Nouvelle réglementation Européenne sur la protection des données personnelles | Le Net Expert Informatique

Comment être prêt à répondre aux exigences de la nouvelle réglementation européenne sur la protection des données personnelles ?

Les apports du projet de règlement UE sur la protection des données personnelles en matière de gestion de crise sont nombreux et les entreprises peuvent d'ores et déjà se préparer à plusieurs niveaux.
Vous êtes le dirigeant d'une entreprise de la grande distribution, vôtre RSSI vous informe que malgré les mesures de sécurité mises en œuvre, l'entreprise est victime d'un vol massif de données clients. Vous avez conscience que c'est impactant pour votre entreprise mais heureusement les législations européennes et françaises, en matière de violation des données à caractère personnel, ne visent que les fournisseurs de communication électronique. Vous êtes épargnés d'un point de vue réglementaire… Certes, mais plus pour longtemps.
Le projet de règlement sur la protection des données destiné à remplacer la Directive 95/46/CE doit actuellement repasser devant la Commission et son adoption ne saurait tarder. Le règlement vise désormais toutes les organisations traitant des données à caractère personnel et en lien avec l'UE (territorial, résidents UE…).
Celui-ci impose notamment, que si les conséquences de la compromission de données, constituent un risque élevé pour les droits et libertés des personnes physiques concernées, l'organisation doit les informer au plus vite. Elle doit aussi en informer les autorités compétentes en matière de protection des données à caractère personnel. Pour ce faire plusieurs actions doivent être réalisées en étroite collaboration avec le soutien du Data Privacy Officer (DPO) de l'organisation.

La qualification de l'incident
L'objectif est de déterminer si le risque est élevé pour les personnes concernées. Pour ce faire il convient en premier lieu de répondre à deux questions :
• Les données volées rendent-elles les personnes concernées identifiables ?
• Les personnes concernées peuvent-elles connaître des conséquences significatives voire irrémédiables (discrimination, vol/usurpation d'identité, perte financière, atteinte à la réputation) ?
A l'issue de cette première phase, si le risque est élevé pour les personnes concernées (données identifiables et conséquences majeures), il faudra procéder à la notification de l'autorité compétente et des personnes concernées.
L'organisation ne sera toutefois pas tenue de notifier les personnes concernées par la violation si :
• Le responsable du traitement a mis en œuvre des mesures de protection technologiques appropriées rendant les données incompréhensibles à toutes personnes non autorisées à y avoir accès (ex : chiffrement) ;
• Ou si la notification risque d'entrainer des mesures disproportionnées eu égard notamment au nombre de cas concernés ;
• Ou si la notification risque de porter atteinte à un intérêt public important.

La notification de l'incident
Pour la notification à l'autorité en charge de la protection des données, la CNIL en France, l'organisation victime de l'attaque dispose d'un délai de 72 heures. Cette notification devra notamment comporter les éléments suivants :
- La nature de la violation
- Le nombre approximatif de personnes et des enregistrements concernés
- La description des conséquences probables de la violation
- La description des mesures prises

Pour la notification aux personnes concernées, celles-ci doivent aussi être averties sans retard injustifié. Trois éléments principaux doivent être communiqués :
- La nature de la violation des données à caractère personnel
- Les mesures prises ou proposées pour remédier à la violation
- Les recommandations afin d'atténuer les effets négatifs de la violation

Durant toute la gestion de la crise ainsi que durant la sortie de crise, le responsable du traitement doit alimenter puis conserver une trace documentaire de la violation des données à caractère personnel en indiquant son contexte, ses effets et les mesures prises pour y remédier. Ce document aura valeur juridique et pourra être opposable.

En parallèle à ces actions, la gestion de la crise comporte également une gestion technique de l'attaque, une campagne de communication de crise afin de sauvegarder la réputation, ainsi qu'une démarche judiciaire et assurantielle notamment si l'organisation a adopté une cyber-assurance.

Le rôle du DPO
En temps de crise, le Data Privacy Officer (DPO) pourra veiller à ce que les mesures adaptées et la notification à l'autorité de contrôle et aux personnes concernées soient réalisées. Il pourra par ailleurs effectuer toutes les procédures requises auprès de la CNIL ainsi que suivre le dossier. En outre, les relations entre le CIL et la CNIL déjà établies en amont de la crise permettent d'alléger les procédures.

L'existence du CIL dans les entreprises peut être ainsi un élément favorisant l'adoption de réponses adaptées en temps de crise et pouvant réduire le montant de la sanction administrative dans le cas où la responsabilité du responsable de traitement ou du sous-traitant est démontrée.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.itpro.fr/a/nouvelle-reglementation-ue-sur-protection-donnees-personnelles/
Par Francesca Serio – Consultante spécialisée en Gestion de crise et Continuité d'Activité – Provadys