LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Le RGPD en quelques mots…

- En vigueur depuis le **25 mai 2018**,
- En tant que règlement, il impose un cadre juridique unique au sein de l'Union Européenne tout en permettant quelques variations propres à chaque État[1].
- Encadre les traitements de données à caractère personnel des organisations publiques et privées,
- Responsabilise les personnes qui traitent de la donnée à caractère personnel (responsables de traitement et sous-traitants),
- Renforce les droits des personnes afin qu'elles puissent mieux maîtriser les données les concernant,
- Renforce les sanctions en cas de non-conformité.

A - Quel est l'intérêt du RGPD ?

La mise en œuvre du RGPD dans votre structure est l'occasion de :

- améliorer votre image en mettant en avant une éthique des données à caractère personnel au sein de votre structure,
- établir une relation de confiance avec les personnes qui vous confient leurs données à caractère personnel,
- fiabiliser vos données en les mettant à jour,
- optimiser vos données en identifiant les données réellement utiles à la réalisation de traitements,
- avoir une vision globale de l'ensemble des traitements manipulant des données personnelles au sein de votre structure et des données concernées ;
- améliorer la sécurité des données à caractère personnel,
- améliorer les risques liés à la sous-traitance des données à caractère personnel.

B - Qui est concerné par le RGPD ?

- Toute organisation publique ou privée **établie dans l'Union Européenne** qui traite des données à caractère personnel, que ce soit pour son propre compte ou non, et quel que soit le lieu de résidence des personnes concernées.

  Exemples :

  - une administration française traitant des données à caractère personnel de résidents français
  - une société établie en France qui collecte des données de personnes situées en dehors de l'Union Européenne

- Les organisations publiques ou privées établies en dehors de l'Union Européenne qui traitent des données à caractère personnel **relatives à des personnes situées sur le territoire de l'Union Européenne**, que ce soit pour son propre compte ou non.

  Exemple :

  - une société établie en dehors de l'Union Européenne proposant un site de e-commerce en français et livrant des produits en France.

1 Article 6-2 du RGPD

C - Les étapes à suivre pour se conformer au RGPD

Les étapes précisées dans la suite de ce chapitre sont susceptibles d'avoir déjà été déclinées au sein de votre organisation. Il convient de prendre les renseignements nécessaires à ce sujet avant de les adapter à votre propre niveau.

1. Désigner un délégué à la protection des données (DPD)

Les autorités publiques sont dans l'obligation de désigner leur DPD[2]. Son rôle consiste à accompagner l'autorité publique dans sa conformité au RGPD (voir la fiche « Rôle du DPD »).

2. Tenir un registre des traitements à jour[3]

⇨ Dans quel cas le registre est-il obligatoire ?

- Toujours si vous comptez plus de 250 employés
- Si vous comptez moins de 250 employés, les seuls traitements de données suivants doivent être inscrits à votre registre :
  - les traitements non occasionnels,
  - les traitements susceptibles de présenter un risque pour les droits et libertés des personnes concernées,
  - les traitements qui portent sur des données sensibles (santé, infractions…)

⇨ Que doit contenir ce registre au sens de l'article 30 du RGPD ?

- La première page doit recenser l'ensemble des traitements mis en œuvre.
- La suite du registre doit détailler chaque traitement en indiquant les informations suivantes :
  - Nom et coordonnées du responsable de traitement,
  - Nom et coordonnées du délégué à la protection des données (DPD),
  - La finalité du traitement : *décrire pourquoi vous collectez ces données à caractère personnel,*
  - Les catégories de personnes concernées : *lister le type de personnes concernées par la collecte,*
  - Les catégories de données personnelles : *identification, vie privée, vie professionnelle, données financières, données de connexion, données de localisation…,*
  - Identifier si des données sensibles sont collectées : *santé, condamnation pénales ou infractions, convictions religieuses ou philosophiques, données génétiques, données biométriques, données concernant la vie sexuelle, données relatives à l'origine raciale ou ethnique, données relatives à l'appartenance syndicale,*
  - Les catégories des destinataires auxquels les données à caractère personnel ont été ou seront communiquées (en interne et en externe), y compris les sous-traitants auxquels vous faites appel.

    À recenser : les contrats passés avec vos sous-traitants ou avenant au contrat avec vos sous-traitants.
  - Les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale : *indiquer dans quels pays ces transferts ont lieu et prévoir des garanties spécifiques pour certains pays.*

    À recenser : les documents liés aux transferts justifiant des garanties prises (clauses contractuelles…)

2 Article 37 du RGPD
3 Article 30 du RGPD

- Durée de conservation des données : *indiquer la durée de conservation et justifier le choix de cette durée ; il convient de respecter les recommandations émises par la CNIL pour certains traitements.*
- Description générale des mesures de sécurité techniques et organisationnelles mises en œuvre : *contrôle d'accès des utilisateurs, mesures de traçabilité, mesures de protection des logiciels, sauvegarde des données, chiffrement des données.*

À recenser : historique des violations de données

⇨ **Conseil : enrichir son registre pour en faire un outil de pilotage :**

- Indiquer la base juridique du traitement : consentement, contrat, obligation légale, exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.

À conserver en fonction des cas : preuve du consentement ; contrat, avenant au contrat…

3. Effectuer une étude d'impact sur la protection des données :

Une étude d'impact doit être réalisée pour les traitements présentant des risques élevés pour les droits et libertés des personnes physiques.

Elle a pour objet de déterminer si le traitement de données personnelles respecte la vie privée. À ce titre, elle doit contenir :

- 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 règlement.

Si vous disposez d'une autorisation CNIL en cours de validité pour votre traitement, cette autorisation vaut étude d'impact jusqu'à réalisation de celle-ci.

4. Informer les personnes :

- Prévoir pour chaque traitement les mentions d'information nécessaires au regard des dispositions du RGPD[4].
- Si vous devez recueillir le consentement de la personne afin de pouvoir collecter ses données, vous devez conserver la preuve de ce consentement.
- Déterminer la procédure afin de répondre aux réclamations et aux demandes des personnes quant à l'exercice de leurs droits d'accès, de rectification, d'opposition, de portabilité, retrait de consentement.

5. Mettre en place une procédure de violation de données

Déterminer la procédure à mettre en place en cas de violation de données : notification à l'autorité de protection des données dans les 72h et aux personnes concernées dans les meilleurs délais.

6. Responsabiliser vos sous-traitants

Si vous faites appel à un sous-traitant, les contrats doivent définir les rôles et les responsabilités de chacun au regard du RGPD.

À ce titre, vous devez conserver les contrats de sous-traitant.

Ces derniers feront partie de votre dossier de conformité.

4 Article 13 et 14 du RGPD

Organisation pour le MTES et le MCTRCT

Les responsables de traitement de données à caractère personnel sont invités à saisir la direction des affaires juridiques (bureau AJAG 1-2 : ajag1-2.daj.sg@developpement-durable.gouv.fr) de notre pôle ministériel (MTES-MCTRCT) en informant de leur saisine le correspondant privilégié du délégué à la protection des données ministériel de leur structure.

S'agissant des traitements effectués par les directions départementales interministérielles, les traitements en lien avec une politique publique portée par notre pôle ministériel sont mis en œuvre sous la responsabilité du ministre en charge de ces politiques. Ces traitements seront instruits par la direction des affaires juridiques en lien avec le délégué à la protection des données ministériel (Directeur/Directrice des affaires juridiques).