2. vous munir d'une Charte Vie Privée, qui doit également être aisément accessible à tout moment.

Lorsque le traitement repose sur le consentement de la personne, celle-ci doit l'avoir donné par un acte positif clair et explicite.

À l'avenir, la personne concernée doit manifester son accord au traitement des données la concernant de façon libre, spécifique, éclairé et univoque. Celle-ci doit donner son consentement de manière active. Il ne sera dès lors plus possible d'obtenir le consentement de la personne par la technique du pré-cochage d'option sur un site web ou même par son silence. Celle-ci devra, par exemple, cocher une case lors de la visite sur votre site web, ou effectuer une déclaration indiquant clairement l'acceptation d'un traitement déterminé.

Une acceptation implicite ou passive, même circonstanciée, n'est donc plus admise. En d'autres termes, si la personne n'a pas dit « oui », ce sera « non ».

Exceptions

Avons-nous toujours besoin du consentement du client ? Dois-je lui demander explicitement si je peux utiliser ses données pour lui envoyer une facture concernant les services qu'il m'a commandés ? Non, il existe heureusement des exceptions logiques. Sur ce plan, le RGPD n'a rien inventé : ces exceptions figurent déjà dans la législation actuelle en la matière.

Obligation contractuelle

La principale exception est sans doute que l'autorisation n'est pas requise lorsque le traitement est nécessaire à l'exécution d'une convention à laquelle la personne concernée est partie.

Si un client vous achète des services, cela fait naître une relation contractuelle. Vous fournissez le service, et le client vous rétribue pour votre prestation. Pour obtenir cette rétribution, il faut que le client puisse vous payer. Cela passe par l'envoi d'une facture (sur papier ou électronique) portant diverses informations nécessaires. Lorsque vous traitez les données du client pour établir et envoyer la facture, vous le faites pour exécuter le contrat passé avec le client. Dans un tel cas, vous n'avez pas besoin du consentement du client.

Si vous collaborez avec un réseau de revendeurs, vous conservez probablement les coordonnées d'un grand nombre de personnes travaillant chez ces revendeurs. Quand vous devez contacter ces personnes pour régler des questions pratiques, en principe, vous n'avez pas besoin d'autorisation de traitement, à condition que celui-ci s'inscrive dans la mise en œuvre de votre collaboration.

Obligation légale

Une autre exception concerne l'existence d'une obligation légale imposant le traitement.

Encore un exemple : vous collectez une foule d'informations de vos salariés, vous les enregistrez dans un fichier, et vous transmettez celui-ci à votre secrétariat social. Vous faut-il pour cela un consentement explicite ? Non, car votre secrétariat social a besoin des données pour calculer les salaires et payer vos employés. Les secrétariats sociaux doivent aussi transmettre des copies des documents salariaux aux autorités. Le fisc est parfaitement au courant de ce que vous gagnez. Vous vous en êtes déjà aperçu si vous utilisez Tax-on-Web. Dans cet exemple, il est clairement question d'une obligation légale à respecter, l'équivalent du consentement de la personne concernée.

Autres exceptions

Il reste 3 autres exceptions. Passons-les brièvement en revue :

- Le traitement est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- Le traitement est nécessaire pour accomplir une tâche d'intérêt général ;
- Le traitement est nécessaire pour défendre les intérêts légitimes du responsable de traitement ou d'un tiers.

Ces 3 dernières exceptions sont beaucoup plus vagues. Il est certain qu'elles vont susciter à l'avenir quelques frictions. Qu'est-ce qu'un intérêt légitime ? Puis-je conserver toutes les données transactionnelles de mes clients sous prétexte qu'on pourrait un jour me les demander dans le cadre d'une enquête judiciaire ?

Enfin, la personne doit pouvoir retirer son consentement à tout moment et aussi facilement qu'il a été donné. Néanmoins, rassurez-vous, ce retrait n'a aucune influence sur la licéité du traitement fondé sur le consentement effectué avant ce retrait. Ainsi, le retrait du consentement ne vaut que pour l'avenir.

En tant que responsable du traitement, vous devrez pouvoir démontrer à tout moment que la personne concernée a donné son consentement au traitement de ses données à caractère personnel. La preuve du consentement doit porter sur trois éléments : l'identité de la personne qui a consenti, le moment où elle a donné son consentement, et enfin l'objet du consentement (ce à quoi la personne a consenti).

