L'ECLAIRAGE DU MARDI

par

COMETH CO CONSULTING

Règlement Général sur la Protection des Données Personnelles — Mardi 28 mars 2017

Le nouveau Règlement Européen sur la Protection des Données personnelles « **RGPD** » entrera en application le **24 mai 2018**. Cette réforme poursuit trois objectifs :

- Renforcer les droits des personnes ;
- Responsabiliser les acteurs traitant des données physiques ;
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités compétentes.

Nouvelles obligations et responsabilités

- **Renforcement du contrôle des citoyens européens sur l'utilisation de leurs données personnelles :**

  - Consentement : toute personne a le droit d'accepter ou non que ses données à caractère personnel fassent l'objet d'un traitement. Son consentement doit être « explicite » et « positif ».
  - Profilage : toute personne a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage.
  - Portabilité : toute personne a le droit de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et le cas échéant, de les transférer ensuite à un tiers.
  - Droit à l'oubli : toute personne a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, des données à caractère personnel la concernant.

- **Sécurisation des données :**

Le Règlement renforce les obligations du **Responsable de traitement** dans la sécurisation des données pour prévenir, le plus en amont possible, l'atteinte aux droits des personnes :

  - Protection des données dès la conception : Il doit mettre en œuvre des mesures techniques et organisationnelles appropriées à la protection des données. Ces mesures portent notamment sur la pseudonymisation[1] et des moyens garantissant la confidentialité, l'intégrité et la disponibilité de ces données.

[1] Définition : Il s'agit d'un processus par lequel les données perdent leur caractère nominatif.

- Protection des données par défaut : Il doit garantir que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont recueillies et traitées. De plus, il est garant de la limitation des accès aux données personnelles.
- Analyse des risques et études d'impacts : Pour tout traitement susceptible d'entraîner un risque, une étude d'impact PIA « Privacy Impact Assessment » doit être effectuée. Il est nécessaire d'évaluer la données régulièrement durant son cycle de vie.

- **Désignation d'un DPO « Data Protection Officer » :**

Cette nouvelle fonction clé au sein des entreprises sera chargée :

- D'informer et de conseiller le responsable de traitement ou le sous-traitant ;
- De contrôler le respect du règlement et du droit sur la protection des données ;
- De conseiller l'organisme sur la réalisation de PIA et d'en vérifier l'exécution ;
- De coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

- **Traçabilité documentaire :**

Pour assurer une protection des données en continu, il est demandé de formaliser et d'assurer la mise à jour régulière :

- De la documentation sur les traitements traitant de données personnelles ;
- De l'information des personnes : les mentions d'information, les modèles de recueil du consentement des personnes et les procédures mises en place pour l'exercice des droits ;
- Des contrats qui définissent les rôles et les responsabilités des acteurs.

- **Notification des violations des données à caractère personnel :**

Le responsable de traitement est tenu de notifier une violation de données à caractère personnel à l'autorité de contrôle **72 heures au plus tard** après en avoir pris connaissance. S'il ne respecte pas ce délai, il devra préciser les motifs du retard.
Quant à l'information de la personne concernée, elle doit se faire dans les meilleurs délais lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique.

Démarche de préparation à l'application du RGPD

Un processus en six étapes pour s'y préparer :

Source : CNIL https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

Moins de formalités, mais des sanctions plus importantes

Le règlement va remplacer et/ou faire évoluer de nombreuses formalités auprès de la CNIL. En contrepartie, la responsabilité des organismes sera renforcée et les régulateurs auront le pouvoir d'appliquer des sanctions financières allant **jusqu'à 4 % du chiffre d'affaires mondial annuel** d'une entreprise ou **20 millions d'euros** (le montant le plus élevé étant retenu), en cas de non-respect.

Rendez-vous mardi prochain pour un nouvel éclairage