WilhelmGilliéron
AVOCATS

Auteur: Wilhelm Gilliéron Avocats | Le : 3 mai 2021

La nouvelle loi fédérale sur la protection des données : s'en préoccuper, oui ! Paniquer, non !

« *Que faites-vous de mes données ?* », « *Pourquoi me demandez-vous mon numéro de téléphone ?* », « *Suis-je obligé de remplir une fiche client ? Dois-je vous communiquer toutes ces indications ?* ». Toutes ces questions, auxquelles bien des commerçants doivent aujourd'hui faire face, ne se posaient pas il y a encore quelques années.

A l'ère du tout numérique, **difficile en effet d'échapper à la sensibilisation qui existe autour de la protection des données, renforcée par l'intérêt des médias à faire état du moindre incident**. L'accélération de la numérisation comme résultat de la pandémie n'a fait que renforcer cette attention.

Bien souvent qualifiée d' « *usine à gaz* », on ne saurait cependant dénier à la protection des données un rôle protecteur fondamental pour lutter contre l'asymétrie d'informations toujours croissante qui oppose les fournisseurs aux individus, une disparité manifeste quand on pense au rôle prépondérant joué par les *Big Tech*.

A l'heure où une nouvelle loi fédérale sur la protection des données vient d'être adoptée et où le Conseil fédéral travaille sur des projets d'ordonnances pour une entrée en vigueur qui devrait intervenir d'ici fin 2022 ou début 2023, la question se pose de savoir quelles sont les démarches à entreprendre en tant que société pour témoigner que votre société a pris conscience de **l'importance à accorder à la protection des données et du sérieux avec lequel les données de vos clients sont traitées**.

En réalité, point n'est besoin d'en faire une « *usine à gaz* », les mesures à prendre dépendant très largement d'une appréciation du niveau de risques eu égard aux données traitées, leurs catégories, leurs volumes, leurs finalités, etc.

Dans la très grande majorité des cas, les six mesures suivantes, susceptibles d'être prises pour un coût raisonnable, suffiront à assurer une mise en conformité suffisante :

1. **Inventaire des données personnelles**

La mise sur pied d'un inventaire consiste à répertorier les différents types de traitements de données qu'effectue la société. S'il ne sera pas exigé pour de nombreuses sociétés n'atteignant pas une taille critique, son établissement apparaît comme une *best practice* qui permettra de prendre conscience à l'interne des traitements effectués et de sensibiliser la direction et les employés au domaine de la protection des données. **Prendre le temps nécessaire pour l'établir est donc loin d'être du temps perdu**.

Les types de traitements opérés peuvent être plus ou moins nombreux. Pour la très grande majorité des PME, ils concerneront typiquement deux grandes catégories d'individus que sont les employés d'une part (paiement des salaires et cotisations sociales, traitement des congés maladie, vacances, entretiens, etc.) et les clients d'autre part (passation de commande, service après-vente, marketing).

Pour chaque type de traitement, **on identifiera les sous-traitants, toujours plus nombreux en matière informatique** (par exemple Microsoft en cas de recours à une plateforme comme Azure ou O365, ou encore SAP dans le domaine des ressources humaines pour ne prendre que deux exemples parlant) et l'éventuel transfert des données traitées à l'étranger. La mise sur pied de l'inventaire sera ainsi l'occasion de s'interroger sur les prestataires existants, l'existence de contrats en bonne et due forme (comprenant des clauses en matière de protection des données et de sécurité) ainsi que sur **la durée de conservation de ces données**, souvent totalement ignorée.

Pour les plus petites sociétés désireuses de dresser un tel inventaire, cette tâche pourra être exécutée par une personne. Pour les PME de taille plus importante, elle devra être déléguée aux responsables d'unités, en contact direct avec les traitements de données auxquels leur unité est rattachée. Si cette tâche doit être exécutée à l'interne, mon expérience m'enseigne que le soutien et la

relecture par un juriste n'est pas inutile, **les équipes à l'interne ayant souvent bien du mal à identifier tous les prestataires qui traitent leurs données, notamment en matière informatique**.

Le document mis sur pied n'est pas statique, mais dynamique et évolutif. Aussi devra-t-il être complété au fur et à mesure des nouveaux traitements effectués.

Les autorités fournissent souvent des documents utiles pour aider à l'établissement de l'inventaire et se poser les bonnes questions ; ainsi en va-t-il en particulier de la CNIL en France.

2. **Politique en matière de confidentialité et autres documents contractuels**

Pour montrer patte blanche, l'établissement de certains documents contractuels apparaît primordial, sans exiger beaucoup d'efforts. On peut ici distinguer suivant que le document revêt une nature interne ou externe.

