Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer ! – Data Security BreachData Security Breach

	Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !

La directive européenne de protection des données personnelles est morte ! Vive le règlement général sur la protection des données (GDPR). Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !

En 1995, l'Europe s'équipait de la directive européenne de protection des données personnelles. Mission, protéger les informations des utilisateurs d'informatique. 21 ans plus tard, voici venir le règlement général sur la protection des données (GDPR). La Commission européenne avait proposé en 2012 un nouveau règlement portant sur un ensemble de règles unique pour toutes les données collectées en ligne afin de garantir qu'elles soient conservées de manière sûre et de fournir aux entreprises un cadre clair sur la façon dont les traiter.

Mercredi 13 avril 2016, le paquet législatif a été formellement approuvé par le Parlement dans son ensemble. Le GDPR impose aux entreprises (petites ou grandes) détenant des données à caractère personnel d'alerter les personnes touchées par une fuite, une perte, un piratage de la dire informations privée.

Grand groupe, PME, TPE doivent informer les autorités de contrôle nationales (CNIL) en cas de violation importante de ces données.
Comme je pouvais déjà vous en parler en 2014, il faut alerter les autorités dans les 72 heures après avoir découvert le problème. Les entreprises risquent une grosse amende en cas de non respect : jusqu'à 4% de son chiffre d'affaire. Les informations que nous fournissons doivent être protégées par défaut (Art. 19). A noter que cette régle est déjà applicable en France, il suffit de lire le règlement de la CNIL à ce sujet. Faut-il maintenant que tout cela soit véritablement appliqué.

Fuite, perte, piratage de données
Parmi les autres articles, le « 7 » indique que les entreprises ont l'obligation de demander l'accord « *clair et explicite* » avant tout traitement de données personnelles. Adieu la case par défaut imposée, en bas de page. De l'opt-in (consentement préalable clair et précis) uniquement. Plus compliqué à mettre en place, l'article 8. Je le vois dans les ateliers que je mets en place pour les écoles primaires et collèges. Les parents devront donner leur autorisation pour toutes inscriptions et collectes de données. Comme indiqué plus haut, les informations que nous allons fournir devront être protégées par défaut (Art. 19). Intéressant à suivre aussi, l'article 20. Comme pour sa ligne téléphonique, le numéro peut dorénavant vous suivre si vous changez d'opérateur, cet article annonce un droit à la portabilité des données. Bilan, si vous changez de Fournisseur d'Accès à Internet par exemple, mails et contacts doivent pouvoir vous suivre. L'histoire ne dit pas si on va pouvoir, du coup, garder son adresse mail. 92829@orange.fr fonctionnera-t-il si je passe chez Free ?
La limitation du profilage par algorithmes n'a pas été oublié. En gros, votre box TV Canal +, Orange ou Netflix (pour ne citer que le plus simple) utilisent des algorithmes pour vous fournir ce qu'ils considèrent comme les films, séries, émissions qui vous conviennent le mieux. L'article 21 annonce que l'algorithme seul ne sera plus toléré, surtout si l'utilisateur n'a pas donné son accord.
Enfin, notre vie numérique est prise en compte. Les articles 33 et 34 s'annoncent comme les défenseurs de notre identité numérique, mais aussi notre réputation numérique. L'affaire Ashley Madisson est un des exemples. Votre identité numérique est volée. L'entreprise ne le dit pas. Votre identité numérique est diffusée sur Internet. Vous ne la maîtrisez plus.
Bref, 33 et 34 annonce clairement que les internautes ont le droit d'être informé en cas de piratage des données. La CNIL sera le récipiendaire des alertes communiquées par les entreprises piratées. Bref, fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !
Les entreprises ont jusqu'au 1er janvier 2018 pour se mettre en conformité. Les 28 pays membres doivent maintenant harmoniser leurs lois sur le sujet. Je me tiens à la disposition des entreprises, associations, particuliers qui souhaiteraient réfléchir à leur hygiène informatique.

Police : nouvelles règles sur les transferts de données
Le paquet sur la protection des données inclut par ailleurs une directive relative aux transferts de données à des fins policières et judiciaires. La directive s'appliquera aux transferts de données à travers les frontières de l'UE et fixera, pour la première fois, des normes minimales pour le traitement des données à des fins policières au sein de chaque État membre.
Les nouvelles règles ont pour but de protéger les individus, qu'il s'agisse de la victime, du criminel ou du témoin, en prévoyant des droits et limites clairs en matière de transferts de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales – incluant des garanties et des mesures de prévention contre les menaces à la sécurité publique, tout en facilitant une coopération plus aisée et plus efficace entre les autorités répressives.

« ***Le principal problème concernant les attentats terroristes et d'autres crimes transnationaux est que les autorités répressives des États membres sont réticentes à échanger des informations précieuses*** », a affirmé Marju Lauristin (S&D, ET), députée responsable du dossier au Parlement.
« ***En fixant des normes européennes sur l'échange d'informations entre les autorités répressives, la directive sur la protection des données deviendra un instrument puissant et utile pour aider les autorités à transférer facilement et efficacement des données à caractère personnel tout en respectant le droit fondamental à la vie privée***« , a-t-elle conclu… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertise techniques et judiciaire en litige commercial, piratages, arnaques Internet;
- Expertise de systèmes de vote électronique;
- Formation en cybercriminalité;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.

Contactez-nous

Suivez nous sur

Réagissez à cet article

Source : *Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer ! – Data Security BreachData Security Breach*