actuEL | Direction Juridique
Un journal en ligne des Éditions Législatives

Règlement européen sur les données personnelles : une "opportunité" pour Christoph Geiger

07/10/2016

A la question : "le règlement représente-t-il une contrainte ou une opportunité ?", la réponse du General Counsel de Siemens SA est nette. Le texte allège le formalisme demandé aux entreprises, même s'il leur impose d'avoir une attitude plus responsable vis-à-vis de la donnée.

Au mois de mai, l'Union européenne (UE) adopte le règlement européen sur la protection des données personnelles. Puis en juillet, la Commission européenne valide le *Privacy Shield*. L'actualité règlementaire aura été riche ces derniers mois sur la problématique données. Comment la direction juridique de Siemens appréhende-t-elle ces nouveaux textes ? Réponse de Christoph Geiger son General Counsel.

Comment Siemens utilise les données personnelles ?

Siemens dispose de différentes données. Tout d'abord, nos produits collectent des données (dont des données personnelles) des salariés de nos clients et des utilisateurs finaux, tel que notre scanner médical. Nos clients peuvent alors nous demander d'analyser les données des machines Siemens (ce que l'on dénomme le smart data), pour rendre plus efficace la production de celles-ci. C'est le cas des éoliennes connectées au big data, à savoir à la météo. Ainsi, l'éolienne connectée adapte son ergonomie à la météo pour améliorer son rendement de 1 %. Nous analysons également les données de nos clients d'un point de vue marketing (ou du CRM (*client relation management*)). Enfin nous avons à gérer les données de nos propres salariés.

La donnée personnelle est-elle une bombe à retardement ?

Le règlement européen sur la protection des données personnelles, qui entrera en vigueur en mai 2018, va changer la donne (voir notre article). Il met en place un contrôle *a posteriori* du traitement de la donnée à la place du système déclaratif existant - *ex-ante* - à réaliser auprès de la CNIL. En ce sens, chaque entreprise devra se responsabiliser (principe d'*accountability*) sur la question des données personnelles par l'adoption d'un système adéquat de protection et par l'utilisation du *privacy by design* (voir notre article). De plus, la responsabilité du fournisseur pourra être engagée en plus de celle du responsable de traitement de la donnée. Ces nouvelles obligations impliquent que les entreprises s'y adaptent bien en amont de l'entrée en vigueur du texte. Et les sanctions en cas de non-respect sont très élevées [*jusqu'à 4 % du chiffre d'affaires mondial de l'entreprise, ndlr*].

Le règlement représente-t-il une contrainte ou une opportunité pour les entreprises ?

Le règlement est une opportunité. Il allège encore plus le formalisme lié à la matière. De plus, il offre des règles harmonisées pour l'UE et devra être interprété de manière homogène en Europe. Ainsi, une coordination des différentes CNIL des États membres est organisée par le texte et le futur Comité européen de protection des données (CEPD) tranchera les litiges entre elles. Le règlement devrait aussi motiver les entreprises à utiliser des outils qui respectent la donnée personnelle - du fait du *privacy by design* -, comme par exemple les programmes détruisant les cookies de manière automatique. Enfin, le CEPD aura le pouvoir de mettre en place des *guidlines* afin de renforcer la mise en place des techniques de chiffrage ou d'anonymisation. Ceci facilitera aux entreprises l'utilisation et l'analyse des data.

Quelles sont vos pistes de travail pour vous mettre en conformité avec le règlement ?

Tout d'abord nous devrons réfléchir à aménager le principe de responsabilité. Un audit sera à mener en ce sens. Nous devrons désigner le DPO (*data protection officer*) (voir notre article). Nous aurons aussi à mener une analyse des risques et à définir les moyens qui nous permettrons d'y faire face (via des *privacy impact assessment*). Cela nécessite une certaine organisation interne. L'esprit du règlement me fait beaucoup penser à la mise en place du programme de compliance dans le domaine de l'anti-corruption (via l'adoption d'un code de conduite, de formations internes, etc.), comme peut l'aborder aujourd'hui le projet de loi Sapin II (voir notre article). Notre approche ira dans le même sens. Par exemple, le DPO, qui sera un membre de la direction Legal & Compliance, mènera des audits avec le business sur des problématiques données personnelles. Enfin, concernant la responsabilité possible du fournisseur prévu par le règlement, il faudra définir les rôles respectifs clients/fournisseur sur le traitement des données personnelles. Nous devrons revoir nos contrats au cas par cas en ayant cela en tête.

Comment avez-vous géré l'invalidité du s*afe harbor* et l'entrée en vigueur du *Privacy Shield* ?

Il a fallu agir suite à l'invalidation du *safe harbor* par la Cour de justice de l'UE (voir notre article).

Siemens avait déjà mis en place des *binding corporate rules* (BCR), un code de bonne conduite, pour l'échange d'informations, et ainsi de données, entre les différentes entités du groupe. Tous nos flux de données vers l'entité américaine du groupe, et d'autres dans le monde en dehors de l'UE, sont gérés par

les BCR. Par ailleurs, la CNIL a allégé la mise en place des BCR le 27 mars dernier avec l'introduction de l'autorisation unique.

Pour nos relations avec nos partenaires externes, cela a été plus compliqué. Nous avons réalisé une *due diligence* pour identifier les fournisseurs basés aux États-Unis qui recevaient nos données, notamment des données sur les salariés de Siemens liées aux logiciels de paie. Des clauses contractuelles types, acceptées par la Commission européenne et la CNIL, ont alors été signées avec nos fournisseurs pour le traitement des données. Mais nous sommes toujours sous une épée de Damoclès car un recours a également été porté par Max Schrems - auteur des premiers recours contre Facebook ayant donné lieu à l'invalidation du Safe Harbor - sur la validité de ces clauses types. Il a été porté devant l'autorité irlandaise de protection des données qui souhaite s'en remettre à l'analyse de la CJUE. Si ces clauses étaient remises en cause, il nous faudra alors trouver de nouvelles solutions, via l'anonymisation ou le cryptage des données, par exemple.

Le *Privacy Shield*, approuvé par la Commission européenne le 12 juillet 2016, prévoit, lui, des garanties au traitement des données personnelles et une auto-certification des entreprises américaines (voir notre interview). 4000 entreprises s'y sont inscrites et ont à encadrer leur traitement des données personnelles. Dès lors, si vous traitez avec une entreprise qui en bénéficie, vous pouvez lui transférer vos data suite à une simple déclaration auprès de la CNIL.

propos recueillis par Sophie Bridier