Qu'implique le RGPD en ce qui concerne l'email marketing ?

L'Email Marketing sous le RGPD, signifie principalement, le consentement que vous collectez devra être donné de façon libre, spécifique, éclairée et univoque (Article 4). Afin de se conformer au RGPD, vous devez adopter de nouvelles pratiques :

1. Nouvelles règles de consentement (opt-in) des consommateurs;
2. Système de stockage des preuves de consentement; et
3. Une méthode par laquelle les consommateurs peuvent demander à leurs données d'être supprimées et/ou modifiées.

Concernant l'impact du RGPD (EU GDPR) sur le B2B et le B2C en 2018, la nouvelle réglementation Européenne s'applique aux deux modèles d'achat. Ni le soft opt-in ni le soft opt-out ne sont permis; nous vous recommandons d'utiliser le double opt-in afin de respecter les exigences du RGPD.

Qu'est-ce-que la procédure double opt-in ?

Elle consiste à demander une double confirmation à chaque internaute pour recevoir vos campagnes d'email marketing.

Comment écrire une demande de consentement de manière claire et concise ?

La demande de consentement doit être facilement compréhensible pour tout individu. Toute technique de déstabilisation, comme pré-cocher la case d'opt-in ou avoir recours à une formulation trop vague ou prêtant à confusion (emploi de double négation ou incohérences) sera refusée par le RGPD.

Voici un exemple de message clair et concis :

"Vous acceptez que [nom de votre organisation] collecte et utilise les données personnelles que vous venez de renseigner dans ce formulaire dans le but de vous envoyer des offres marketing personnalisées que vous avez acceptées de recevoir, en accord avec notre politique de protection des données [lien de votre politique]. Veuillez cocher les cases ci-dessous si vous acceptez de recevoir : [cases appropriées]."

Comment envoyer des emails marketing en conformité avec le RGPD ?

a – Effectuez un audit de votre base de données actuelle.

- Savez-vous où vos contacts se situent géographiquement ?
- Gardez-vous des preuves de leur consentement ?

b – Connaissez vos contacts et la manière dont vous les avez collectés.

- Gardez-vous une trace de la provenance de vos contacts ?
- Comment sont-ils arrivés dans votre base de données ?
- Détenez vous des preuves suffisantes, c'est-à-dire jugées valables devant un tribunal, du consentement de chacun de vos utilisateurs et la raison précise pour laquelle ces derniers ont donné leur consentement ?
- Avez-vous toujours eu recours à une procédure en double opt-in ?

c – Vérifiez et rendez publiques vos pratiques de collectes et d'usage de données.

- Vos pratiques sont-elles transparentes et facile à comprendre pour vos utilisateurs ?
- Votre politique de confidentialité (ou autre documentation en ligne) détaille-t-elle comment vous collectez, stockez, transférez et utilisez vos données de manière claire et concise ?
- Demandez-vous l'autorisation de vos utilisateurs pour collecter leurs données ?

d – Assurez-vous que tous vos futurs projets sont conformes au RGPD.

- Toute nouvelle initiative devrait prendre en compte ces futures exigences de conformité, afin que vous n'ayez pas à revenir rétroactivement sur ces projets pour ajuster vos procédés.

Est-ce que je peux continuer à envoyer mes campagnes d'email marketing à ma liste de contacts existante ?

Le RGPD ne s'applique pas seulement aux données collectées après son applicabilité, le 25 mai 2018, mais également aux données collectées avant. Est-ce que les enregistrements de consentement de vos contacts prouvent que vous avez l'autorisation claire de leur envoyer des campagnes d'email marketing ? Tout enregistrement ambigu impliquerait l'obtention d'une autorisation nouvelle et expresse de la part de ces contacts, afin de pouvoir envoyer de nouveau des campagnes d'email marketing.

Le désabonnement sous le RGPD ?

Tous les spécialistes de l'email marketing doivent veiller à ce que leurs contacts disposent d'un moyen approprié pour se désabonner, afin d'être conforme au RGPD. Le processus de désabonnement sous GDPR doit être clair et simple. Il est nécessaire d'inclure un lien de désabonnement visible dans chaque email marketing où votre abonné peut :

1. Se désabonner de cette communication marketing
2. Se désabonner de toutes vos communications
3. Contacter une adresse email de retour

Permettre à vos contacts de s'abonner et de se désabonner facilement sont tout aussi important pour assurer le respect du RGPD.