A l'interne, il est utile d'avoir **une politique en matière de confidentialité** (généralement mentionnée sur le site Internet et complétée par une notice en matière de cookie), qui définit de manière générale le type de données collectées et les traitements opérés. La mise sur pied d'une directive concernant les traitements de données des employés est également désormais usuelle.

A l'externe, on veillera à mettre sur pied un accord de traitement en matière de données type, pour s'assurer que les prestataires externes satisfont à un certain niveau d'exigence. Si de nombreux prestataires auront aujourd'hui leur propre accord en la matière, avoir un document type permettra de s'assurer que celui du prestataire correspond aux exigences de la société et, le cas échéant, de le lui remettre s'il n'en dispose d'aucun.

3. **Analyse d'impact en matière de traitement de données**

Lorsqu'un traitement de données envisagé est susceptible de présenter un risque élevé pour l'individu (par exemple traitement à grande échelle de données médicales), **il convient alors d'effectuer ce que la loi appelle une analyse d'impact**. L'objectif d'une telle analyse consiste à déterminer le niveau de risque du traitement quitte, le cas échéant, à devoir obtenir l'aval préalable du Préposé. En ce cas, l'exercice, pluridisciplinaire, exigera le plus souvent le recours à un juriste à même d'apporter son expertise en la matière.

Pour la très grande majorité des PME, un tel exercice devrait toutefois demeurer limité, exception faite de certains domaines particuliers comme celui de la santé.

4. **Processus relatif à l'exercice des droits dévolus aux individus**

Avec l'entrée en vigueur de **la nouvelle loi fédérale, les droits des individus seront étendus**. En substance, tout société devra être à même d'indiquer à tout individu qui le souhaite si elle traite des données le concernant et, le cas échéant, lesquelles.

Il est alors utile de s'assurer que ces données peuvent être facilement décelées, ce qui devrait être le cas pour les petites PME, mais peut parfois s'avérer plus délicat lorsque les données des individus sont traitées à différents niveaux par différents intervenants. **L'inventaire sera alors un instrument utile pour localiser ces données** au vu des traitements opérés.

La mise sur pied de processus standards et de modèles de réponses peut alors être utile pour faciliter et systématiser de manière uniforme et cohérente le traitement de telles demandes.

5. **Etablissement d'un plan de réponse en matière d'incident de sécurité**

Tout incident en matière de sécurité étant aujourd'hui susceptible d'avoir un impact réputationnel important quand il n'est pas opérationnel, il est fondamental de s'assurer que les données traitées sont entourées de cautèles adéquates en matière de sécurité compte tenu du niveau de risque.

De deux choses l'une : soit **la société en question sous-traite la gestion de son infrastructure IT à un tiers**, et il lui incombe

alors de s'assurer que, sur le plan contractuel, le prestataire en question a fourni les garanties nécessaires en matière de sécurité (par exemple en étant au bénéfice de certaines certifications, ou que le centre de données utilisé est en Suisse ou à tout le moins en Europe, voire qu'un plan de recouvrement de données est en place, etc.) ; soit la société gère son infrastructure IT, et elle doit alors s'assurer que le niveau de sécurité qui entoure le traitement des données est suffisante.

On considère bien souvent aujourd'hui que la question n'est pas de savoir si un incident en matière de sécurité est susceptible de survenir, mais quand. De multiples questions se posent alors : **comment réagir ? Qui doit réagir ? Que faut-il faire en premier ? Dois-je fermer les comptes, isoler le système ? Qui doit être informé ?** Y a-t-il lieu d'informer les employés, les autorités, le public ? Formaliser le processus à suivre dans l'hypothèse où un tel incident surviendrait, c'est donc faire preuve de prudence et témoigner, là encore, d'une prise de conscience de l'importance qu'il y a à protéger les données.

6. **Formation**

Enfin, il est utile de **sensibiliser les employés** à cette thématique en leur assurant une formation qui peut être uniforme ou, le cas échéant, précisée suivant le poste occupé par l'employé (par exemple réceptionniste, ressource humaine, marketing, etc.). L'expérience m'enseigne qu'une formation de base peut aisément être dispensée en 1h à 1h30, un lapse de temps raisonnable pour responsabiliser chaque employé.

7. **Conclusion**

L'ignorance est souvent source de rejet. La protection des données n'y fait pas exception. Méconnue, elle est souvent rejetée par peur des efforts et budgets que l'on croit devoir y consacrer. Pourtant, **quelques mesures simples aux coûts raisonnables suffisent** à se doter d'un niveau de conformité acceptable pour la grande majorité des PME dont les traitements demeurent souvent limités et les risques aisément cantonnés.

Source : https://www.wg-avocats.ch/actualites/protection-des-donnees/nouvelle-loi-protection-donnees/