RGPD : prendre les mesures qui s'imposent

Cela mérite réflexion

La nouvelle législation imposée par le RGPD entraîne la mise en place de mesures de sécurisation des données personnelles afin d'éviter le vol. Cela va donc avoir un impact budgétaire, mais aussi en terme de procédure interne.

Bon, mais encore ?

Vous devez tenir une documentation interne complète sur les traitements de données personnelles au sein de votre entreprise ou pour le compte de celle-ci, et vous assurer que ces traitements respectent bien les nouvelles obligations légales. Ces obligations impliquent notamment la tenue d'un registre de données personnelles reprenant les informations suivantes :

- les différents types de traitements de données personnelles (collecte, stockage, modification, etc..) ;
- les catégories de données personnelles traitées (nom, prénom, adresse email, téléphone, données de connexion, etc..) ;
- les objectifs poursuivis par les opérations de traitements de données personnelles (gestion de la clientèle, marketing, profilage, newsletter, etc..) ;
- les acteurs (internes ou externes) qui traitent ces données personnelles ;
- les flux en indiquant l'origine et la destination des données personnelles, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.

Une organisation de moins de 250 personnes peut limiter l'objet de son registre à ses traitements habituels de données, comme la gestion des salaires et du personnel. Les traitements occasionnels de données peuvent ne pas figurer dans le registre à moins qu'il ne s'agisse de traitements à risque pour les droits et liberté des personnes concernées ou de traitements de données sensibles au sens large.

Le responsable du traitement des données personnelles doit prendre les mesures nécessaires, tant au niveau technique qu'organisationnel, pour garantir la sécurité des données personnelles traitées.

Les données personnelles doivent être conservées uniquement le temps nécessaire à l'accomplissement de l'objectif qui était poursuivi lors de leur collecte. Les données qui ne présentent plus d'intérêt doivent être supprimées sans délai. En cas de procédure de suppression automatique, vous devez vous assurer que les données sont effectivement supprimées. Des mesures techniques et organisationnelles doivent donc être mises en place afin que cet effacement soit effectif.

Soyons concrets

La protection des données personnelles impose des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Si les données sont stockées, ces mesures de sécurité doivent au moins prendre en compte les précautions élémentaires suivantes :

- mettre en place des outils tels que des pare-feu et des logiciels anti-virus;
- sensibiliser les collaborateurs internes à la manipulation des données personnelles ;
- authentifier les collaborateurs internes ayant accès à des données personnelles ;
- gérer les habilitations ;
- tracer les accès et gérer les incidents ;
- sécuriser les postes de travail ;
- sécuriser l'informatique mobile ;
- protéger le réseau informatique interne et sécuriser les serveurs ;
- sécuriser les sites web ;
- sauvegarder et prévoir la continuité d'activités ;
- protéger les locaux ;
- chiffrer les données personnelles.

Concernant la sécurité informatique, il est conseillé de faire un audit interne afin d'identifier les réels besoins. Ces mesures feront l'objet d'une charte informatique qu'il est recommandé d'annexer au règlement de travail. Ce dernier sera ainsi réputé connu par tout le personnel qui devra s'y référer.

Afin de garantir la confidentialité des données personnelles, il est utile d'inclure, dans vos contrats de travail, une clause d'engagement de confidentialité pour le personnel ayant vocation à manipuler des données personnelles. Enfin, lorsque le stockage des données personnelles est confié à un sous-traitant, vous devez vous assurer, que votre prestataire présente des garanties suffisantes en matière de sécurité et de confidentialité des données personnelles qui lui sont confiées.

Lors de la collecte des données online, cette obligation d'information devra se coupler avec le consentement de l'utilisateur. Il est donc préférable de privilégier l'inscription via un site internet ou une page web dédiée. Dans le cadre du site internet, une politique de respect du RGPD doit être mise en place, notamment en mettant à jour la charte de confidentialité et la politique de cookies.

Retenez bien ceci

En cas de constatation d'une violation de données personnelles, vous devez le notifier à la Commission de la vie privée dans les 72h du constat. L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de ces personnes. Le piratage extérieur est l'exemple le plus connu, mais on peut également pointer la perte d'une clé USB ou d'un ordinateur portable contenant des données à caractère personnel.

Le RGPD impose que les informations suivantes soient communiquées :

- la nature de la violation, si possible en mentionnant les registres de données à caractère personnel concernés et les personnes concernées; le nom et les coordonnées du délégué à la protection des données (DPD) ou un autre point de contact ;

- les conséquences probables de la violation de données à caractère personnel ;
- les mesures proposées par le responsable du traitement pour remédier à cette violation.

Toutefois, s'il est impossible de fournir toutes les informations nécessaires lors d'une seule notification, le RGPD prévoit que ces informations peuvent également être fournies en plusieurs étapes dans un délai raisonnable. Afin d'agir de manière la plus adéquate possible, il convient d'établir, de manière proactive, une politique ou une feuille de route dans laquelle les étapes qui doivent être suivies dans de telles situations sont décrites.

Pour être conforme au RGPD, hormis la définition des procédures de notification de brèches de sécurité, il sera également nécessaire de mettre en place une organisation chargée de traiter les demandes des personnes concernées par la collecte de leurs données personnelles, car elles disposent d'un certain nombre de droits. C'est pourquoi nous recommandons la mise en place d'un service au sein de votre entité permettant de pouvoir répondre aux demandes des personnes concernées. Les informations de contacts de ces services devront être communiquées lors de la collecte des données personnelles.

Les tuyaux du net

- Les conditions de désignation d'un délégué à la protection des données : https://www.privacycommission.be/fr/dossier-thematique-delegue-a-la-protection-desdonnees
- Le guide de la cyber-sécurité : http://static1.squarespace.com/static/55d339cfe4b05cbbf5e4a24e/t/56cb0a56356fb0ec8c2f27ec/1456147034545/CSIMG_2016_FR.pdf
- Un kit cybersecurity : https://www.cybersecuritycoalition.be/resource/cyber-security-kit-french/
- Les documents utiles pour le RGPD sont à retrouver sur : http://attractions-et-tourisme.be/etudes_analyses_sectorielles.html

Le mot : DPD

Le Délégué à la protection des données (DPD) est chargé de mettre en oeuvre la conformité au RGPD au sein de l'organisme qui l'a désigné. Dans votre cas, la désignation d'un DPD n'est a priori pas obligatoire mais rien n'empêche d'en désigner un sur une base volontaire, en respectant les mêmes conditions que dans l'hypothèse d'une désignation obligatoire. Il serait moins contraignant de désigner une personne responsable en interne sans lui donner la qualification de DPD. La désignation d'un DPD est obligatoire quand vos activités de base impliquent le traitement à grande échelle de données sensibles (par exemple un hôpital), ou impliquent un suivi régulier et systématique à grande échelle des personnes concernées (par exemple une entreprise de sécurité sécurisant un site public). Le DPD peut être un membre du personnel de votre organisation ou faire l'objet d'un contrat externe, sur la base d'un contrat de service. Un DPD peut être une personne ou une organisation.

Résumons-nous

- Des mesures très précises sont à mettre en place dans les entreprises pour assurer la sécurisation des données personnelles et réagir adéquatement à leur possible violation.