Droits des personnes concernées….

Toute personne dont les données sont traitées dispose, notamment, des droits suivants :

1. Un droit d'accès : la personne a le droit de recevoir, de manière compréhensible, une copie de ses données collectées et traitées.

2. Un droit de rectification : la personne peut, sans frais, faire rectifier ses données qui seraient inexactes, incomplètes ou non pertinentes.

3. Un droit d'opposition : la personne a le droit de s'opposer à ce que ses données la concernant fassent l'objet d'un traitement, et ce pour des motifs sérieux et légitimes. Le droit d'opposition n'est pas possible si le traitement de données est nécessaire à la conclusion ou à l'exécution d'un contrat. Attention toutefois, la personne peut s'opposer au traitement de ses données personnelles sans aucune justification lorsque les données sont collectées à des fins de marketing direct (c.-à.-d. à des fins publicitaires).

La personne concernée a également le droit à l'effacement (ou « droit à l'oubli »), soit le droit à l'effacement de ses données à caractère personnel, dans certaines hypothèses énumérées par la loi. Ainsi, la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de ses données à caractère personnel, notamment dans les cas suivants :

• Les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

• La personne concernée a retiré son consentement sur lequel est fondé le traitement, et il n'existe pas d'autre fondement juridique au traitement ;

• La personne concernée fait valoir son droit d'opposition et il n'existe pas de motif légitime impérieux justifiant le traitement, ou la personne s'oppose spécifiquement au traitement de ses données à des fins de marketing direct ;

• Les données personnelles ont fait l'objet d'un traitement illicite ;

• Les données doivent être effacées conformément à une obligation légale découlant du droit de l'Etat membre auquel le responsable est soumis ou du droit de l'Union européenne.

Toutefois, le droit à l'effacement n'est pas absolu. En effet, le RGPD prévoit une série de cas dans lesquels le droit à l'effacement ne s'applique pas. Le traitement de données pourra, par exemple, être maintenu lorsqu'il s'avère nécessaire à l'exercice du droit à la liberté d'expression et d'information, ou à la constatation, à l'exercice ou à la défense de droits en justice.

Enfin, le RGPD instaure notamment un nouveau droit, celui de la « portabilité des données ». Ce dernier implique le droit pour toute personne concernée d'obtenir du responsable du traitement une copie de ses données personnelles traitées, et le cas échéant, le transfert de ces données à un tiers.

Pour exercer ces droits, la personne concernée doit adresser sa demande au responsable du traitement en faisant la preuve de son identité (par exemple, en communiquant une copie de sa carte d'identité ou de son passeport).

Quid des sous-traitants…

Le principe de base est que la majorité des responsabilités et obligations reposent toujours sur le responsable du traitement. Celui-ci doit être en mesure de prouver– à tout moment – qu'il respecte bien la réglementation, par exemple en démontrant les mesures techniques et organisationnelles prises afin d'assurer la sécurité des données.

Le RGPD instaure des règles de partage des responsabilités entre le responsable du traitement et le(s) sous-traitant(s).

Il faut savoir que le responsable du traitement ne doit pas nécessairement effectuer lui-même le traitement de données à caractère personnel. Le responsable du traitement peut, en effet, faire appel à un sous-traitant, qui - mandaté par lui - effectuera concrètement le traitement. Le sous-traitant est donc la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Ainsi, le sous-traitant agit toujours conformément aux instructions du responsable du traitement.

C'est pourquoi, le RGPD prévoit l'obligation pour le responsable du traitement et le sous-traitant de régler contractuellement, par écrit, les modalités d'exécution et d'organisation du traitement des données confié à ce dernier.

Ce contrat doit reprendre certaines informations obligatoires (finalité, catégorie de données, objet et durée du traitement, missions et devoirs du sous-traitant à l'égard du responsable, etc.). En tout état de cause, le sous-traitant devra respecter certaines obligations légales, à savoir qu'il doit garantir la confidentialité des données qu'il reçoit du responsable, qu'il ne peut pas en principe faire de copie de ces données, qu'il doit prévoir des mesures techniques et administratives appropriées pour protéger ces données personnelles. Par conséquent, le RGPD prévoit que le sous-traitant peut engager sa responsabilité en cas de non-respect du RGPD et/ou s'il n'a pas agi conformément aux instructions (conformes à la loi) du responsable du traitement.

