RÈGLEMENT (UE) 2016/679

La *data compliance*, un avantage compétitif pour les entreprises ?

En association avec le cabinet DLA Piper, le Cercle Montesquieu a récemment organisé une conférence sur le renforcement des règles entourant la protection des données personnelles, issues du règlement européen 2016/679. Qu'il s'agisse d'organismes publics, privés, ou même d'individus, ce règlement va « profondément modifier la manière dont les données personnelles sont encadrées ».

©A.P.

Marie Abadie, Valérie Valais, Jeanne Bossi Malafosse et Florence Raynal.

Et si la protection des données personnelles était source d'avantages concurrentiels pour les entreprises ? C'est en tout cas ce qu'a souhaité transmettre Valérie Valais, directrice Affaires publiques et Corporate Development de Dassault Systèmes, en conclusion de la conférence intitulée « Le règlement européen sur la protection des données personnelles et ses implications pour les entreprises », organisée récemment par le Cercle Montesquieu, en partenariat avec DLA Piper.

En effet, à première vue, le règlement (UE) 2016/679 semble plutôt rimer avec contraintes et coûts supplémentaires pour les entreprises en charge du traitement de données personnelles.

D'autant plus que le texte est « *copieux* », selon Jeanne Bossi Malafosse, avocate chez DLA Piper, puisqu'il est commun à l'ensemble des États membres et « *prend en compte le développement d'internet et son explosion* » (Big data, internet des objets…). Mais ce règlement est surtout porteur d'un « *changement de paradigme* » : les pays membres de l'UE vont passer d'un contrôle *a priori* (exercé par les 28 Cnil européennes) à une responsabilisation accrue des acteurs (avec suppression des formalités préalables) et un renforcement du contrôle *a posteriori* des autorités (pouvoir de sanction accru), qui auront désormais un rôle de conseil.

Le Comité européen à la protection des données (CEPD) va ainsi remplacer le G29. Il sera chargé de régler les litiges entre les dif-

férentes autorités de régulation, et d'élaborer une « *doctrine européenne* » (un pouvoir de sanction lui sera également octroyé).
Aussi, ce principe d'*accountability* (de responsabilisation des acteurs) va s'accompagner de la notion de « *privacy by design* », c'est-à-dire que la protection des données devra être prise en compte *ab inito*, dès la conception du projet. L'entreprise devra donc mettre en place des « *processus techniques et organisationnels de nature à être "compliant" à tout moment avec la protection des données* ». De nouveaux outils ont de fait été créés pour laisser la possibilité aux responsables de traitement de démontrer leur respect du règlement : le texte consacre les codes de bonne conduite et les certifications ; des mesures qualifiées de « *soft law* » par Jeanne Bossi Malafosse, puisque les acteurs sont « *associés à la définition de ces règles* ».
Dans le même sens, Florence Raynal, directrice adjointe et chef du Service des affaires européennes et internationales de la Cnil, a souligné que le règlement allait provoquer un véritable « *changement d'état d'esprit* » pour les entreprises. Les organismes devront ainsi passer d'une « *conformité statique, bureaucratique* » à cette « *conformité dynamique* », où l'entreprise devient redevable de sa mise en conformité.

Des droits individuels renforcés

C'est aussi un changement pour les individus, qui « *avaient une impression de perte de leurs données personnelles* », et dont certains droits seront renforcés. C'est d'abord le cas du droit à la portabilité (tirés du droit à l'accès aux données), un droit « *essentiel* » pour la directrice adjointe de la Cnil, en ce qu'il donne la possibilité à l'individu d'être « *indépendant des plateformes* » auprès desquelles il aura « *développé une activité une existence en ligne* ».
En effet, ce droit lui permet de récupérer unilatéralement les données qu'il a fournies, pour les utiliser « *comme bon lui semble, dans un format interopérable* ». En plus de renforcer l'autonomie des internautes, le droit à la portabilité ouvrira la voie à de nouveaux services spécialisés dans la récupération de ces données personnelles.
Le droit à l'oubli est également consolidé par le règlement, dans la suite logique de l'arrêt Costeja (C-131-12) de la cour de justice de l'Union européenne. Le moteur de recherche Google avait, en l'espèce, été reconnu responsable du traitement des données à caractère personnel apparaissant sur des pages web publiées par des tiers. C'est aussi et enfin le cas du droit peu connu à la limitation du traitement, qui permettra la suspension d'un traitement de données à caractère personnel.
En complément, et pour une meilleure application de ces droits, le règlement consacre une « *obligation de transparence* » vis-à-vis de l'internaute, qui oblige les responsables de traitement à communiquer sur le traitement effectué et la manière d'exercer les droits précités. Ainsi, pour Florence Raynal, le règlement « *rééquilibre une relation qui était asymétrique entre l'entreprise et l'individu* ».
Mais qui sera alors chargé du respect de ces règles au sein de l'entreprise ?

