RGPD : la bonne gouvernance des données est un atout

le 31 juillet 2018 - Anne Moreaux - Droit - Actualité du droit

Cela fait déjà deux mois que le fameux Règlement général européen 2016/679 sur la protection des données à caractère personnel – le RGPD - est entré en application. Et pourtant, la grande majorité des organisations n'est toujours pas en conformité. C'est dans ce contexte que l'Institut du Risk & Compliance a organisé une conférence pour échanger sur les mesures à prendre afin d'y parvenir et imposer la gouvernance des données à la tête des entreprises.

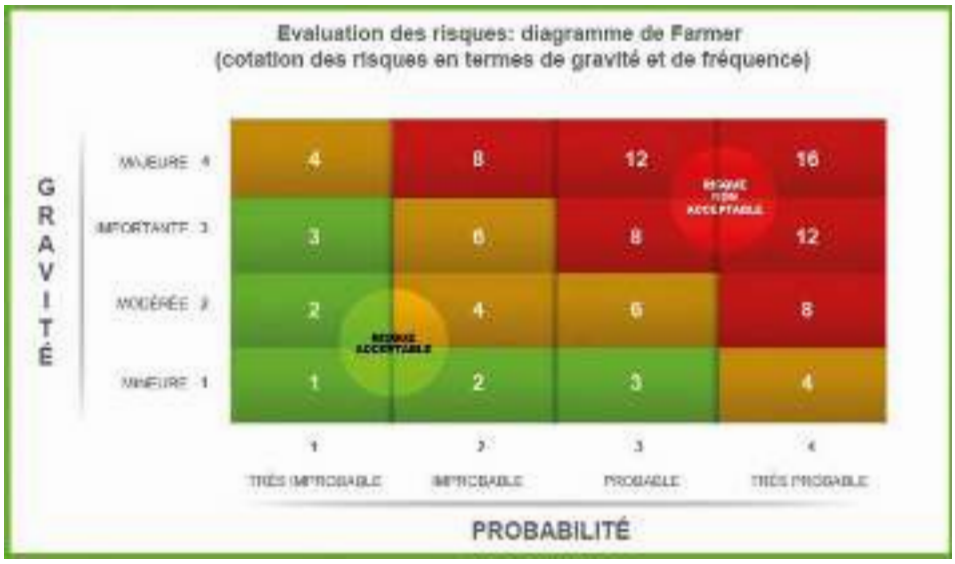
Depuis le 25 mai dernier, date d'entrée en application du RGPD, la Commission nationale informatique et liberté (Cnil) peut venir vérifier le niveau de conformité des organisations (entreprises et associations) et éventuellement prononcer des sanctions.

Cet état de fait provoque des frissons chez de nombreux chefs d'entreprise, directeurs juridiques et directeurs des systèmes d'information (DSI).

En effet, pour la grande majorité d'entre eux, le “projet RGPD” est loin d'être achevé. Comment affiner les prises de décision et mettre en place une bonne cartographie des risques ? Qu'attendre de ses sous-traitants en informatique ?
Quelles sont les bonnes pratiques en cas de contrôle? Comment procéder à l'étude d'impact pour la mise en place du PIA ? Quelles sont les premières étapes en cas de crise ?
Quelles questions restent en suspens ?

C'est pour répondre à ces interrogations et rassurer les chefs d'entreprise que l'association Institut du Risk & Compliance a réuni un panel d'experts dynamiques. Ces derniers ont informé les participants avec des présentations vivantes « en essayant d'éviter que le droit n'assèche les relations humaines avec trop de technicité », a plaisanté Maître Michaël Amado, président de l'association.

Ce dernier est ensuite entré dans le vif du sujet avec une présentation pleine d'humour, introduite par le générique de Retour vers le futur, sur les responsables de traitement des données et les sous-traitants.



Revoir les contrats de sous-traitance informatique

Selon l'avocat, le RGPD oblige les sociétés à refondre les contrats avec leurs sous-traitants. De fait, les devoirs des responsables de traitement des données et des sous-traitants ont évolué. Désormais, les obligations du sous-traitant sont la transparence et la traçabilité, la tenue du registre de traitement des données, la nomination d'un data protection officer (DPO), la prise en compte des principes généraux (privacy by design et by default) et la garantie de la sécurité des données traitées (processus techniques d'anonymisation, notification des violations…). Comme le résume très bien la Cnil, « le sous-traitant est ainsi tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière d'accountability ».

« Ce qui est important est que le contrat détermine bien les critères de traitement de donnée », explique l'avocat qui conseille à l'assemblée de jeter un coup d'œil au contrat-type de la Cnil « extrêmement bien fait ».

Il convient toutefois de rédiger un contrat personnalisé prenant en compte les spécificités de chaque sous-traitant. « C'est un métier de créatif, avocat et juristes doivent aller sur le terrain, comprendre le client et faire un contrat sur-mesure », conseille Me Amado.

Veiller sur la cartographie des risques

« Le RGPD est un énorme challenge technique, surtout pour garantir l'oubli et la qualité de traitement des données », s'est exclamé Paolo Rodeghiero, business analytics advisor et data architect chez Iconsulting, en entamant sa présentation plus technique que juridique sur le rôle et l'importance de la cartographie des risques pour être « RGPD compliant ».