Le registre…

En raison d'une charge administrative trop importante, la notification préalable à la Commission de la protection de la vie privée est appelée à disparaître, au profit d'une nouvelle obligation dans le chef de certaines entreprises : celle de tenir un registre des activités de traitement de données mis en œuvre par l'entreprise. Ne sont pas concernées par cette obligation les entreprises comptant moins de 250 travailleurs. Attention toutefois, la loi prévoit des cas dans lesquels cette obligation leur est applicable, par exemple lorsque l'entreprise traite des données sensibles.

Le registre doit contenir certaines informations détaillées sur le traitement (catégories de données collectées et traitées, méthode de collecte, finalités du traitement, personnes concernées par le traitement, description des mesures de sécurité, lieu du traitement, etc.). En pratique, le registre doit se présenter sous une forme écrite (y compris une forme électronique) ou sous une autre forme non lisible pouvant être convertie en forme lisible.

Plus de détails :

En principe, l'obligation de tenir un registre des traitements **concerne tous les responsables de traitement** (le cas échéant leurs représentants) et leurs sous-traitants. Néanmoins, le règlement prévoit une **exemption, qui reste en pratique très limitée**. Les entreprises ou organisations comptant moins de 250 employés ne sont pas contraintes de tenir ce registre, sauf dans les cas suivants :

- le traitement est **non occasionnel**, c'est-à-dire qu'il est habituel. Ainsi, selon les récentes recommandations de la CPVP, sont considérés comme « habituels » les traitements de données entourant la gestion de la clientèle, la gestion des fournisseurs ou encore la gestion du personnel (ressources humaines) ; ou
- le traitement est **susceptible de comporter un risque** pour les droits et libertés des personnes dont les données sont traitées ; ou
- le traitement porte sur des **données dites « sensibles »** (telles que des données médicales, relatives à l'orientation sexuelle, aux convictions religieuses, philosophiques, politiques, etc.) ; ou
- le traitement porte sur des **données judiciaires** (ex. condamnations pénales).

Dans la **grande majorité des cas**, la tenue d'un registre des traitements s'avère **obligatoire**. En tout état de cause, sa mise en place est **vivement recommandée** tant le registre s'avère utile dans le cadre de la mise en conformité et du suivi du respect des obligations légales.

Que faut-il indiquer dans le registre des traitements ?

Les informations à indiquer dans le registre varient selon que vous agissez en qualité de « responsable du traitement » ou en qualité de « sous-traitant ».

Si vous êtes « (co-)responsable du traitement », le registre doit recenser, au moins, les informations suivantes :

- votre nom et vos coordonnées ainsi que ceux du délégué à la protection des données (DPO) ;
- une description des finalités du traitement, c'est-à-dire les buts pour lesquels les données sont traitées (ex : gestion de la clientèle, gestion du personnel, etc.) ;
- une description des catégories de données traitées (par exemple, données d'identification, données financières, données de géolocalisation, etc.)
- une description des catégories de personnes dont les données sont traitées (ex : clients, visiteurs du site web, prospects, employés, prestataires, mineurs d'âge, etc.) ;
- les destinataires auxquels les données ont été ou seront communiquées (y compris les destinataires situés dans des pays tiers à l'UE) ;
- les éventuels transferts des données vers un pays tiers ainsi que la documentation attestant de l'existence de garanties appropriées entourant chaque transfert ;
- le délai de conservation pour chaque catégorie de données ;
- une description générale des mesures de sécurité techniques et organisationnelles.

Si vous êtes « sous-traitant », le registre devra comporter, au moins, les informations suivantes :

- votre nom et vos coordonnées ainsi que ceux du responsable du traitement pour le compte duquel vous agissez ainsi que, le cas échéant, les coordonnées du délégué à la protection des données (DPO) ;
- les catégories de traitement effectués pour le compte du responsable ;
- les éventuels transferts de données vers un pays tiers et les documents qui attestent de l'existence de garanties appropriées ;
- une description générale des mesures de sécurité techniques et organisationnelles.

Il s'agit des informations minimales à mentionner. Il est donc tout à fait possible d'indiquer d'autres éléments (tels que le fondement légal, le résultat de l'analyse d'impact (si nécessaire), etc.).

