Règlement européen sur la protection des données personnelles (RGPD)

Ce règlement sera applicable en MAI 2018

Certaines formalités auprès de la CNIL vont disparaître. Il ne sera plus nécessaire de faire une déclaration pour obtenir un numéro d'agrément lors de traitements de données à caractères personnelles.
En contrepartie, la responsabilité des organismes sera renforcée. **Tous les organismes publics ou privées** sont concernés dés lors qu'une donnée informatique ou papier contenant des informations permettant d'identifier une personne physique sont collectées.

L'objectif de ce règlement est de responsabiliser les acteurs qui stockent ces informations en donnant des droits aux personnes concernées par ce stockage.

Le droit de ces personnes est principalement de 2 ordres.

- Une collecte légitime et légale
Le règlement interdit la collecte d'information non légitime, par exemple une société de marketing n'a pas le droit de collecter des données sensibles comme un numéro de sécurité sociale.
Toutes personnes doit avoir un droit d'accès, de modification, de suppression et de portage de ses données. L'organisme collecteur doit être en mesure de savoir où se trouve cette donnée et doit pouvoir la communiquer de façon lisible sur simple demande authentifiée.
Enfin tous traitements sur ces données et leurs finalités doivent obtenir un accord explicite (et non implicite) de l'intéressé.

- Une garantie de sécurité
L'organisme se doit d'assurer la protection des données personnelles. Toutes personnes ayant accès à ces données doit être clairement identifiées. Leur accès aux données doit être justifié pour réaliser les traitements légitimes.
La sécurité des Systèmes d'Information doit être en rapport avec les risques associés à ces données. Tout piratage des données par une personne non autorisée doit faire l'objet d'une communication des personnes concernées afin de les sensibiliser au niveau du risque encouru.

Les risques :

En cas de manquement à ce règlement de façon délibérée ou par négligence, le risque est de **20 millions d'euro d'amende ou 4 % du chiffre d'affaires annuel mondial** (le maximum des 2 étant retenus). En cas d'infraction au cas par cas, il est prévu 1500 € par anomalie constatée sur un individu.

Les acteurs de ce nouveau règlement dans les organisations:

- Le Responsable de Traitement, est la personne qui a une responsabilité juridique dans l'organisation qui collecte des informations personnelles.

- Le Délégué à la Protection des Données (DPD), il doit être désigné par le Responsable de Traitement et ne doit pas avoir de conflit d'intérêt avec l'organisme (ne peut pas être un membre du comité de direction ou avoir des responsabilités opérationnelles liées à la collecte des données personnelles).
Il a un rôle de chef d'orchestre de la conformité. Il doit informer/conseiller et contrôler le respect du règlement.

La mise en conformité des organisations en 6 étapes :

1- Nommer un Délégué à la Protection des Données (DPD)
2- Cartographier les traitements de données personnelles
3- Identifier les anomalies et prioriser les actions
4- Mesurer et gérer les risques associés à ces données
5- Organiser les processus internes
6- Documenter la conformité

Vous pouvez faire appel à http://confiance-digitale.fr pour vous accompagner sur l'ensemble de ces points.