Comprendre le RGPD et ses conséquences

Le Règlement Général pour la Protection des Données est un règlement européen, applicable depuis le 25 mai 2018, qui a été traduit en droit français le 20 juin 2018, et applicable immédiatement, sous le contrôle de la CNIL.

Ce règlement a pour but de protéger les personnes physiques de toute utilisation abusive de données les concernant. Il remplace la loi « Informatique et Liberté » qui était en application depuis 1978.

Les principes majeurs de ce règlement sont les suivants :

- Chaque entreprise européenne doit se mettre en conformité pour l'ensemble des données personnelles qu'elle manipule. Il ne s'agit pas d'une certification qui porte sur les logiciels ou les outils utilisés par l'entreprise mais bien un travail et une **responsabilité de l'entreprise**. Pour preuve, même les informations détenues dans des dossiers « papier » sont concernées.
- **Une donnée personnelle c'est** :
    - Ce qui permet d'identifier précisément une personne : nom, prénom, téléphone, email, numéros d'identification pour l'administration, la sécurité sociale …
    - Toute donnée attachée à une personne identifiable : adresse personnelle, données physiques, physiologiques, économique, culturelle, voix, image …
    - Certaines données personnelles sont aussi qualifiées de « sensibles » (santé, judiciaire, religion, ethniques …) et ne doivent pas être conservées sauf pour raisons légales et explicites
- Chaque entreprise, quelle que soit sa taille et son métier, doit s'engager à :
    - **Identifier toutes les données personnelles** qu'elle détient et tenir un registre des objectifs ou finalités qui en justifient la conservation ➔ *registre des données personnelles, registre des traitements et des finalités, des durées de conservation nécessaires, et suppression de toutes les données ou traitements non justifiables*
    - **Sécuriser ces données** pour éviter qu'elles ne soient utilisées à d'autres fins ou diffusées à d'autres que les utilisateurs légitimes ➔ *sécurisation technique et sécurisation des procédures, y compris des sous-traitants (outils ou structures qui traitent des données personnelles pour le compte de l'entreprise)*
    - **Obtenir le consentement** explicite des personnes concernées après les avoir informées de ces finalités et des données concernées, et être capable de rectifier, supprimer ou restituer les données personnelles à la demande d'une personne concernée ➔ *consentement explicite, droit à l'oubli, portabilité*
    - **Informer** rapidement la CNIL et toutes les personnes concernées en cas d'incident générant une diffusion non contrôlée de ces données (piratage…) ➔ *devoir d'information en moins de 72 heures*
- Pour mener à bien ce projet, dans l'entreprise, il faut au minimum désigner un référent qui gèrera ce projet, et éventuellement un DPO (Data Protection Officer = responsable des données personnelles) si le métier de l'entreprise consiste à traiter à grande échelle des données personnelles.

Charte des engagements AGIRIS pour le RGPD

Pour la conformité d'AGIRIS, et pour faciliter la mise en conformité de nos clients, nous nous engageons à mettre en œuvre et garantir dans la durée les pratiques suivantes :

1. Actualiser la **cartographie** de nos propres outils liés aux traitements de données personnelles
2. Mettre en place un **registre des traitements** dans notre entreprise
3. **Respecter nos engagements contractuels de responsable des traitements ou sous-traitant** liés au traitement des données personnelles dans le cadre du RGPD
4. **Collecter les données personnelles dans le cadre légal**
5. **Notifier toute violation de données**, une fois le périmètre impacté identifié
6. Prendre les mesures nécessaires pour vous **garantir un niveau de sécurité des données et des traitements** adaptés aux risques
7. Permettre aux personnes dont les données personnelles sont collectées de **faire valoir leurs droits** (accès, rectification, portabilité) – L'adresse dataprivacy@agiris.fr a été créée pour permettre aux personnes concernées de faire valoir leur droit auprès d'AGIRIS.
8. **En tant qu'éditeur de logiciels** :
    - Veiller à ce que les personnes autorisées à traiter des données personnelles soient engagées contractuellement à une obligation de confidentialité
    - Intégrer des fonctions renforçant la sécurisation des données dans les évolutions des logiciels (cryptage de données sensibles s'il y a lieu, contrôle des droits des utilisateurs…)
    - Simplifier les opérations dans les logiciels permettant d'assurer la portabilité des données ou le droit à l'oubli
    - Produire des documentations destinées à nos clients pour leur faciliter l'établissement de leur propre registre des traitements (pour les données concernées dans chaque logiciel)
9. **En tant qu'hébergeur de systèmes informatiques**
    - Veiller à ce que les personnes ayant accès à des données personnelles soient engagées contractuellement à une obligation de confidentialité
    - Informer et contractualiser tout recours à un sous-traitant ultérieur en nous assurant qu'il présente des garanties suffisantes pour la protection des données personnelles
    - Respecter le cadre légal imposé en cas de recours à un sous-traitant
    - Garantir l'absence de transmission d'informations hébergées à des tiers et qui ne serait pas prévue contractuellement

J'utilise un logiciel AGIRIS : que dois-je faire ?

1. PRENDRE CONNAISSANCE DE LA RÉGLEMENTATION.

Des documents simples et clairs sont publiés par la CNIL pour faciliter la compréhension de cette réglementation.

