# Comment devenir DPO Délégué à la Protection des Données dans le cadre du RGPD, Règlement européen de protection des données ?

| Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | Comment devenir DPO Délégué à la Protection des Données dans le cadre du RGPD, Règlement européen de protection des données ? | | | | |

**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 GRPD 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 responsabilité 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…

**Le délégué à la protection des données**

Le règlement européen consacre la fonction de Délégué à la Protection des Données (DPD ou en anglais DPO) dans les organismes.

Les responsables de traitement et les sous-traitants devront obligatoirement désigner un DPO :

1. s'ils appartiennent au secteur public,
2. si leur activité principale les amène à réaliser un suivi régulier et systématique des personnes à grande échelle,
3. si leur activité principale les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations.

**Les responsables de traitement peuvent opter pour un DPO mutualisé ou externe.**

Véritable « chef d'orchestre » de la conformité en matière de protection des données, le DPO est chargé :

1. d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que ses employés ;
2. de contrôler le respect du règlement et du droit national en matière de protection des données ;
3. de conseiller l'organisme sur la réalisation d'une analyse d'impact (PIA ou EIVP) et d'en vérifier l'exécution ;
4. de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

**QUI PEUT ÊTRE DPO ?**

Le DPO est désigné sur la base de son expertise.

**CONSEILS POUR LA MISE EN PLACE DU FUTUR DPO**

Compte tenu que jusqu'au 25 mai 2018, ne non respect de la Loi Informatique et Libertés est passible de 5 ans de Prison et jusqu'à 300 000 euros d'amende, nous vous conseillons fortement d'entamer au plus vite les démarches suivantes déclarer un CIL avant le 25 mai 2018 ou désigner un DPO après. Puis :

1. Réaliser ou faire réaliser un indispensable état des lieux (appelé aussi audit) afin d'identifier l'ensemble des traitements de données personnelles et l'ensemble des lieux dans lesquels des données personnelles sont traitées ;
2. Identifier dans la Loi Informatique et Libertés ou dans le RGPD des particularités propres à votre métier qui vous autorise à certains traitements interdits à d'autres activités ou qui nécessiteraient une demande d'autorisation ;
3. Faire une analyse de risque autour des traitements et des données personnelles présentes dans votre établissement.  Cette étape indispensable peut être assurée par notre Expert Denis JACOPINI, Certifié ISO 27005 Risk Manager ;
4. Porter au registre l'ensemble des traitements identifiés ;
5. Mettre en conformité les traitements qui ne respectent pas la loi ou le règlement.
6. Suivre régulièrement l'évolution des traitements au sein de l'organisme.

**Articles du règlement associés**

Article 13 | Article 14 | Article 30 | Article 33 | Article 35 | Article 36 | Article 37 | Article 38 | Article 39 | Article 47 | Article 57

**Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.**

---

**Besoin d'un expert pour vous mettre en conformité avec le RGPD ?**

Contactez-nous

---

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

*« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».*

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

**Quelques articles sélectionnés par nos Experts :**

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

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

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

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

---

Réagissez à cet article

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