GDPR: pièges et erreurs au quotidien par Brigitte Doucet - 03/01/2018

“Pas concerné”. Cette réaction qu’ont eue nombre de sociétés ou d’organismes en tous genres en entendant parler de l’entrée en vigueur (fin mai 2018) du nouveau Réglement Général européen pour la Protection des Données (GDPR) est non seulement erronée mais aussi – Dieu merci – de moins en moins vraie. Toutefois, les sociétés qui proposent des services de mise en conformité relèvent encore, quotidiennement, des erreurs d’appréciation, des domaines où les sociétés, de toutes tailles, pèchent encore par légèreté ou manque de compétences.

Peut-être vous reconnaîtrez-vous dans les quelques soucis sur lesquels Charles Delhaye, responsable du département Consulting de NRB, a mis l’accent lors d’un entretien que nous avons récemment eu avec lui au sujet de l’état de préparation sur le terrain… Quels sont les problèmes de conformité rencontrés ou les aspects que les entreprises négligent le plus souvent?

Attention aux embûches inattendues, voire paradoxales

Dans toute infrastructure informatique, dans tout portefeuille de logiciels ou d’applications qu’utilise une société se nichent des outils qui risquent d’amplifier le problème de non-conformité. Exemple typique: les outils de profilage qui opèrent sur base d’algorithmes. Et il y en a évidemment de plus en plus…

Il y a, à l’évidence, une contradiction et une opposition potentielles entre le département marketing d’une société, qui désirera collecter toujours davantage de données à caractère personnel sur les clients, et la personne chargée de veiller à une gestion scrupuleuse de ces données. “Une discussion est absolument nécessaire afin de veiller à la légitimité du stockage de données, de prévoir les mesures obligatoires en amont – comme par exemple l’obtention d’un consentement explicite – et de garantir la transparence pour ce qui est de l’utilisation qui est faite des outils analytiques, sociaux, marketing…”, rappelle Charles Delhaye. Et, chose encore plus fondamentale: le fonctionnement précis de tous ces outils et solutions doit être maîtrisé par ceux qui les utilisent !

Deuxième embûche: le droit à l’oubli. Voilà un droit qu’apprécie chacun d’entre nous, dans la mesure où cela lui donne la possibilité de faire “effacer” des données personnelles inexactes, obsolètes ou qui n’ont aucune raison d’exister dans les bases de données au regard de la finalité légale poursuivie par la société qui les détient.
Mais ce “droit à l’oubli” impose de mettre en oeuvre des procédures strictes qui doivent pouvoir être appliquées rétroactivement. Comme le souligne Charles Delhaye, “les politiques d’archivage existent souvent depuis de nombreuses années et n’ont pas anticipé l’arrivée de ce droit à l’effacement…”

Troisième élément-clé d’une mise en conformité GDPR: les “registres” – ceux qui répertorient et documentent les consentements des personnes “fichées”, les traitements qui

sont faits de leurs données… Un recensement manuel, bien entendu, est souvent chose impossible ou devient vite une tâche herculéenne. Il existe certes des outils qui passent au crible et répertorient les données existantes, les classant et inventoriant mais ces *"data sniffing tools"* ne sont pas forcément à la portée de toutes les bourses ou compétences. Et – retour au paradoxe -, ce type d'outil induit de nouveaux risques de non-conformité!

La raison? Nombre de ces outils sont hébergés et gérés dans le cloud. "Il y a donc un risque de voir les données de l'entreprise filer vers le cloud. Autrement dit, il y a là une réflexion à mener." Et une prise de conscience à prendre… Charles Delhaye préconise dès lors de procéder à un premier inventaire manuel des données à caractère personnel. Deuxième étape: constituer un registre des traitements. Et "ensuite seulement, consacrer de l'énergie à une véritable analyse des risques qui sont réellement encourus, en fonction de chaque contexte métier, selon que l'on opère dans un modèle B2B ou B2C, que l'on ait ou non beaucoup de clients, etc. Cela permet de définir une feuille de route en fonction du "poids" et du niveau de risque."

Priorités

L'exercice et le chantier ne s'arrêtent bien évidemment pas là. Etapes suivantes?

- "conscientiser et informer le personnel
- définir un code de conduite, la liste des choses qui sont ou non permises
- adapter les processus et opérations qui sont perçues comme étant trop risquées – il faut procéder de manière pragmatique pour atténuer sensiblement les risques
- pouvoir s'appuyer sur une politique de classification des données, selon 4 niveaux: données publiques, données privées, données confidentielles, données ultra-confidentielles ; l'idéal pour ces dernières est sans doute de les crypter systématiquement
- détecter les fuites et implémenter des processus de notification aux responsables."
-

Pour ce qui est de "cartographier" les données à caractère personnel collectées et stockées, un travail d'audit du passé est nécessaire mais un autre conseil impératif est de prendre, dès à présent, de nouvelles habitudes qui soient conformes GDPR.
Deux conseils de Charles Delhaye en la matière. Primo: faire revoir les conditions de consentement explicite par le département juridique ou un juriste. Deuzio: "Dès à présent, procéder à l'inventaire et mémoriser systématiquement le fait que telle ou telle personne a cliqué sur le bouton de demande de consentement explicite, à telle heure, sur telle page… Et cela, pour disposer des indispensables éléments de preuve qui ne manqueront pas d'être réclamés en cas d'incident."

