Protection des données : ce qui va changer pour les entreprises en 2018

Protection des données : ce qui va changer pour les entreprises en 2018

En mai 2018, un règlement européen va entraîner d'importants changements dans la pratique des entreprises en matière de gestion des données personnelles. En quoi consistent ces changements et comment s'y préparer ?

Protection des données : ce que prévoit le règlement européen de 2016

Contrairement à une directive, le règlement européen, adopté en 2016, est directement applicable dans l'ensemble de l'Union européenne sans nécessiter de transposition dans les différents Etats membres et ce à partir du 25 mai 2018. Il concerne toutes les entreprises utilisant des données personnelles.
Ainsi, à cette date, les responsables de traitement devront s'être mis en conformité avec le règlement sous peine de sanctions.

Principal changement :
Ce règlement marque le passage d'une logique de « formalités préalables » (déclarations, autorisations) à une logique de « conformité » dont les acteurs seront responsables sous le contrôle du régulateur (la CNIL en France). Ainsi, les responsables de traitements de données n'auront plus à effectuer de déclarations à la CNIL dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes.
Par contre, ils devront d'entrée mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »). Ils devront également être capables de démontrer cette conformité à tout moment.

	Pour les traitements à risque, il faudra toutefois conduire une étude d'impact complète faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Cela concerne notamment les données sensibles qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi les données génétiques ou biométriques. En cas de risque élevé, il faudra consulter la CNIL avant de mettre en œuvre ce traitement, cette dernière pouvant décider de s'y opposer.

Ce règlement renforce par ailleurs les droits des personnes. En effet, chaque personne concernée par les traitements de données va avoir le droit à la mise à disposition d'une information claire, intelligible et aisément accessible et va devoir donner son accord pour le traitement des données. La preuve de ce consentement incombant au responsable de traitement.

Protection des données : mise en place des délégués à la protection des données

Le règlement européen instaure des délégués à la protection des données (DPD). Ce seront les successeurs des correspondants informatique et libertés (CIL) dont plus de 17 700 organismes sont d'ores et déjà dotés en France et dont la mise en place permet de se dispenser de certaines déclarations.
A la différence du CIL, dont la désignation est actuellement optionnelle, la désignation du DPD est obligatoire dans le secteur public et pour les responsables de traitement et les sous-traitants dont les activités principales les amènent :
• à réaliser un suivi régulier et systématique des personnes à grande échelle ;
• à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations pénales et infractions.
Pour les autres, leur désignation est facultative…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Protection des données : ce qui va changer pour les entreprises – Editions Tissot*