Maître Bensoussan répond à vos questions

Au cœur du projet de règlement européen, le Data Protection Officer (DPO) va devenir un acteur incontournable de la conformité relative à la protection des données. Les entreprises doivent d'ores et déjà connaître les contours des obligations et les challenges qui vont être pris afin d'intégrer ce nouvel acteur. Maître Alain Bensoussan répond à vos questions pour vous permettre un passage en douceur lors de la promulgation du futur règlement.

Pourquoi un projet de règlement européen sur la protection des données ?

Le projet de règlement européen est un très grand projet qui reprend tous les essentiels de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Et il rajoute des concepts qui s'additionnent à la majorité des principes de la directive sur la protection des données personnelles et de la libre-circulation des flux à l'intérieur de l'Europe.

Le projet de règlement a vu le jour du fait de la très grande fragmentation qui existe entre les différentes législations. Malgré la mise en place de la directive 95/46, l'harmonisation entre les pays européens ne s'est pas faite. De hautes autorités sont des juridictions dans certains pays d'Europe et pas dans d'autres. Certaines autorités sont extrêmement sévères alors que d'autres le sont beaucoup moins. Face à ce constat et au fait que la protection des droits des personnes est un droit essentiel, il ressort de l'article 8 de la Charte des droits fondamentaux européens et l'article 16 du Traité de fonctionnement de l'Union européenne (TFUE) – Traité de Lisbonne – que chacun des citoyens européens mérite ce droit fondamental. Il est donc nécessaire qu'il puisse s'exercer dans tous les pays de la même manière, ce qui n'est pas le cas aujourd'hui. Et c'est donc au titre de ce constat de grande diversité qu'il a été décidé de prendre un règlement.

La différence entre une directive et un règlement est importante. Dans le premier cas, les Etats ont un pouvoir d'interprétation de la directive puisqu'ils doivent la transposer (c'est-à-dire la traduire) au sein du "corpus légal" préexistant alors que dans le second cas, l'application du règlement est immédiate sans aucune possibilité pour les Etats d'intervenir. Cela n'est possible qu'au titre des principes de subsidiarité et de proportionnalité (art. 5 TUE), le premier permettant de réserver aux instances européennes ce que les États membres ne peuvent effectuer que de manière moins efficace (en l'occurrence, la protection des données personnelles) et le second, de ne pas excéder ce qui est nécessaire à la réalisation des objectifs (c'est-à-dire éviter des législations trop détaillées).

Quelles seront les principales dispositions du projet de règlement européen sur la protection des données ?

Le projet reprend tous les grands principes de la loi Informatique et libertés : la collecte loyale ; la finalité, la qualité des données qui doivent être adéquates, pertinentes et non excessives ; la durée de conservation nécessairement limitée par le droit à l'oubli (NDLR : il y a un certain délai de péremption) ; le respect du droit des personnes (information, accès, rectification, opposition), la sécurité et les formalités préalables. L'ensemble de ces principes sont repris sauf celui des formalités préalables qui sont supprimées.

En revanche, trois nouveaux principes sont ajoutés :

- Un grand principe tout d'abord : celui de "minima" ou de "subsidiarité". Il s'agit de l'article 5c du projet de règlement qui précise que les données doivent être utilisées de manière limitée au strict minimum c'est-à-dire sans excéder ce qui est nécessaire pour atteindre l'objectif pour lequel elles ont été collectées . Et la charge de la preuve du respect de ce principe repose sur les épaules du responsable du traitement qui doit démontrer que le traitement en question s'impose. C'est une véritable révolution. C'est là une grande différence entre l'Europe et les Etats-Unis. L'Europe a pris comme principe que le traitement de données à caractère personnel en Europe doit être l'exception à l'inverse des Etats-Unis.

Ainsi, aux Etats-Unis prévaut le "principe de liberté sauf" et en Europe, le "principe d'interdiction sauf" qui ne sera pas sans conséquence sur l'activité respective des sociétés utilisant des données à caractère personnel.

Les deux autres principes sont de nature beaucoup moins importante :
- Il s'agit de l'article 17 consacrant le droit à l'oubli dans l'Union européenne, jusque-là sous-jacent par le biais de la date de péremption des données ;
- Le second principe est celui de la portabilité, c'est-à-dire que les personnes ont le droit d'obtenir de la part du responsable de traitement la copie de leurs données à caractère personnel dans un format qui peut être réutilisé par d'autres prestataires. Il s'agit de l'article 18 du projet de règlement. Toutefois, ici on est plutôt en présence de la manifestation d'un droit de la consommation que d'un droit de l'homme.

Au-delà des principes que nous venons d'évoquer, sur le plan concret quelles seront les principales obligations ?

Il y a quatre ajouts fondamentaux : l'accountability, le privacy by design, l'étude d'impact et les failles de sécurité. En contrepartie, il y a suppression des formalités préalables.

- **L'accountability** est un principe qui nous vient des Etats-Unis. L'accountability est l'obligation pour les responsables du traitement de garantir la conformité à la loi Informatique et libertés. Les responsables du traitement doivent donc documenter l'ensemble des actions de leur politique Informatique et libertés pour pourvoir démontrer dans le cadre d'un contrôle ou d'une plainte, qu'ils ont bien rempli leur obligation.
- **Privacy by design** signifie que les responsables de traitement, doivent intégrer l'ensemble des obligations Informatiques et libertés dès la conception des projets informatiques, c'est-à-dire de la création au développement d'application, de la livraison à l'installation, de la recette à la maintenance en passant par la garantie.

