Uranie
L'informatique à vos côtés

RGPD Etape 1 : Désigner un Pilote

Il faut désigner une personne chargée de réaliser une cartographie des traitements de données personnelles :
o Désignation d'une personne chargée de ces questions.
o Obligation de désigner un Délégué à la protection des données personnelle DPO :

- Pour les autorités et organismes publics (ministères, collectivités territoriales, établissements publics).

- Pour les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle (compagnies d'assurance ou les banques pour leurs fichiers clients, opérateurs téléphoniques ou fournisseurs d'accès internet).

- Pour les organismes dont les activités de base les amènent à traiter à grande échelle des données dites "sensibles" (données biométriques, génétiques, relatives à la santé, la vie sexuelle, l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale) ou relatives à des condamnations pénales et infractions.

- Possibilité de désigner un DPO mutualisé ou externe.

Uranie
L'informatique à vos côtés

RGPD Etape 2 : Cartographier

Il faut faire un audit des traitements de données personnelles existants dans votre structure :

o **Inventaire des traitements de données personnelles actifs**.

- o Objectifs :
  - Evaluer les pratiques et les écarts avec la réglementation : cette étape permet souvent de « découvrir » certaines pratiques.
  - Identifier les risques associés à ces opérations.
  - Arrêter un plan d'action pour remédier aux éventuels écarts.

Appréciation des risques :Si identification de traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées.

- Réalisation obligatoire d'une ***étude d'impact sur la protection des données*** (PIA).
- Consultation de l'autorité de protection des données avant de mettre en œuvre ce traitement qui pourra s'y opposer.

Que contient une étude d'impact sur la protection des données (PIA) ?

- Une description du traitement et de ses finalités.
- Une évaluation de la nécessité et de la proportionnalité du traitement.
- Une appréciation des risques sur les droits et libertés des personnes concernées.
- Les mesures envisagées pour traiter ces risques et se conformer au RGPD.

Modèles et guides pour réaliser une PIA sur le site de la CNIL

Uranie
L'informatique à vos côtés

RGPD Etape 3 : Prioriser

Il faut réaliser un audit technique et un audit des prestataires :

o Objectifs :

- Evaluer le niveau de sécurité des applications vous permettant de gérer ces données.
- Evaluer le niveau de sécurité et de conformités des sous-traitants impliqués dans le traitement de ces données.
- Identifier les risques.
- Définir les améliorations nécessaires.

Cela ne concerne bien évidemment pas que les traitements informatiques. Les données papiers, le stockage des archives sont également concernés.

Uranie
L'informatique à vos côtés

RGPD Etape 4 : Gérer les risques

Déterminer les actions à mettre en œuvre pour respecter la nouvelle réglementation.

Si l'audit fait apparaître des défaillances, il est impératif de vérifier :

- Que seules les données strictement indispensables à la poursuite du traitement sont collectées.
- Que la base juridique sur laquelle se fonde le traitement est identifiée : contrat, obligation légale, consentement de la personne.
- Que les mentions d'information doivent être conformes aux exigences de la règlementation.
- Que les sous-traitants connaissent leurs (nouvelles) obligations et responsabilités : vous pouvez trouvez sur le site de la CNIL des modèles de clauses contractuelles rappelant les obligations du sous-traitants.
- Que les modalités d'exercice des droits des personnes ont été prévues : droits d'accès, de rectification, de portabilité de retrait du consentement…
- Que les mesures de sécurité techniques sont mis en place.

Une vigilance particulière doit être portée sur les traitements :

- Portant sur des données sensibles (santé, concernant des mineurs…).
- Portant sur des données de vidéo surveillance.
- Portant sur l'évaluation systématique et approfondie d'aspects personnels permettant la prise de décisions (profilage).
- Transférant des données hors de l'Union européenne.

Uranie
L'informatique à vos côtés

RGPD Etape 5 : Organiser

Mettre en place un registre des traitements (si nécessaire) :

Le registre est obligatoire pour les entreprises de plus de 250 salariés

ou

Lorsque le traitement effectué est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel, ou s'il porte notamment sur des données sensibles ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions.

Des modèles de registre sous Excel sont accessibles sur le site de la CNIL. Des modèles de déclaration CNIL peuvent également vous aider pour déterminer les finalités des traitements.

Un registre des traitements doit avoir la mention, pour chaque traitement recensé, de :

Qui : responsable du traitement.
Quoi : catégories de données traitées, données pouvant soulever des risques (santé par exemple).
Pourquoi : finalités du traitement.
Où : lieu d'hébergement des données et éventuellement pays de transit.
Jusqu'à quand : durée de conservation des données.
Comment : mesure de sécurité mise en place pour minimiser les risques d'accès.

Uranie
L'informatique à vos côtés

RGPD Etape 6 : Documenter

Organiser les procédures internes et documenter les actions :

Définir les procédures mises en place pour assurer le « bon usage » des données tout au long des traitements.

Documenter : nécessité de prouver la conformité à la CNIL en cas de contrôle.

Actualiser les documentations et les procédures en cas d'évolution des traitements.