

# Le Règlement Général sur la Protection des Données (RGPD)

## 1. Contexte général

Le règlement européen relatif à la protection des données à caractère personnel, et la directive qui lui est associée et qui porte sur les données pénales à caractères personnel, entreront en vigueur le 25 mai 2018. Le règlement prévoit de nouvelles règles qui modifient substantiellement le régime des formalités préalables. Ces modifications ont notamment pour conséquences de mettre à la charge des responsables de traitement de nouvelles obligations, suivant une double logique :

- une responsabilisation accrue, dans l'idée d'un contrôle interne et avec soutien d'un « tiers », le délégué à la protection des données ;
- le renforcement des contrôles a posteriori par l'autorité de régulation.

En particulier, le règlement impose :

1. l'élaboration par le responsable de traitement d'un registre recensant l'ensemble des traitements mis en oeuvre au sein de l'organisme ;
2. la réalisation d'analyse d'impact pour les traitements les plus sensibles et présentant des risques pour les droits et les libertés des personnes physiques ;
3. l'évaluation des traitements les plus sensibles ou des traitements modifiés à échéances régulières ;
4. une limitation des consultations préalables de la CNIL ;
5. l'obligation, pour le responsable de traitement, de notifier à la CNIL toute violation de données à caractère personnel ;
6. la mise en oeuvre par le responsable de traitement de toutes mesures techniques et organisationnelles de nature à garantir que les traitements sont effectués conformément aux prescriptions des règlement et directive ;
7. la désignation d'un délégué à la protection des données (DPD), chargé d'aider le responsable de traitement et les employés traitant des données à caractère personnel en les informant et en les conseillant sur le respect des obligations leur incombant en matière de protection des données et assistant le responsable de traitement sur l'ensemble des points ci-dessus.

## 2. La mise en oeuvre

### 2.1 Dispositions générales

- Le RGPD s'impose à toutes les organisations qui traitent des données à caractère personnel de ressortissants des Etats membres de l'UE. Au sein de l'UE, il se substitue aux législations nationales existantes en applications de la directive EU 96/46/EC .

- Il introduit des dispositions beaucoup plus strictes, notamment autour des points suivants :
  - Le rôle du DPD (« délégué à la protection des données »)
  - Les signalements des violations de données
  - Le consentement et le droit à l'oubli des personnes concernées
  - Une responsabilité et des amendes accrues : Ces amendes peuvent désormais atteindre jusqu'à 20 millions EUR ou 4% du chiffre d'affaire mondial (le montant le plus élevé sera retenu) pour les violations critiques, et jusqu'à 10 millions EUR ou 2% du chiffre d'affaire mondial (le montant le plus élevé sera retenu), pour les autres violations individuelles

## 2.2 Points d'application du règlement pour la DGAC

- Réaliser un inventaire et une cartographie des données
- Elaborer un registre des traitements des données
- Définir un système de gouvernance pour limiter les atteintes aux données
- Désigner un correspondant du délégué à la protection des données du ministère: Un rôle complexe et transverse car il doit disposer de compétences juridiques sur les règles de protection des données, mais aussi des connaissances en matière de SSI, une connaissance de l'évaluation et de la gestion des risques et une capacité à coopérer avec l'autorité de contrôle
- Organiser la protection des données par la gestion des risques
- notifier obligatoirement toute faille de sécurité à la CNIL dans un délai de 72 h

Pour la DGAC, le RGPD constitue un important chantier de transformation qui vient d'être lancé.

Le sujet ne se restreint pas à la mise en conformité car la DGAC devra assurer cette conformité dans la durée, dans un contexte où la législation évoluera et se durcira certainement ; **Le travail à fournir est donc considérable** ; cependant, on peut aussi voir le RGPD comme une vraie opportunité pour lancer une action autour de la protection des données personnelles et de la sécurité.