Autre conseil: le caractère explicite que doit désormais revêtir le consentement de chaque personne dont on collecte et traite les données implique une totale transparence par rapport à l'usage qui est fait de ces données. Et cela inclut également le "comportement" des *cookies*. Plus question de se contenter, sur un site, d'indiquer que des *cookies* sont à l'oeuvre. "Il faut en décrire les fonctionnalités, décrire clairement quelles données seront collectées, à quelle finalité…"

Charles Delhaye (NRB): “Etablir une cartographie des données et procéder à une analyse d’impact sont essentiels pour mesurer les dommages potentiels provoqués par une fuite de données, par exemple, et pour mettre en oeuvre une gestion des incidents qui soit adaptée et qui inclue un volet communication [aux autorités de contrôle et aux individus concernés] de la nature des dommages subis.”

“Une réelle prise de conscience est nécessaire”, insiste Charles Delhaye. “Les entreprises doivent prendre acte du fait que les informations et les données sont une forme de capital. Les informations, aujourd’hui, sont consubstantielles [lisez: indissociables] de leur proposition de valeur.

Or, les entreprises n’ont pas encore pris conscience de la complexité de l’enjeu, en termes de gestion, de stockage de gestion de l’intégrité des données… Certes, le problème n’est pas neuf mais le fait est qu’il n’a jamais été au centre des préoccupations de la majorité des sociétés. En ce sens, le GDPR force les acteurs à s’interroger sur la manière de traiter et de gérer les informations. Il s’agit dès lors de mettre en oeuvre des modèles de bonne gouvernance: qui fait quoi? quand? pourquoi? et pour combien de temps? C’est là quelque chose de fondamental.”

Quelques conseils

L’un des conseils qui vient immédiatement à l’esprit de Charles Delhaye est de “ne pas taire les incidents” lorsque ceux-ci se produisent malgré tout. D’une part, parce que le nouveau Règlement européen exige une totale transparence et une information aux autorités de contrôle et aux individus concernés. D’autre part, parce que la chose sera tôt ou tard connue.

“Voyez le mal qu’a récemment fait à Uber le fait de ne pas avouer le vol de données de clients, en ce compris leurs coordonnées bancaires! Dans le cas d’Uber, la société avait choisi de taire le piratage mais les banques ont été amenées à investiguer suite à des retraits d’argent illicites… Uber en a donc souffert, en termes de réputation, de perte de confiance pouvant aller jusqu’à un problème pour la continuité des activités.”
Ce qui fait dire à Charles Delhaye: “plus on informe tôt [d’un incident], plus faible sera l’impact mais aussi la responsabilité finale.”

Bien entendu, pour informer rapidement, il faut d’abord que la société soit consciente qu’elle a été victime d’un piratage, d’un vol de données. “C’est aujourd’hui le point faible majeur de nombreuses sociétés. Elles ne sont pas en mesure de détecter rapidement des pertes de données et d’en identifier la cause. Ou encore d’évaluer l’importance des données perdues.”
Seule solution: se munir d’outils de cybersécurité pouvant identifier des tentatives de piratage (dans leurs multiples formes), déterminer leur impact et, si possible bien entendu, les bloquer ou prévenir.

Erreurs flagrantes récurrentes

Au gré des missions de conseils et d'accompagnement qu'a menées NRB, quels sont les travers et les erreurs qui sont le plus souvent détectés et auxquels il convient de remédier et, si possible, d'éviter tout particulièrement? Charles Delhaye en cite trois:

- ne pas être en mesure de détecter une fuite de données: "on peut investir beaucoup dans les différents aspects du GDPR mais une fuite de données est le risque principal. Or, trop peu est fait pour mettre en oeuvre un système de surveillance du réseau, des applications et des systèmes"
- sous-estimer l'importance du Règlement ou "considérer que le GDPR est une contrainte qui n'apporte pas de valeur. En réalité, le GDPR est peut être le bon incitant pour se poser les bonnes questions en termes d'utilisation et d'exploitation des données au sein de l'entreprise. C'est l'occasion de mettre en oeuvre des processus d'amélioration afin d'encore mieux valoriser l'information"
- ne pas former, ne pas informer, faire l'impasse sur les budgets à investir pour conscientiser le personnel de l'entreprise. "80% des vulnérabilités sont en effet d'origine humaine. Il faut donc former et informer de manière régulière, prévoir des cycles de certification du personnel pour éviter les erreurs ou les fautes."