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

https://www.cnil.fr/rgpd-notions-cles-et-bons-reflexes

https://www.cnil.fr/rgpd-passer-a-laction

2. CRÉER VOTRE REGISTRE DES TRAITEMENTS

L'essentiel est d'identifier les données personnelles détenues sur les salariés et les clients/prospects, dans toutes les formes possibles :

- Dossiers papiers
- Logiciels bureautiques (notamment les tableurs), photos, vidéos, enregistrements …
- Logiciels professionnels

et les documenter dans un registre des traitements (le plus facile est d'utiliser un tableur). La CNIL fournit un modèle de registre (https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx). Ce modèle n'est pas obligatoire et pourrait être simplifié dans le cas d'une TPE n'ayant que quelques salariés et un fichier de ses prospects/clients/fournisseurs, souvent sans autres informations que des données de contacts (adresses, téléphone, email).

Il n'existe pas de certification CNIL pour les logiciels car tout logiciel permet, dans une zone commentaire de fiche client, ou dans une cellule de tableur, de saisir une information qualifiable de « données personnelles » sans aucun contrôle possible par le logiciel. Il est donc inutile de demander un tel certificat aux éditeurs, mais vous pouvez contacter votre éditeur si vous pensez que le niveau de sécurité des données personnelles qui y sont traitées n'est pas suffisant. La CNIL annonce a engagé en 2018 des travaux pour construire un référentiel de certification des DPO et des formations, mais n'annonce rien concernant les logiciels.

Les risques les plus élevés pour les données personnelles sont souvent dans des fichiers tableurs disséminés sur des postes non sauvegardés et peu sécurisés (le mot de passe d'un tableur est aisément contournable). C'est pour ce type de fichiers qui contiennent des données RH ou des données clients/prospects, que le **risque de divulgation est le plus élevé** car il suffit d'une copie ou d'un envoi par mail, au contraire d'une base de données souvent sécurisée qui nécessite l'accès au logiciel. Un inventaire exhaustif est indispensable, et aboutit souvent à la détection d'un grand nombre de données personnelles, souvent inutiles, qui néanmoins sont réparties sur les postes de l'entreprise.

Pour les logiciels professionnels, les éditeurs de logiciels sont sensibilisés et vont généralement renforcer la sécurité ou le cryptage des données. Mais tout cela est inutile si les utilisateurs de l'entreprise se transmettent leurs mots de passe, ou bien laissent leurs postes non verrouillés en cas d'absence, ou bien si la gestion des droits utilisateurs n'est pas rigoureusement définie dans les logiciels ou sur les serveurs.

L'établissement du registre des traitements peut être un gros travail selon l'activité de l'entreprise, mais c'est l'occasion de se poser un grand nombre de bonnes questions qui **amèneront de la sécurité à votre entreprise**, et pas uniquement vis-à-vis des données personnelles.

3. ÉVALUER LES RISQUES ET LES PROCÉDURES À METTRE EN PLACE

Une fois le registre établi, il est souhaitable d'identifier les principaux risques pour l'entreprise en cas de perte ou fuite de données personnelles. Pour chacun des risques identifiés, il faudra décider de la réponse qui sera mise en œuvre le cas échéant.

Au minimum, il faut définir la procédure pour deux situations :

- Une personne demande la modification ou la suppression des données personnelles la concernant : à qui s'adresse-t-elle ?
- Un incident provoque la diffusion non souhaitée de données personnelles : comment en informer les personnes concernées en moins de 72 heures ?

4. FAUT-IL NOMMER UN DPO ? (DATA PROTECTION OFFICER = RESPONSABLE DES TRAITEMENTS DE DONNÉES PERSONNELLES)

Nommer un DPO est obligatoire pour :

- les entreprises du domaine public,
- les entreprises privées dont une activité majeure est de traiter des données personnelles (vente à distance aux particuliers, compagnies d'assurance, sites de rencontre …)
- les entreprises qui traitent des données « sensibles » (santé, judiciaire, ...).

Pour la plupart des petites entreprises, il n'est donc pas obligatoire de nommer un DPO.

Cependant, et même si la nomination d'un DPO n'est pas impérative pour votre entreprise, il est recommandé de désigner un référent pour la protection des données personnelles qui tiendra à jour ses connaissances sur le sujet et gèrera les principales obligations évoquées ci-dessus.

5. ET SI JE NE SAIS PAS COMMENT DÉMARRER ?

Dans certains cas, il est difficile d'évaluer le travail ou les démarches à réaliser. Il est préférable alors de prendre contact avec vos conseillers habituels qui sauront vous orienter. De nombreuses propositions vont vous parvenir pour vous vendre des prestations d'accompagnement estampillées « RGPD ». Assurément elle ne se valent pas toutes, et, sur ce sujet sensible, la confiance est le premier critère de choix d'un partenaire. Les futures certifications CNIL seront un gage de sécurité supplémentaire.

En tant que personnes, nous sommes tous attachés à ce que nos données personnelles soit protégées,

en cohérence, il faut engager cette démarche dans toutes les entreprises qui en détiennent,

afin de contribuer, chacun à son niveau, à la protection de tous.