



RGPD
MISE EN
CONFORMITÉ
DES
PME ET ETI



RGPD

Ce qu'il faut savoir

Le Règlement Général 2016/679 de l'UE sur la Protection des Données personnelles **est entré en vigueur le 25 mai 2018.**

Toute entreprise touchant aux données personnelles **doit dorénavant mettre en œuvre les mesures appropriées** afin de garantir notamment « *la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* ».

Le **RGPD** fait entrer le droit des données dans l'ère de la *compliance* : **l'entreprise devra démontrer** qu'elle met en place les politiques internes, les processus et les mesures techniques conformes au règlement.

En cas de non conformité, les **sanctions** prévues vont jusqu'à 20.000.000 euros ou 4 % du CA annuel mondial.

La mise en œuvre du **RGPD** est contraignante mais elle doit être vue comme une **opportunité de valoriser l'entreprise** auprès de ses collaborateurs, de ses partenaires, de ses clients, et de ses concurrents.



Les 5 étapes de la mise en conformité

GPDR

La démarche de mise en conformité

5. DOCUMENTATION ET ORGANISATION

Rédaction des documentations recommandées et mise en place de l'organisation de sensibilisation.

4. MESURES CORRECTIVES

Implémentation des mesures correctives juridiques et recommandations techniques nécessaires pour la mise en conformité.



1. ANALYSE DE LA MATURITE

Evaluer le niveau de maturité de l'entreprise quant à la mise en conformité

2. TRAITEMENT DES DONNEES

Identifier où se trouvent les données personnelles et répertorier les traitements associés

3. AUDIT JURIDIQUE ET SI

Identification des risques juridiques et sur le Système d'Information.



Notre démarche étape par étape

La démarche

Phase 1 - Analyse de la maturité de l'entreprise au regard de la mise en conformité

Principaux objectifs

- **Evaluer** le niveau de maturité de l'entreprise quant à la mise en conformité au RGDP.
- **Définir** le périmètre des actions à réaliser pour la mise en conformité.
- **Cadrer** la démarche dans l'entreprise.



Activités

- Réunion avec au moins un représentant de l'entreprise sur la base d'une **Check list** d'environ 40 questions.
- Restitution sous la forme des **actions et de la documentation** à produire pour la mise en conformité.
- **Cadrage** de la démarche : les phases, le planning, les intervenants (DPO ?), l'organisation, etc.



Livrables

- ✓ **Restitution** de la réunion « Check list ».
- ✓ **Cadrage** de la démarche **cartographie des systèmes de traitements** des données personnelles.

La démarche

Phase 2 - Analyse des traitements de données et diagnostic

Principaux objectifs

Cartographie des données

- Identifier **quelles sont et où** se trouvent les données personnelles dans l'entreprise.
- Identifier l'existence de données personnelles **sensibles**.
- Identifier l'existence de traitements de **données hors UE**.



Activités

- **Identifier** les traitements de données personnelles et en établir la liste.
- **Détailler les informations** relatives à chaque traitement et aux données concernées à l'aide du « Registre des traitements de données personnelles ».
- Réaliser une **Analyse d'Impact relative à la Protection des Données**.



Livrables

- ✓ **Liste** des traitements de données personnelles.
- ✓ **Registre des activités de traitements** de données personnelles*.
- ✓ Restitution de l'**analyse d'impact**.
- ✓ **Registre des sous-traitants** et des traitements confiés*.

* Certains livrables peuvent être optionnels pour la mise en conformité.

La démarche

Phase 3 - Audit juridique et SI

Principaux objectifs

Identification des risques du Système de traitement des données

- Identifier les **risques SI** en fonction de 3 typologies (Sécurité du SI, Protection des données personnelles, Droits de la personne).
- Etudier la **conformité juridique** des traitements : respect des principes du RGPD, identification des bases légales et cadre contractuel (collaborateurs, clients, partenaires et sous-traitants).



Activités

- Réaliser une **étude des risques SI** sous l'angle de la Sécurité, de la Protection des données personnelles, et des Droits des personnes.
- **Cadrage juridique** de la conformité : identifier les non conformités majeures (principes généraux du RGPD, bases légales, contrats), données sensibles, sous-traitance, traitements de données hors UE .



Livrables

- ✓ **Matrice des risques** identifiés par typologie.

La démarche

Phase 4 - Mesures correctives

Principaux objectifs

- Définir et implémenter les **mesures correctives**



Activités

- Listes les risques et **déterminer les mesures correctives** à mettre en œuvre pour un système de traitement des données conforme SI et juridique.



Livrables

- ✓ Recommandations juridiques
- ✓ Recommandations techniques et opérationnelles

La démarche

Phase 5 - Documentation et organisation

Principaux objectifs

Mise en œuvre des politiques et procédures conformes au RGPD

- Mettre à jour les contrats
- Implémenter les droits des personnes
- Adapter l'organisation interne au RGPD
- Prévoir les mesures en cas de violation de données personnelles.



Activités

Documentation

- Registre de traitement des données
- Analyses d'impact sur la protection des données
- Procédure d'information des personnes concernées
- Procédure de conservation des données personnelles
- Procédure de revue régulière et de mise à jour des données personnelles
- Procédure de traitement des demandes des personnes concernées
- Procédure des relations contractuelles (collaborateurs, clients, responsables conjoints et sous-traitants, français et internationaux)
- Procédure de gestion des incidents de sécurité

Organisation

- Formation et sensibilisation du personnel
- Désignation d'un interlocuteur informatique et liberté interne
- Désignation d'un délégué à la protection des données (DPD)
- A terme, souscrire à des codes de bonne conduite et/ou des systèmes de certification et de labellisation.



Livrables

- ✓ Procédures
- ✓ Organisation

Nos prestations

PRESTATIONS DE MISE EN CONFORMITE



Pilotage
projet



Audit



Mise en œuvre
conformité



Production de la
documentation

PRESTATIONS D'ACCOMPAGNEMENT



Accompagnement
à la mise en œuvre
des mesures correctives
IT et juridiques



Communication vers
les clients et tout
autre tiers

A black and white photograph of a person walking across a vast, flat, white landscape, possibly a salt flat or a beach at low tide. The person is in the center of the frame, walking towards the right. The horizon is low, and the sky is a uniform, overcast grey. The overall mood is one of solitude and vastness.

Qui sommes-nous ?



Fondé en 2010 par un juriste de formation, DFC est une société de conseil et d'accompagnement de projets informatiques tous secteurs confondus.

DFC est spécialisée sur la sécurisation des projets et les projets de transformation avec une volonté de rendre l'informatique accessible à tous les métiers de l'entreprise.



Maître Juan-Carlos ZEDJAOUI a fondé le cabinet **Adroit** dans le souci de proposer une approche pragmatique et moderne du droit à ses clients.

Maître ZEDJAOUI est notamment spécialisé en droit de la propriété intellectuelle et en en droit des nouvelles technologies, de l'informatique et de la communication.

Il justifie d'une expérience de plus de 20 dans ces différents secteurs d'activité.

Mentions déontologiques :

Le réseau d'avocats **Adroit** est domicilié au 7, avenue de la Bourdonnais – 75007 Paris / Tél : 01.71.19.71.47 / e-mail : contact@avocat-adroit.com / site : <http://avocat-adroit.com>