En pratique, comment tenir le registre ?

En l'état actuel, il n'existe **aucun modèle type obligatoire**. Vous êtes donc libre de choisir la forme de votre registre. Néanmoins, celui-ci doit se présenter sous la **forme écrite**, y compris sous une **forme électronique**. Il doit être clair, compréhensible et lisible.

Que risquez-vous si vous ne tenez pas (correctement) le registre des traitements ?

Outre ses prérogatives en tant qu'autorité de contrôle (émettre un avertissement, limiter de manière temporaire ou permanente le traitement, retirer une certification, etc.), celle-ci peut vous condamner au paiement d'une **amende administrative pouvant aller jusqu'à 10.000.000,00€** ou jusqu'à 2% du chiffre d'affaires annuel mondial.

<u>Le Délégué à la protection des données…</u>

Dans certaines circonstances, un délégué à la protection des données devra être désigné au sein de l'entreprise. Il peut être interne ou externe à l'organisme qui le désigne. Le délégué est principalement chargé :

• de contrôler le respect par l'entreprise de la réglementation ;

• de conseiller et d'informer l'entreprise (et ses employés) et les éventuels sous-traitants ;

• d'être le point de contact avec l'autorité de contrôle (par exemple la Commission belge de la vie privée).

Le délégué devra disposer de qualités professionnelles et de connaissances spécifiques dans le domaine du droit et des pratiques en matière de protection des données. Il devra par ailleurs exercer ses fonctions et missions en toute indépendance, qu'il soit employé ou non du responsable du traitement.

La désignation d'un délégué est notamment obligatoire lorsque les activités de base du responsable du traitement consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique des personnes dont les données sont collectées et traitées.

En dehors des cas de désignation obligatoire, le responsable du traitement dispose de la faculté de désigner un délégué à la protection des données (qui peut être interne ou externe à l'entreprise).

Sécurisation…

Le RGPD renforce le principe de sécurisation des données. Les données à caractère personnel devront être traitées de manière à assurer la sécurité et la confidentialité des données. C'est pourquoi, vous devrez prendre toutes les mesures techniques et organisationnelles raisonnables afin d'assurer la sécurité des données ; le but étant d'éviter à tout prix les fuites, les divulgations non autorisées et les vols de données.

Lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnelles concernées, vous devrez effectuer au préalable une analyse d'impact complète afin d'évaluer et de mesurer les risques liés à la sécurité des données. Le but est d'évaluer la nature, la portée, le contexte et la gravité des risques pour les droits et libertés des personnes concernées et de prévoir ensuite des mesures concrètes pour réduire et atténuer ces risques. Selon le RGPD, l'analyse d'impact est notamment requise pour les traitements à grande échelle de données sensibles ou en cas de surveillance systématique à grande échelle d'une zone accessible au public. Les autorités de contrôle vont, en outre, établir et publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact est requise.

Le RGPD impose désormais à tout responsable du traitement de notifier à l'autorité de contrôle national, les brèches de sécurité, c'est-à-dire toute violation des données à caractère personnel (vol, fuite, accès ou divulgation non autorisé(e), destruction des données, etc.).

En cas de brèche de sécurité susceptible d'engendrer un risque pour les droits et libertés des personnes concernées par la violation des données, le responsable du traitement devra la notifier à l'organe de contrôle national dans les meilleurs délais et, à tout le moins, dans un délai de 72 heures à partir de la prise de connaissance de cette violation. Le sous-traitant, quant à lui, doit informer le responsable du traitement de toute violation des données dans les meilleurs délais après en avoir pris connaissance.

Il s'agira principalement pour le responsable du traitement d'indiquer dans la notification quelles sont les données touchées, la quantité de données dont il est question ainsi que les conséquences que peut avoir la violation de données pour les personnes concernées. En outre, le responsable du traitement devra indiquer les mesures prises, avant et après la violation des données.

En pratique, l'appréciation par le responsable du traitement de la présence ou de l'absence de risques pour les droits et libertés des personnes concernées s'avère délicate.

Sanctions…

Les entreprises qui ne respectent pas la nouvelle réglementation pourront être condamnées par l'autorité de contrôle à d'importantes amendes, dont le montant peut s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial annuel de l'entreprise..