Les enjeux du Règlement général sur la protection des données (RGPD) analysés par le grand spécialiste du sujet, l'avocat **Alain BENSOUSSAN** (cabinet Lexing)

En exclusivité pour les dirigeants des entreprises adhérentes aux syndicats de la Ficime, Alain BENSOUSSAN, le dirigeant du cabinet d'avocat Lexing, grand spécialiste des questions du droit lié aux évolutions technologiques, est venu expliquer, détailler et commenter le fameux RGPD, règlement général sur la protection des données, qui s'impose à toutes les entreprises, même filiales de groupes étrangers.

Voici un résumé de ses propos
pour ceux qui n'ont pu assister à ce moment privilégié.

« Avant le 25 mai, la CNIL cherche la non-conformité, après elle demande aux entreprises de justifier de leur conformité en fournissant la documentation liée au RGPD ! »

C'est ce que Maître Alain BENSOUSSAN, accompagné par Céline AVIGON, avocats du Cabinet Lexing Alain BENSOUSSAN, est venu expliquer aux nombreux dirigeants des entreprises adhérentes aux syndicats de la FICIME qui se sont réunis lors de la matinée des dirigeants dédiée au RGPD le 23 mai dernier. « Accountability », « DPO », « DPA », « privacy by design », « privacy by default », « pseudonymisation », faille de sécurité,… ont été présenté au cours de cette matinée.

Alain BENSOUSSAN a mis en place, pour guider les entreprises dans leur mise en conformité, une feuille de route en 20 étapes, avec une dizaine de documents par étape, à présenter à la CNIL lors d'un contrôle.

Au cours de cette matinée, 2 risques ont été tout particulièrement identifiés compte tenu de la spécificité des adhérents, à savoir d'une part, les flux de données transfrontières et, d'autre part, le traitement des données sensibles.

Il est impératif lors de flux de données transfrontières de s'assurer de la légalité de ces transferts.

Il a insisté sur le fait que *« les opérateurs économiques ont un travail important à mener dans la mesure où il est nécessaire, non seulement d'intégrer les nouvelles obligations du règlement européen 2016-679, mais également de purger celles de la loi informatique et libertés de 1978. À ce sujet, si la CNIL a indiqué faire preuve de pédagogie sur les nouvelles obligations du RGPD, il en va autrement de celles issues de 1978, 1995 ou 2004, et en particulier en ce qui concerne les données dites sensibles (santé, religion, appartenance syndicale, raciale, ethnique, orientation et vie sexuelle) pour lesquelles en cas de non-respect, la CNIL sanctionnera »*. Par conséquent, pour éviter des poursuites, Maître BENSOUSSAN conseille de régulariser sans délai la situation et de respecter ces obligations anciennes.

Le RGPD veut rendre la maîtrise de la donnée à ses titulaires !

Ensuite, il a rappelé l'importance des sanctions prévues en cas de non-respect du RGPD, à savoir 10 millions d'euros ou 2% du CA mondial pour les unes, et 20 Millions d'euros ou 4% du CA mondial pour les autres.

Les entreprises présentes ont toutes été vivement invitées à adresser, dans un premier temps une lettre de posture vis-à-vis des salariés et clients, afin de rappeler l'importance accordée aux traitements de leurs données personnelles et de la prise en compte des règles y afférentes. Puis dans un second temps, de mettre en place un Code ou Charte éthique, une politique interne sur les données personnelles, une politique externe,… Il est essentiel que les dirigeants définissent et impulsent la gouvernance et l'organisation de la mise en conformité afin que le principe directeur du RGPD, à savoir l'accountability (documentation), soit respecté.

Conseil aux dirigeants : mettre en place une délégation pénale liée à la protection des données personnelles au profit des collaborateurs concernés

Enfin, il a été rappelé que les dirigeants et directeurs métiers (DRH, DSI, ou autres) n'ont pas vocation à être nommés délégués à la protection des données (DPO), dans la mesure où cela créerait un conflit d'intérêts entre les deux fonctions.

Cette mise en conformité du RGPD se fait selon 3 principes :

- en l'état des connaissances,
- en tenant compte du coût économique
- en tenant compte de la probabilité de la survenance de ces risques.

Cela implique de définir à la fois une stratégie organisationnelle et une stratégie juridique.

Un rapport de diagnostic

Face à l'ampleur des travaux à mener par chacun, le cabinet Lexing met en place une Intelligence Artificielle « Dis-moi Eva » dédiée au macro-diagnostic en matière de conformité relative à la protection des données personnelles.

Un Questionnaire avec une 100 aine de questions, le texte de loi y afférent et en dessous là où l'on se situe dans les 20 étapes à passer. Une fois que l'on a terminé de répondre aux questions, le logiciel établit un rapport. Il y a une jauge pour mesurer son état de conformité général mais également pour chacune des étapes.

« Le Logiciel permet d'avoir un premier document et d'être en conformité si l'ensemble des points et préconisations sont respectés » assure Alain BENSOUSSAN.

Pour ce faire, une demi-journée de workshop dans l'entreprise de 3 à 4h est nécessaire pour établir le diagnostic de conformité de l'entreprise. S'en suit ensuite, une demi-journée de restitution par un collaborateur du cabinet avec la feuille de route permettant de savoir ce qu'il reste à faire. En fonction, l'entreprise pourra avoir recours soit à ses ressources internes (création des documents de procédures politiques et autres….), soit recourir au cabinet LEXING pour être accompagnée.

Enfin, un accès à un site web RGPD, destiné à accueillir et centraliser la documentation de conformité du RGPD, est mis à la disposition des utilisateurs du macro diagnostic afin de les retrouver facilement lors des contrôles.

Les 10 premières entreprises adhérentes présentes bénéficiaient d'un prix privilégié pour utiliser le macro diagnostic. **Une proposition de prestation de macro diagnostic est proposée en exclusivité aux entreprises adhérentes aux syndicats regroupés au sein de la FICIME, à des conditions financières privilégiées.**

Les demandes sont centralisées auprès de Céline AVIGNON à l'adresse suivante :
celine-avignon@alain-bensoussan.com

Questions - réponses

> Alain ROSAZ : Est-ce que les positions que vous avez sur les textes sont les mêmes que celles de la CNIL, et sécurisent-elles vos clients qui les suivent ?

Alain BENSOUSSAN : *« Le fait d'avoir été le premier à établir des positions permet de ne pas être sanctionnable en tant que tel et, en cas de divergences avec la CNIL, on fera les modifications nécessaires au fur et à mesure des évolutions doctrinales de l'autorité de régulation. »*

> Participant : Comment puis-je contrôler si le sous-traitant respecte bien le RGPD ?

Alain BENSOUSSAN : *« En matière de sous-traitance, l'article 28 permet contractuellement de contrôler et contraindre le sous-traitant au respect de ses obligations. De la même manière, lorsque vous utilisez des fichiers clients achetés, il est nécessaire contractuellement de s'assurer du respect du RGPD et de demander la communication d'une attestation d'assurance couvrant le risque y afférent. »*

FICIME
L'alliée de votre réussite

43-45 rue de Naples – 75008 PARIS
TEL : *01 44 69 40 82* **– FAX :** *01 44 69 40 61*
e-mail : *info@ficime.fr – http://www.ficime.com*
N° RCS : *PARIS B 784 311 854* **– APE :** *911 A*