

**Se préparer aujourd'hui aux réformes de l'UE sur la protection des données**

**Sécurité**

Posté par : JPilo

Publiée le : 7/5/2014 13:30:00

Le Parlement européen a récemment voté une révision majeure de la législation sur la protection des données, la première depuis 1995, qui modifiera profondément la manière dont les données personnelles sont utilisées. Les 28 Etats membres auront 2 ans pour se plier aux nouvelles réformes à compter de leur approbation par le Conseil européen.

Ce délai semblera probablement large pour certaines entreprises. D'autres seront même tentées de n'agir que lorsque les nouvelles normes seront obligatoires.

Pour leur part, les consommateurs européens attendent depuis longtemps un renforcement des droits et de la protection des données personnelles, dont la nécessité a récemment été rappelée par les révélations médiatisées d'un ancien consultant de la NSA sur l'espionnage gouvernemental. De nombreuses entreprises risquent ainsi d'être confrontées à de nouvelles obligations qu'elles n'avaient pas anticipées.

Les réformes de l'UE sur la protection des données remplaceront l'ensemble des lois nationales actuelles. Les entreprises devront alors répondre devant une seule autorité européenne au lieu de 28, ce qui simplifiera les procédures de l'UE, avec à la clé des économies estimées à 2,3 milliards d'euros par an.



Les nouvelles règles viendront clarifier les questions de consentement et de notification des violations des données. Quantité d'entreprises investissent aujourd'hui davantage dans la remédiation des pertes de données et les investigations que dans la protection des données elle-même.

Un changement s'impose, qui est tout l'objectif des nouvelles réformes. Tout défaut de protection des données aura d'ailleurs de sévères conséquences financières. Les amendes en cas d'incident peuvent en effet atteindre 5 % du chiffre d'affaires annuel d'une société privée.

Mais les amendes pour violation de données ne sont pas nouvelles et elles n'ont manifestement que peu d'effet sur la responsabilisation des entreprises vis-à-vis de la gestion et de la protection des données sensibles. Les entreprises feraient bien de renforcer dès à présent leurs capacités de protection des informations, indépendamment des craintes concernant les nouvelles réglementations à venir.

C'est à elles qu'il revient d'évaluer, de gérer et de limiter l'exposition au risque de leurs informations d'un bout à l'autre de la chaîne, dans le cadre d'un programme de responsabilité des informations d'entreprise (ou Corporate Information Responsibility, CIR).

En Allemagne, elles ont déjà pour obligation de désigner parmi leur personnel un(e) responsable de la protection des données et du maintien de la conformité avec la loi. Voilà un bon exemple à suivre pour les autres pays de l'UE. Pour satisfaire les nouvelles exigences, les entreprises vont devoir dresser un bilan de leurs pratiques actuelles et s'assurer que les procédures et politiques en place sont à la hauteur.

Attendre que la législation entre en vigueur n'est pas une bonne stratégie. Il va leur falloir vérifier que leurs processus d'identification et de signalement des incidents sont efficaces, et surveiller systématiquement l'intégrité des données ; une tâche que complique la multiplication des médias sociaux et des terminaux mobiles.

Les entreprises vont devoir rendre compte d'où se trouvent les informations qu'elles possèdent, de ce qu'elles recèlent, sur quels supports et dans quels formats physiques et électroniques.

En plus des risques financiers, une violation de données peut sérieusement dégrader la réputation d'une société, avec les conséquences dramatiques que cela peut engendrer sur la confiance des clients.

Avec la généralisation des médias sociaux, les réputations se défont plus vite que jamais, au point qu'une violation de données, aussi minime soit-elle, peut occasionner de graves préjudices pour l'entreprise dont la responsabilité serait engagée.

Toutes les entreprises doivent endosser pleinement leur rôle de gardien des informations sensibles. En Europe, elles auraient tout intérêt à faire dès à présent le point sur les règles en place et à s'interroger sur leur capacité à prévenir les pertes de données. Par Christian Toon, directeur de la sûreté des informations et responsable des services de sécurité d'Iron Mountain en Europe.