Pour le droit à l'oubli, cela signifie que pour chacune des données en relation avec le traitement, on a une date limite d'utilisation même si très souvent, elle n'existe pas parce qu'une information peut se trouver dans plusieurs traitements et donc avoir plusieurs dates limites.

- **L'étude d'impact** est l'article 33 du projet de résolution. C'est l'obligation de faire des études sur les risques ainsi que sur les mesures à prendre lorsque ces risques se réalisent. Il s'agit en quelque sorte de mettre en œuvre un plan de prévention pour gérer les risques en matière de violation des droits des personnes, éviter qu'ils se réalisent ; et dans le cas contraire, mettre en œuvre toutes les mesures prévues pour revenir à un système où les droits des personnes concernées ne sont pas mis en cause.

Alors quels sont les traitements à risque ? Pour l'instant, il y a encore des arbitrages mais c'est essentiellement les traitements portant sur les données sensibles (informations religieuses, raciales, politiques, syndicales, vie sexuelle, santé…), mais aussi tous les traitements qui gèrent de quantités phénoménales de données (big data), et enfin, les dispositifs de surveillance des lieux publics, en particulier utilisés à grande échelle (notamment une ville).

Maître Bensoussan répond à vos questions *(suite)*

- La **notification des failles de sécurité** à l'autorité de régulation – en France, la CNIL – dans les plus brefs délais (c'est-à-dire inférieur à 24 heures). L'autorité de régulation des données personnelles doit être informée très rapidement de cette violation afin de prendre toutes les mesures, en concertation avec le responsable de traitement, et éventuellement le sous-traitant, et supprimer les conséquences de cette faille de sécurité. En fonction du niveau de gravité, l'autorité a la possibilité de prévenir toutes les personnes concernées par ladite faille afin de leur permettre de prendre les mesures nécessaires.

Quel sera le rôle du DPO ?
Le projet de règlement engendre une autre grande modification : les entreprises employant plus de 250 personnes devront intégrer un Data Protection Officer (DPO) dont le rôle n'a plus rien à voir avec celui de Correspondant informatique et libertés (CIL).Il s'agit pour lui, de passer d'une obligation d'assurer la conformité" (article 22 de la Loi française) à une obligation de contrôler au sens de surveiller et d'auditer l'entreprise. Ce sont les premiers pas d'un commissaire aux données. Il s'agit là d'une modification fondamentale du règlement qui fait du DPO, un relais des autorités de protection des données à caractère personnel.

Il a l'obligation d'informer et de garder la trace de toutes ses relations avec l'autorité, mais il doit aussi vérifier la prise en compte des grandes obligations Informatiques et libertés par le responsable de traitement, c'est-à-dire l'accountability, la privacy by design, l'étude d'impact et le respect des dispositions relatives aux failles de sécurité. Il doit contrôler la politique Informatique et libertés, y compris avec le sous-traitant, la mise en œuvre de toutes les obligations. Il doit veiller à ce que la documentation soit à jour, contrôler cette documentation et répondre aux éventuelles demandes d'autorités de contrôle. C'est le début d'un commissariat aux données, à termes donc, une modification radicale.

Quelles seront ses qualifications ?
Le DPO doit avoir une compétence technique certaine, une compétence du métier principal du responsable de traitement et être capable de maîtriser la compréhension des grandes questions informatiques. Il n'y a pas d'obligation encore particulière. Il doit avoir la capacité lui permettant de maîtriser ses obligations. C'est le 5e alinéa de l'article 35 : le responsable de traitement sous-traitant désigne un délégué à la protection des données sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées de la législation et des pratiques en matière de protection des données, ainsi que de sa capacité à accomplir les tâches énumérées à l'article 37. Cette fonction requiert un haut niveau de connaissances spécialisées notamment en fonction du traitement effectué des données et de leur niveau de protection exigé.

C'est bien une adéquation entre compétence métier, légale, et informatique qui doit être réunie dans ce triptyque pour permettre au DPO d'être un commissaire aux données et non un CIL.

Quid du calendrier ?
Le calendrier publié par le Parlement européen prévoit un examen en séance plénière, 1ère lecture/lecture unique, le 11 mars 2014 (Date indicative). Il devrait vraisemblablement aboutir à une publication au premier semestre 2014. S'agissant d'un règlement européen, il ne fera pas l'objet d'une transposition dans le droit national, mais sera d'application immédiate deux ans après sa publication, donc en mai 2016.

Faut-il anticiper ?
Clairement oui. Il faut nécessairement anticiper les appels d'offres en cours dont les grandes applications seront mises en œuvre en 2016, à peut près en même temps que le règlement européen.

D'ici mai 2014, il faut penser à indiquer dans les appels d'offre que l'entreprise s'engage à livrer une application conforme au règlement dans le cadre de la réalisation des applications entrant en vigueur en 2016. Pour les projets en cours de signature, il faudra les faire évoluer dans la mesure du possible en fonction de l'état de la situation pour assurer leur conformité au règlement.

Vidéosurveillance Infos est une publication bimestrielle éditée par Chrystallia SAS au capital de 5 000 € - 752 071 019 RCS Evry - APE 7221 Z
24, domaine de Bel-Abord - 91380 Chilly-Mazarin - Tél. 06 06 91 38 06
Directrice de la publication : Evelyne Guitard - Impression : Imprimerie Blr.com
Abonnement annuel : 120 € HT (format papier) - 60 € HT (format électronique) - 15 € HT (vente au numéro) - Tarif applicable jusqu'au 31 décembre 2013