Règlement général sur la protection des données

Une actualité forte

- Depuis le 25 mai 2018, le règlement européen sur la protection des données est applicable.

- De nombreuses formalités de la CNIL ont disparu. En contrepartie, la responsabilité des organismes a été renforcée.

  - Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE (RGPD).

Qu’est-ce qu’une donnée personnelle?

- Le RGPD définit une donnée personnelle comme étant « *toute information se rapportant à une personne physique identifiée ou identifiable (…) directement ou indirectement* ».

Qui est concerné?

Toute entité qui détient des données personnellement identifiables sur les citoyens européens, même les entités en dehors de l’Europe.

Le RGPD s’applique :

- Aux traitements effectués par le responsable de traitement ou le sous traitant établis sur le territoire de l’UE
- Aux traitements effectués pour le compte du responsable de traitement ou du sous traitant non établis sur le territoire de l’UE dès lors qu’ils visent des personnes se trouvant sur le territoire de l’UE

Quelles mesures mettre en œuvre ?

- **1) Recensez vos fichiers**

Identifiez les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données (exemple : gestion de la paie, recrutement etc.). Appuyez vous sur le modèle de registre proposé par la CNIL sur son site internet https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf. Dans votre registre, créez une fiche pour chaque activité recensée en précisant, la finalité, la catégorie de donnée, les personnes qui ont accès aux données, la durée de conservation des données.

- **2) Faites le tri dans vos données**

Pour chaque fiche de registre créée, vérifiez :

- que les données sont nécessaires à vos activités
- que vous ne traitez pas de données dites « sensibles » ou si tel est le cas, que vous avez bien le droit de les traiter
- que seules les personnes habilités ont accès aux données dont elles ont besoin
- que vous ne conservez pas vos données au-delà de ce qui est nécessaire

- **3) Respectez les droits des personnes**

Obligation de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, etc.)

- **4) Sécurisez vos données**

Vous êtes tenu d'assurer la sécurité des données personnelles que vous détenez en minimisant les risques de pertes de données ou de piratage (mettez à jour les antivirus, logiciels, changez régulièrement de mot de passe etc.).

La licéité du traitement de données

- Le traitement de données n'est licite que si au moins une des six conditions suivantes est remplie :

  - La personne concernée à consenti au traitement de ses données personnelles pour une ou plusieurs finalité(s) spécifique(s).
  - Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.
  - Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.
  - Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.
  - Le traitement est nécessaire a l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.
  - Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données personnelles, notamment lorsque la personne concernée est un enfant.

Les sanctions

- Les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités.

- Le détournement de finalité est pénalement sanctionné (article 226-21 du Code pénal) par 300 000 euros d'amende et 5 ans d'emprisonnement
  Par ailleurs, le RGPD prévoit des sanctions à hauteur de 4% du chiffre d'affaire ou 20 millions d'euros (le montant le plus élevé étant retenu).

Les liens utiles

- https://www.cnil.fr/fr/reglement-européen-protection-données
- https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf
- https://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf
- https://www.cnil.fr/fr/rgpd-un-logiciel-pour-realiser-son-analyse-dimpact-sur-la-protection-des-donnees-pia
- https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique
- https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo