HARLAY
AVOCATS

ACTUALITÉ JURIDIQUE

Harlay Avocats | Juin 2017 | Données personnelles | Newsletter N°57

Les premières actions vers la conformité au Règlement sur la protection des données personnelles (RGPD)

Les premières actions concrètes à mettre en place dans la perspective d'une mise en conformité au RGPD doivent être prises dès à présent. C'est ce que recommande la CNIL dans un guide publié le 15 mars 2017.

À compter du 25 mai 2018, le Règlement Général sur la Protection des Données (RGPD) sera applicable. Les entreprises vont devoir assurer une protection renforcée des données à caractère personnel. À défaut, les sanctions financières de la CNIL pourront s'élever au maximum à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial consolidé (le montant le plus élevé étant retenu). Dans son guide pratique, la CNIL prévoit les 6 étapes clés suivantes : désigner un pilote, cartographier les traitements de données, prioriser les actions à mener, gérer les risques, organiser les processus internes, documenter la conformité.

Pour se mettre en conformité avec le RGPD, une entreprise pourra structurer sa démarche en réalisant un audit de conformité, désigner un CIL (futur DPO) et rassurer ses clients en obtenant auprès de la CNIL le label Gouvernance.

DPO ou Délégué à la protection des données

Le DPO a pour fonction de piloter et structurer les processus de gestion des données dans l'entreprise. Il pourra s'appuyer sur des relais internes (Relais Informatique et Libertés) dans les différentes lignes métiers de l'entreprise qui lui communiqueront tout nouveau traitement mis en place.

Avant même qu'il soit obligatoire de nommer un DPO et dans le cas même où on ne serait pas soumis à cette obligation, il est fortement recommandé de désigner un Correspondant Informatique et Libertés (CIL). Structurer la gouvernance permet de déterminer les premières actions et de faciliter la sensibilisation en interne. Par exemple, le CIL tiendra un registre des traitements, ce qui deviendra obligatoire pour tout responsable de traitement et sous-traitant dans le cadre du RGPD.

Ce CIL peut être désigné parmi les collaborateurs de l'entreprise s'il justifie de compétences techniques et juridiques en matière de protection des données. L'entreprise peut également choisir d'externaliser la fonction auprès d'un consultant externe ou d'un conseil spécialisé en matière de données personnelles.

Audit de conformité et analyse de risques

Il est recommandé aux entreprises de réaliser un audit de conformité au RGPD pendant cette phase transitoire.
L'audit doit permettre en particulier d'établir une cartographie des données, de recenser les différentes finalités de traitements, d'identifier les utilisateurs, destinataires des données et transferts hors Union européenne, de comprendre les processus relatifs à l'usage, à la conservation et à la destruction de ces données, d'analyser les mesures de sécurité. Ces processus internes devront prévoir notamment de protéger les données dès la conception (minimisation des données traitées au regard des finalités).

Il suppose dans la plupart des cas à tout le moins une consultation de la Direction Générale, de la DSI, du RSSI, du CIL, de la direction des ressources humaines, de la direction marketing et de la direction commerciale.

Les traitements à risques en matière de protection des données feront l'objet d'une analyse de risques et/ou d'impact vie privée. Cette analyse sera obligatoire lors d'un traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques (profiling) ou d'un traitement à grande échelle de données sensibles. Cette analyse permettra aux entreprises d'évaluer ces risques et de mettre en place les mesures (juridiques/sécurité) adéquates pour y faire face.

L'audit s'achèvera par la formalisation de recommandations qui seront présentées à la direction sous la forme d'un plan d'action adapté avec des priorités définies.

Enfin, les entreprises devront tenir une documentation sur leurs procédures internes de gestion des données pour prouver leur conformité au RGPD ("Accountability"). Cette documentation pourra être réalisée en parallèle de l'audit. Les entreprises devront notamment tenir un registre de l'ensemble de leurs traitements, encadrer les transferts de données hors UE (Clauses contractuelles types ou BCR), revoir leurs contrats sous-traitance, leurs formulaires de recueil du consentement des personnes, etc.

Label CNIL Gouvernance

Le RGPD encourageant les labels et certificats de conformité en matière de protection des données personnelles, il est recommandé aux entreprises disposant d'un CIL d'obtenir un Label Gouvernance.

Ce Label est un véritable indicateur de confiance pour les clients et présente un avantage concurrentiel certain.

Pour rappel, ce Label Gouvernance contient des modèles de documents utiles pour la mise en place des procédures internes dans l'entreprise (par exemple, pour l'exercice des droits d'accès, de portabilité, de suppression ou de gestion des incidents de sécurité).

Pour plus d'information ou toute demande, contactez nous à contact@harlaylaw.com.




Harlay Avocats