

Le RGPD règlement européen de protection des données et les contrats fournisseurs

 <p>Denis JACOPINI</p> <p>VOUS INFORME</p> <p>LCF</p>	<p>Le règlement européen de protection des données et les contrats fournisseurs RDPD,</p>
--	---

Entré en vigueur en mai dernier, le Règlement général sur la protection des données impose de nouvelles règles en matière de gestion des données personnelles. Avec l'obligation pour les entreprises de se mettre en conformité avant mai 2018. Ce qui implique une modification des contrats fournisseurs.

Qui est concerné?

Le RGPD s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. »

Ce règlement s'applique à toute structure (responsable de traitement des données ou sous-traitant) ayant un établissement dans l'Union européenne ou bien proposant une offre de biens ou de services visant les personnes qui se trouvent sur le territoire de l'Union européenne.

Les actions de profilage visant cette cible sont également concernées. Ainsi, alors que la loi Informatique et libertés se basait sur des critères d'établissement et de moyens de traitement, le règlement européen 16-679 introduit la notion de ciblage: le critère principal d'application est désormais le traitement des données d'une personne se trouvant au sein de l'UE.

Qu'est-ce qu'une donnée à caractère personnel?

L'une des difficultés posées par le RGPD va consister à définir les données personnelles concernées. Le règlement stipule qu'il s'agit de « toute information concernant une personne physique identifiée ou identifiable », directement ou indirectement.

Des données indirectement identifiantes, telles qu'un numéro de téléphone, ou un identifiant, sont donc concernées. De même, les données comportementales collectées sur Internet (notamment recueillies dans le cadre d'actions marketing de profilage), si elles sont corrélées à une identité, deviennent des données à caractère personnel.

Selon le traitement appliqué aux données, des informations non identifiantes peuvent ainsi devenir identifiantes, par croisement des informations collectées.

Quelles obligations pour les entreprises?

La loi Informatique et libertés se basait sur du déclaratif initial et des contrôles ponctuels. Le nouveau règlement européen remplace cette obligation de déclaration par une obligation de prouver à chaque moment que l'entreprise protège les données. Dès lors, la structuration même des outils permettant la collecte des données (CRM, DMP, solutions de tracking ou de géolocalisation...), mais aussi les contrats passés avec les fournisseurs et clients sont impactés (voir encadré ci-dessous).

« Le règlement couple des notions techniques et juridiques », souligne Thomas Beaugrand, avocat au sein du cabinet Staub & Associés. Il introduit des nouveaux principes et concepts qui renvoient désormais vers plus de précautions techniques. Par ailleurs, les entreprises ont, entre autres, l'obligation de donner la finalité précise de la collecte des données (il s'agit du principe de minimisation, un des grands principes de la dataprotection, qui impose que seules les données nécessaires à la finalité poursuivie pourront être collectées).

Le RGPD impose également le principe de conservation limitée des données, ainsi que celui de coresponsabilité des sous-traitants et des entreprises en matière de protection de la data, qui permet de distribuer les responsabilités en fonction de la mainmise de chacun sur les données. Cette notion de coresponsabilité doit être intégrée dès maintenant dans les contrats passés avec les fournisseurs: en effet, le sous-traitant désigné par une organisation pour assurer le traitement des données devient, avec le RGPD, coresponsable de la légalité des traitements. Il sera donc tenu d'informer ses clients et de tenir des registres pour recenser les données, ainsi que d'accepter les audits demandés par son client pour s'assurer de la conformité des traitements.

Les sous-traitants concernés peuvent être, par exemple, l'éditeur d'un CRM en ligne, le routeur d'une campagne d'e-mailing, un service de relation client, etc. Le responsable du traitement, de son côté, doit s'assurer que ses fournisseurs ont pris les mesures nécessaires pour assurer la sécurité des données.

Enfin, parmi les changements majeurs, la nomination d'un DPO, ou délégué à la protection des données, qui sera obligatoire dans tout le secteur public, ainsi que dans les structures privées qui font des traitements de données exigeant un suivi régulier et systématique des personnes à grande échelle (dans le secteur du marketing, notamment). Il sera le garant de la conformité au règlement. Quel impact sur les contrats fournisseurs? Pour se mettre en conformité avec le RGPD, les directeurs achats devront veiller à renforcer les contrats passés avec leur fournisseurs...[lire la suite]

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 DRETF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous



Réagissez à cet article

Original de l'article mis en page : Le règlement européen de protection des données et les contrats fournisseurs