Fiducia experts

FICHE CLIENT

Le Règlement Général sur la Protection des Données

Les entreprises vont devoir mettre en conformité leurs procédures et leur système d'information pour appliquer la nouvelle réglementation européenne, connue sous l'acronyme RGPD en français (GDPR en anglais) : Le Règlement Général sur la Protection des Données

Quel est l'objectif de la loi ?

Cette loi a pour objectif de **renforcer les droits des individus concernant leurs données personnelles**, données qui sont stockées sur tout support numérique (Ex : les serveurs de l'entreprise). Elle vise à uniformiser les lois sur la protection des données personnelles au sein de l'Union européenne.

3 grands axes :

- Renforcer les droits des personnes (droit d'accès, droit à l'oubli, droit à la portabilité des données personnelles et dispositions propres aux personnes mineures)
- Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants)
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.

Plus largement, le RGPD a pour ambition de "**redonner aux citoyens le contrôle de leurs données personnelles, tout en simplifiant l'environnement réglementaire des entreprises**". **Toutes** les entreprises sont concernées.

A quelle date prend-il effet ?

Le RGDP remplace la loi de 1995 (EU Data Protection Directive). La loi Européenne relative à la protection des données entrera en vigueur le 25 mai 2018. Donc demain …

Qui est concerné ?

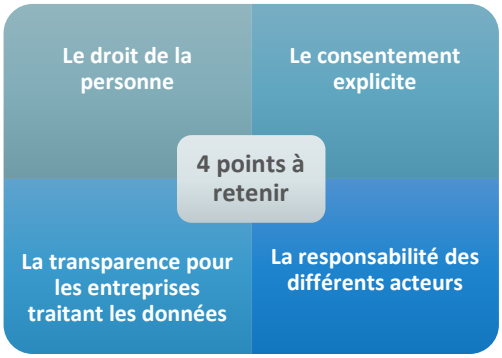
Les règles du RGPD s'appliqueront à toutes les entreprises privées ou publiques des 28 Etats membres de l'Union européenne. Plus précisément, aux entreprises proposant des biens et services sur le marché de l'UE et/ou collectant et traitant des données à caractère personnel sur les résidents de l'UE.

Quel est le périmètre d'application du RGPD ?

Le RGPD concerne uniquement la **protection des données personnelles rattachées à des personnes physiques**.

Le « traitement des données », fait référence à la collecte, à l'accès, au stockage, à la manipulation, à la destruction et à la consultation des données.

Concrètement, une entreprise qui délègue à un prestataire la collecte et le stockage des données fait néanmoins du traitement de données dans la mesure où elle les consulte. (Ex : émission de fiche de paye)



Qu'est-ce qu'un traitement de données conforme au RGDP?

Un traitement est conforme RGPD (6 conditions) si le consentement de la personne concernée a été collecté selon les règles du RGPD ou dans un des cas de traitement sans consentement.

Il faut D'ABORD respecter 6 conditions cumulatives de licéité.

Et du respect de ces 6 principes découle la responsabilité du responsable du traitement.

C'est à la personne responsable de chaque traitement de prouver qu'elle respecte le RGPD (présomption de responsabilité)

Le responsable d'un traitement devra mettre en œuvre des « mesures techniques et organisationnelles appropriées »

Et pour pouvoir prouver respecter toutes ces obligations, les responsables de traitement / sous-traitants peuvent entrer dans une démarche de certification (et audit par un tiers agréé) ou de respect d'un Code de conduite professionnel.

Fiducia experts

FICHE CLIENT

Le Règlement Général sur la Protection des Données

Comment s'assurer que l'on respecte le RGPD ?

Nous proposons une démarche structurée en 6 étapes conforme aux dispositions de la CNIL(organisme de contrôle de la bonne application du RGPD):

1. Désigner un pilote: le DPO (Data Protection Officer)
2. Cartographier vos traitements de données personnelles et identifier les risques
3. Prioriser les actions à mener (plan d'action)
4. Gérer les risques (mise en œuvre du plan d'action)
5. Impact sur les processus internes
6. Documenter la conformité

Les sanctions

La CNIL est chargée du contrôle et des sanctions.

Pour les conditions de licéité des traitements, le format de l'**amende pécuniaire** est « 20 millions d'amende ou 4% maximum du chiffre d'affaires»

En plus des sanctions administratives, le responsable de traitement est également susceptible de devoir **indemniser toute personne ayant subi un dommage** du fait de la violation du règlement (possibilité d'actions de groupe).

A cela peuvent s'ajouter des **sanctions pénales**. En France, les atteintes aux droits de la personne résultant de traitements informatiques sont punies par des peines pouvant aller jusqu'à cinq ans d'emprisonnement et 300.000 € d'amende pour les personnes physiques et 1.500.000 € pour les personnes morales.

Les enjeux de ce nouveau texte et des nouvelles obligations qui en découlent sont significatives.

En conclusion

Si ce règlement vise une simplification des formalités administratives pour les entreprises, il impose néanmoins à ces dernières de démontrer leur bonne application du règlement sous peine de fortes sanctions.

Ceci implique pour l'entreprise de savoir s'entourer des bons professionnels pour les accompagner dans la maîtrise de leurs risques numériques et leurs enjeux de mise en conformité.

Le **Data Protection Officer (DPO)**, véritable "chef d'orchestre" est chargé d'informer et de conseiller le responsable de traitement ou le sous-traitant, mais aussi les employés. Il est le socle de la coordination à la fois en interne et en externe, agissant comme le point de contact de l'autorité de contrôle et des personnes concernées, avec qui il doit coopérer. Il reste indispensable au sein des entreprises.

Trois solutions s'offrent aux entreprises:

- **Désigner** un délégué à la protection des données au sein de l'entreprise (DPO interne mais problématique de compétences)
- **Embaucher** un délégué à la protection des données (Ressource démesurée)
- **Déléguer**: recourir à l'aide d'un DPO externalisé, gage d'indépendance et d'expertise.

Dans cette dernière hypothèse, au-delà d'une mission de diagnostic de votre situation, notre cabinet se propose de vous accompagner dans votre démarche de mise en conformité. Nous vous proposons également de vous assister annuellement dans le suivi de cette conformité en tant que DPO externe.

Compte tenu des enjeux financiers significatifs et du calendrier relativement restreint pour se mettre en conformité, nous prendrons contact avec vous après diffusion de cette information pour examiner la manière dont vous souhaitez aborder cette problématique.