Selon l'expert, le véritable challenge est de maintenir une cartographie dynamique dans une entreprise. En effet, l'écosystème du traitement de données à caractère personnel est vivant et complexe, « la cartographie doit donc être en mouvement ». Il s'agit d'un processus dynamique et continu avec des choix à faire régulièrement.

Le traitement est défini par le fait qu'il s'agit de l'utilisation des données effectuée par un système automatisé.

Pour lui, les organisations doivent apprendre à gérer leurs données comme des « assets » (atouts). En effet, ces dernières représentent le pétrole du XXIe siècle. Il s'agit donc d'un « sujet de gouvernance générale » qui, s'il est bien géré, peut se révéler être un véritable atout business. Pour réussir, il faut que l'initiative soit globale et pas départementale. La stratégie doit ainsi être partagée par tous les services, notamment la tenue du registre des activités de traitement et le PIA (privacy impact assessment).

Pour démarrer, il faut partir sur la base du risque opératif et technique (coût d'indemnisation, caractère sensible, niveau d'activité, prolifération, volume...), puis créer une vision client et la gestion architecturale des consentements des droits par les clients-citoyens. Enfin, il faut adopter une approche “top-down” pour gérer la responsabilité des acteurs.

En conclusion, « la mise en conformité RGPD est une opportunité pour mettre en place une data gouvernance globale ».

Elaborer un PIA adapté au contexte

« On n'a pas besoin de faire de PIA s'il n'existe pas de risque élevé sur des données personnelles, ce qui est finalement très rare », a lancé Corinne Plourde, présidente de 4Cysec, au début de sa présentation sur l'arbre de décision de la réalisation d'un PIA, donc d'une analyse d'impact du traitement de données, adaptée au contexte de son entreprise.

L'article 35 du RGPD impose la réalisation d'une analyse d'impact relative à la protection des données, et explicite quand et comment il convient de la faire.

Cette analyse PIA doit décrire l'intérêt légitime du traitement ;
évaluer sa nécessité et sa proportionnalité ; évaluer les risques pour les droits des personnes concernées ; et apporter les preuves du respect des droits et du RGPD.

Par exemple, un employeur doit impérativement informer ses salariés de la mise en place de caméras de vidéosurveillance et expliciter cette nécessité.

Il existe deux méthodes pour l'analyse des risques : Ebios et ISO 27 005.

La démarche de la Cnil s'inspire de la méthode Ebios avec la détermination du contexte, puis le respect des principes fondamentaux, la gestion des risques et la validation avec un rapport de synthèse pour prouver qu'on est bien en conformité.

Si les cyberattaques se multiplient exponentiellement, l'experte a rappelé que « les événements redoutés ne sont pas qu'informatiques », en citant des exemples d'employés soudoyés par un concurrent pour donner des fichiers de clientèle, ou bien, tout simplement, la perte d'une clé USB ou des archives mal conservées.

Anticiper sa gestion de crise

« Tout se joue en 72 heures pour définir, circonscrire et réagir », s'est exclamé Maître Eric Barbry, du cabinet Racine.

En effet, la gestion de crise due à une atteinte aux données est une question de célérité et d'équipe pluridisciplinaire. « Aujourd'hui, on ne peut pas travailler seul sur le RGPD », explique l'avocat, car c'est « un mélange entre le juridique, le technique, l'organisationnel et la com ». Pour lui, il est évident que « personne n'est RGPD compatible », donc il faut être de savants communicants. C'est pourquoi il fait appel au Dr Raphael Haddad, fondateur de l'agence Mot-clés, afin de prévoir un plan de communication de crise.

En outre, l'article 83 est majeur car il aborde les sanctions financières et la réparation du préjudice, « que l'on a tendance à oublier ».

« Avec le RGPD on a décidé de passer à un nouveau braquet où les responsables ne sont plus que les responsables de traitement », explique Me Barbry.

Dans notre système judiciaire où il y a la possibilité d'avoir des class actions, « ça va saigner dans la réparation du préjudice », pronostique-t-il.

L'avocat a identifié quatre facteurs de risques majeurs :

• le manque de préparation du responsable de traitement et du sous-traitant ;

• le manque de coordination interne entre le DSI, le DJ, le Dircom et le DG ;

• le manque de coordination ente le responsable de traitement et le sous-traitant
(« avoir deux cellules de crise distinctes est pire que de ne pas en avoir ») ;

• le manque de préparation des équipes externes (avocat, expert sécurité, huissier, assureur, agence de communication).

Les cinq réflexes juridiques à avoir, sont :

• la qualification juridique des faits (violation des données ou non qui conditionne la notification à la Cnil et “risque élevé” qui conditionne la communication aux personnes concernées) ;

• la déclaration d'assurance (peut comporter des dispositions data breach) ;

• l'analyse du contrat de sous-traitance si besoin (attention aux clauses data breach) ;

• la gestion des preuves (internes vs externes) ;

• le dépôt de plainte si besoin (l'enquête conditionnant souvent l'action de l'assureur).

