Note d'information

Mise en application le 25 Mai 2018 du RGPD
(Règlement Général pour la Protection des Données)

Chère Cliente, Cher Client,

Vous êtes de plus en plus nombreux à nous solliciter par rapport à la mise en application, depuis le 25 mai 2018, du nouveau Règlement Général européen pour la Protection des Données (RGPD).

Ce règlement a pour but de protéger les personnes physiques de toute utilisation abusive de données les concernant. Il va remplacer la loi « Informatique et Liberté » en vigueur 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** 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 une personne identifiable : adresse personnelle, données physiques, physiologiques, économique, culturelle, voix, image…

- 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.

Depuis toujours, le cabinet EXTENCIA a veillé à protéger et sécuriser les données qu'elle collectait et traitait. Au cours de ces derniers mois, nous nous sommes également assurés du respect de cette nouvelle législation par les éditeurs de logiciels et partenaires avec qui nous travaillons.

A ce Titre, nous avons rédigé une ***Charte d'engagement***
et mis à jour ***notre Politique de protection des données***
que vous pouvez consulter sur notre Site Internet :
http://www.extencia.fr/rgpd/

Nous insistons sur le fait que le RGPD est bien **l'affaire de tous** et notre **devoir de conseil** nous invite à vous fournir les quelques recommandations suivantes :

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.cni l.fr/rgpd-passer-a-laction

2 - Créer votre registre des traitements

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

- Dossiers papiers
- Logiciels bureautiques (notamment les tableurs Excel)
- Logiciels professionnels

et les documenter dans un registre des traitements (le plus facile est d'utiliser un tableur Excel).

Modèle de registre fourni par la CNIL :
https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx

Ce modèle n'est pas obligatoire et peut 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).
Vous pouvez contacter également vos éditeurs de logiciels si vous pensez que le niveau de sécurité des données personnelles qui y sont traitées n'est pas suffisant.

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.

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 - Nommer EVENTUELLEMENT 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 des partenaires de confiance**, telle que la CNIL, qui sauront vous orienter. De nombreuses propositions vont vous parvenir pour vous vendre des prestations d'accompagnement estampillées « RGPD ». Assurément elles ne se valent pas toutes, et, sur ce sujet sensible, la confiance est le premier critère de choix d'un partenaire.

Cordialement,

Le cabinet EXTENCIA

Remarque : Vous disposez d'un droit **d'accès**, de **rectification** et de **suppression** de vos données personnelles. Nous nous engageons à respecter la confidentialité de vos données personnelles et à garantir l'exercice de vos droits. En tant que Coresponsables, nous avons convenu que ceux-ci peuvent être exercés sans aucun coût en nous adressant un simple courrier électronique à dataprotection@extencia.fr en indiquant simplement le motif de votre demande et le droit que vous voulez exercer.