Mise en conformité RGPD : Mode d'emploi

Mettre un établissement en conformité avec le RGPD nécessite la réalisation de certaines tâches plus techniques et organisationnelles que juridiques, même si ce dernier domaine doit aussi être maîtrisé par le DPO (Data Protection Officer).

Une mise en conformité nécessitera donc une excellente connaissance en matière de sécurité informatique, d'analyse de risques, d'organisation des services, de transferts de flux de données et enfin de pédagogie pour que l'ensemble des employés de l'établissement comprenne le but de la démarche pour devenir acteur.

Les étapes à respecter sont :

1. Établir une cartographie de l'ensemble des traitements de données de l'entreprise ou de l'entité publique ;
2. Vérifier les spécificités et dispenses propres à l'activité ou au statut de l'établissement ;
3. Analyser chaque traitement de données en profondeur pour vérifier sa conformité avec le règlement ;
4. Tenir un registre dans lequel seront référencés les différents traitements des données à caractère personnel conformes et à modifier ;
5. Tenir compte de l'évolution de l'entreprise et s'assurer que la conformité est maintenue dans le temps.

Ne pas oublier que le RGPD prévoit l'obligation de déclarer une faille, entraînant une fuite ou un vol de données personnelles, auprès de l'autorité de contrôle dans les 72 heures suivant l'incident. Le DPO pourra accompagner l'établissement dans la gestion de ces incidents.
Enfin, le DPO devra traiter les demandes d'accès à ses données personnelles, formulées par exemple par un client.

Le DPO obligatoire pour qui ?

Le Règlement général sur la protection des données (RGPD), qui sera effectif le 25 mai 2018, rend obligatoire la nomination d'un Data Protection Officer (DPO) pour les entités publiques et certaines entreprises. « *Ce délégué à la protection des données sera au cœur du nouveau cadre juridique européen* », résume le groupe de travail G29, qui réunit les « Cnil européennes ». La nomination d'un DPO sera donc incontournable pour toutes les entités publiques du Vieux Continent, telles que les collectivités locales, les hôpitaux, les universités… Côté entreprises, le DPO sera obligatoire pour celles dont l'activité principale les amènent à réaliser à grande échelle un suivi régulier et systématique des personnes (profiling), ou de traiter des données «sensibles» – santé, opinions politiques ou religieuses, orientation sexuelle, etc. – ou des données relatives à des condamnations et infractions pénales.

Parmi les entreprises qui devraient être concernées par cette obligation : des sociétés d'e-commerce ou de marketing digital, des banques et assurances, des établissements de soins ou encore des entreprises du secteur des télécoms.

« *Même lorsque le RGPD n'exige pas spécifiquement la nomination d'un DPO, les entreprises pourront parfois estimer utile d'en désigner un sur une base volontaire* », poursuit le G29. Car en effet, le nouveau règlement européen renforce très sensiblement les responsabilités des entreprises en matière de protection des données personnelles et surtout les sanctions. En France, le plafond maximal des sanctions de la Cnil est déjà passé de 150000 euros à 3 millions d'euros avec la Loi pour une république numérique de 2016. Les amendes prévues par le RGPD peuvent quant à elles atteindre 20 millions d'euros ou 4% du chiffre d'affaires mondial. De quoi inciter de nombreuses entreprises à nommer un DPO pour s'assurer de leur conformité avec le nouveau règlement.

Le DPO comment ?

Le premier travail d'un DPO sera d'établir une cartographie de l'ensemble des traitements de données de l'entreprise ou de l'entité publique. Pour cela, le DPO devra se rapprocher des représentants des différentes instances de l'organisation pour rassembler les informations nécessaires. Une fois cette cartographie réalisée, le DPO analysera chaque traitement de données en profondeur pour vérifier sa conformité avec le règlement.

Le DPO combien ?

Il n'existe pas encore de grille salariale établie pour le DPO, ses revenus devraient être au moins comparables à ceux du CIL, soit environ 50000 euros par an. La pénurie attendue de candidats au poste de DPO devrait même tirer les salaires vers haut. La Cnil prévoit que plus de 80000 organisations, publiques ou privés, devront se doter d'un DPO en France.

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.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

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 :

Nous animons des Formations sur le RGPD en individuel ou en groupe

Nous vous accompagnons dans la mise en conformité RGPD de votre établissement

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)

[block id="24761" title="Pied de page HAUT"]

Source : Denis JACOPINI et *Data Protection Officer : un gardien pour les données personnelles*