RGPD Règlement Européen sur la Protection des Données : Voici comment être en règle pour 2018

RGPD Règlement Européen sur la Protection des Données : Voici comment être en règle pour 2018

Le GDPR, règlement européen qui renforce le droit des utilisateurs en matière de données personnelles, entrera en vigueur en mai de l'an prochain. D'ici là, 4 actions doivent être menées.

2017 s'annonce chargé pour toutes les entreprises qui collectent et manipulent, de près ou de loin, de la data en provenance de leurs consommateurs. Pour cause, le nouveau règlement européen sur la protection des données personnelles (GDPR) entrera en application le 25 mai 2018. Son objectif est de renforcer les droits des personnes en la matière… et les obligations des entreprises. Voici comment éviter une amende qui sera salée pour les mauvais élèves : 2 à 4% du chiffre d'affaires ou 20 millions d'euros, le montant le plus élevé étant choisi.

Protéger les données personnelles en amont

Commençons par la bonne nouvelle. L'entreprise qui procède à un traitement de données personnelles n'aura plus à remplir de déclaration auprès de la Cnil pour l'en informer, comme elle y est pour l'instant tenue. Ce pilier de la loi « Informatique et liberté » saute.

« Les entreprises doivent 'en échange' se conformer au concept de « privacy by design » érigé par l'article 25 du règlement », explique Matthieu Berguig, avocat spécialisé en droit des nouvelles technologies. Ce concept leur impose de réfléchir à la protection des données personnelles en amont de la conception d'un produit ou d'un service. « Un fabricant d'objets connectés doit donc se poser des questions de base avant de mettre son produit sur le marché : où son stocké les données, par quel protocole de cryptage seront-elles protégées, sont-elles anonymisées… », illustre Matthieu Berguig. Délestée de ce travail de vérification, la Cnil s'évite beaucoup de paperasse… et gagne du temps pour auditer le marché. « On peut être sûrs que les contrôles seront plus nombreux », prévoit Matthieu Berguig.

Nommer un déléguer à la protection des données

La Cnil pourra travailler dans cette perspective main dans la main avec un collaborateur d'un nouveau genre, le délégué à la protection des données (DPD). L'article 37 impose sa nomination dans plusieurs cas de figure : lorsque « le traitement est effectué par une autorité publique ou un organisme public », lorsque le traitement impose « un suivi régulier et systématique à grande échelle des personnes concernées » ou lorsque le traitement à grande échelle concerne « les catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10« . Beaucoup d'entreprises sont donc concernées par l'obligation et toutes sont encouragées à en nommer un.

Chargé de faire respecter le règlement européen sur la protection des données au sein de l'organisme qui l'a désigné, le DPD tient un peu du mouton à cinq pattes. Chez les entreprises déjà bien structurées, le « compliance officer », le collaborateur qui s'assure de la conformité de toute décision business à la législation, sera un candidat naturel à ce rôle de DPD. « Pour toutes les autres, il faut trouver la perle rare, un profil juridique capable également de comprendre les problématiques métiers », note Alan Walter, avocat associé chez Walter Billet Avocats.

Tenir un registre de traitement des données

« En 2017, beaucoup d'entreprises vont s'embarquer dans une totale remise à plat de leurs systèmes de traitement des données à caractère personnel », note Alan Walter. Pour cause, l'article 30 impose aux entreprises de plus de 250 salariés de tenir un registre des traitements effectués. Un registre qui comporte, entre autres, le nom et les coordonnées du responsable du traitement, les finalités du traitement, la catégorie de destinataires auxquels les données à caractère personnel ont été ou seront communiqués. « C'est ce registre qui sera consulté par la Cnil lorsqu'elle voudra entrer en action », précise Matthieu Berguig.

L'article 33 impose d'ailleurs à une entreprise qui a subi une violation de données à caractère personnel d'en notifier l'autorité de contrôle. « Seuls les opérateurs télécoms y étaient jusque-là tenus », note Matthieu Berguig.

Créer une base interopérable pour le droit à la portabilité

L'article 20 du règlement aboutit à la création d'un droit à la portabilité des données personnelles. Si un de vos clients vous quitte pour la concurrence, il a le droit de réclamer le transfert de l'intégralité des données le concernant. « Lorsque cela est techniquement possible », précise l'article. « En d'autres termes, lorsque vous passerez d'une boîte mail à une autre, vous aurez théoriquement le droit d'importer tout votre historique de mails », illustre Matthieu Berguig. Une obligation dont la mise en place pourrait être techniquement compliquée dans de nombreux cas.

Alan Walter souligne un autre écueil, juridique celui-ci, en prenant l'exemple de l'un de ses clients, courtier en assurance pour expatriés. « Les données qu'il recueille sont très sensibles car elles concernent le domaine médical. Elles ne peuvent être transmises à n'importe qui, du fait du secret médical. Donc comment doit-il faire ? », s'interroge-t-il. Dans ce cas, il faudrait s'assurer que le destinataire des données offre les garanties nécessaires pour qu'il ne soit pas porté atteinte aux droits des personnes concernées. Problématique d'autant plus épineuse avec des transferts de données qui sont susceptibles d'intervenir vers des opérateurs situés hors de l'Union européenne et donc soumis à des droits différents. Premiers éléments de réponse début mai 2018.

Original de l'article mis en page : Protection des données : voici comment être en règle pour 2018

A Lire aussi :

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 dessins

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article