DPO or not DPO

Pour assurer le respect de ces règles, les responsables de traitement et sous-traitants auront l'obligation de nommer un délégué à la protection des données (DPD ou DPO en anglais) dans les cas suivants : s'ils appartiennent au service public, si le traitement exige un suivi régulier et systématique des personnes à grande échelle ou si le traitement les amène à manipuler des « *données sensibles* » ou relatives à des condamnations.
Le DPO a avant tout « *un rôle de conseil et d'accompagnement à la conformité* », pour Florence Raynal, d'autant que l'entreprise restera responsable du traitement des données personnelles. Ses missions consistent effectivement à informer, conseiller le responsable de traitement, contrôler le respect du règlement intérieur et du droit national, conseiller l'organisme sur la réalisation d'une analyse d'impact et d'en vérifier l'exécution, et enfin à coopérer avec l'autorité de contrôle et d'être le point de contact avec celle-ci. Quoi qu'il en soit, il peut toujours être opportun de posséder un Data Protection Officer même si la structure n'en a pas l'obligation, selon Florence Raynal.

Vers une entreprise « data compliant »

Quant à l'installation de la *data compliance* dans l'entreprise, il s'agira de « *mettre en place une politique de protection des données* », à diffuser comme toute politique de ressources humaines ou d'utilisation des outils informatiques, a simplifié Jeanne Bossi Malafosse. « *C'est à chacun de trouver les moyens d'être compliant* », a-t-elle ensuite souligné, précisant qu'il fallait produire un travail en parallèle avec le droit positif encore applicable.
Le plan d'action adopté par le G29, organisé autour de trois axes prioritaires (publication de lignes directrices pour les responsables de traitements et sous-traitants, réflexion sur les mécanismes de coopération et mise en place de la CEPD), prévoit la publication des lignes directrices sur le DPO et la portabilité pour décembre 2017 (ce travail vise à préciser certaines notions floues, telles que le caractère « *régulier* » du traitement, de ce que recouvre le terme « *à grande échelle* », ou encore la question de savoir si le DPO facultatif sera soumis aux règles du DPO obligatoire).
Pour finir, il est à noter que les sanctions décidées par les Cnil européennes pourront atteindre 4 % du chiffre d'affaires mondial de l'entreprise incriminée. « *Les autorités basculent dans une autre dimension* » a appuyé en ce sens Valérie Valais. Il est donc indispensable de « *démarrer dès maintenant* », mais aussi et surtout de montrer aux entreprises que ces règles « *ne seront pas une contrainte mais un atout* ».
Ainsi, le respect de ces règles réduit les risques liés à la responsabilité, augmente la confiance des consommateurs, et valorise l'image de marque de la structure. Pour conclure, tant que la *data compliance* « *ne porte pas atteinte au business et correspond aux intérêts et objectifs de l'entreprise* », elle peut tout à fait être source de valeur ajoutée, et constituer un avantage compétitif indéniable.

Quentin Clauzon
redaction@affiches-parisiennes.com

Cercle Montesquieu

Le Cercle Montesquieu, un des premiers lieux de réflexion sur la fonction de directeur juridique dans l'entreprise et sur ses aspects managériaux, regroupe des directeurs juridiques de tous les principaux secteurs d'activité, d'entreprises privées, publiques, d'associations et d'institutions.

☛ *www.cercle-montesquieu.fr*