Sur la partie technique, il y a quatre étapes à suivre : l'analyse de la situation, la prise de mesures d'urgence, documenter chaque intervention et terminer par faire un retour d'expérience afin d'adapter les mesures techniques pour éviter la récidive.

Sur la partie communication, il faut faire preuve d'empathie, de transparence et évidemment proposer une réparation à la clientèle. La Cnil exige un impératif de transparence, ce qui va imposer une meilleure communication des événements de crise. « Le mauvais réflexe est le silence, comme pour le scandale Lactalis », souligne l'expert. La communication des attentats avec l'intervention régulière du procureur général François Molins était très bonne en la matière.

Préparer un contrôle de la Cnil

Le consultant Jean-Marc Berlioux a expliqué quelles sont les bonnes pratiques en cas de contrôle procédé par la Cnil.

Seulement deux heures après l'entrée en application du RGPD, Maximilian Schrems, un activiste et juriste autrichien, déposait plainte auprès des Cnil française, autrichienne, allemande et belge. L'association française la Quadrature du Net a, quant à elle, déjà lancé une class action contre les Gafam (Google, Apple, Facebook, Amazon et Microsoft) devant la Cnil pour obtenir réparation en cas de préjudice dans le traitement des données personnelles de nombreux utilisateurs.

« Entre Narcisse et Big brother, nous construisons notre double digital qu'il faut protéger », a souligné avec justesse le président de l'association.

L'article 5 de la loi du 14 mai 2018 renforce les pouvoirs d'investigation de la Cnil précisés dans l'article 44 de la loi du 6 janvier 1978. Ainsi, la procédure reprend les dispositions de la loi informatique et libertés et du RGPD. Les contrôles peuvent donc « se dérouler sur place, sur pièces, sur audition ou en ligne », a rappelé Jean-Marc Berlioux. La décision de procéder à un contrôle est prise par le président de la Cnil sur proposition de ses services. Un procès-verbal sera dressé.

Pour maîtriser le déroulement du contrôle, « il ne faut pas paniquer, réunir immédiatement un Comité de contrôle RGPD : DPO, DSI, DJ, et directeur du projet RGPD »,
et s'ils existent y adjoindre le directeur de la conformité et le directeur de la sécurité. L'objectif est d'essayer de faire en sorte que les sanctions soient le moins dommageable pour l'organisation, réduire le risque de sanction ultérieure et faciliter les travaux post-contrôle. « Je vous suggère d'oublier d'essayer d'échapper au contrôle », souligne l'expert en souriant. Le législateur a établi des critères d'aggravation et d'allègement des sanctions éventuelles.

« Ne cachez pas les choses car c'est presque plus grave que la violation pour la Cnil », conseille le professionnel averti.

La coopération et la bonne foi sont de mise, il ne faut donc pas procrastiner : « Montrez que vous êtes diligent et pas négligent ! ».

Si le RGPD consacre de « beaux droits pour les citoyens », il crée « un cauchemar légal » pour les professionnels, a constaté Paolo Rodeghiero avec humour.

Succès de l'outil PIA de la Cnil

La Cnil a mis en ligne depuis cet automne un logiciel PIA (Privacy Impact Assessment) qui s'inscrit dans une démarche d'accompagnement des responsables de traitement dans la mise en œuvre des obligations du RGPD. Disponible en français et en anglais, cet outil est téléchargeable gratuitement.Guillaume Desgens-Pasanau, ex-directeur juridique de la Cnil, explique : « Le RGPD prévoit que, pour certains types de traitement de données, les responsables devront rédiger une étude d'impact dont l'objectif est de vérifier les enjeux de protection et évaluer le niveau de risque en matière de protection de la vie privée. Ce document pourra être communiqué sur demande à la Cnil, qui pourra d'ailleurs faire dans certains cas des remarques et bloquer la mise en œuvre du traitement pendant quelques semaines. La Cnil a donc mis en ligne un logiciel libre qui permet de préparer ce fameux document. C'est un outil d'aide à la décision qui va assister le professionnel sur les informations qu'il doit renseigner et comment évaluer le niveau de risque par rapport à un traitement. »

Des sanctions conséquentes

Désormais, les responsables de traitement de données et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du RGPD. Les autorités de protection peuvent notamment :
• prononcer un avertissement ;

• mettre en demeure l'entreprise ;
• limiter temporairement ou définitivement un traitement ;
- suspendre les flux de données ;
• ordonner de satisfaire aux demandes d'exercice des droits des personnes ;•ordonner la rectification, la limitation ou l'effacement des données.
S'agissant des nouveaux outils de conformité qui peuvent être utilisés par les entreprises, l'autorité peut retirer la certification délivrée ou ordonner à l'organisme de certification de retirer la certification.
S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2 % jusqu'à 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

AP REDACTION

AffichesParisiennes
@Annonce_Legales

Ses derniers articles

Rencontres notariales 2018
“New”, un projet “bois et bas carbone” à Asnières-sur-Seine
Deux créatrices récompensées au concours Ateliers d'art de France