RGPD

L'Europe s'attaque à

la protection des données

Une obligation depuis le

25 MAI 2018

De quoi s'agit-il ?

RÉGLEMENT

GÉNÉRAL

PROTECTION SUR LA

DONNÉES DES

Définitions

- L'acronyme RGPD signifie « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Régulation » ou GDPR).
- Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

- Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française Informa-tique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

- Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels.
- Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs.

RGPD

Qu'est-ce qu'une donnée personnelle ?

- Une donnée personnelle constitue « toute information se rapportant à une personne physique identifiée ou identifiable ».

- Une personne peut être identifiée, soit :
  - directement (exemple : nom, prénom)
  - indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, une adresse IP, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

- L'identification d'une personne physique peut être réalisée, à partir :
  - d'une seule donnée (exemple : numéro de sécurité sociale, ADN)
  - du croisement d'un ensemble de données, et même si la personne n'est identifiée , elle reste identifiable.

RGPD

Qu’est-ce qu’un traitement de données personnelles ?

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

RGPD

Quelques exemples de fichiers

- Les données que vous pouvez collecter sur vos clients pour réaliser les prestations demandées.

- Il s'agit aussi des informations que vous détenez sur vos salariés, leur adresse, numéro de sécurité sociale, nombre d'enfants, statut matrimonial, etc…

- Il s'agira d'en faire la liste pour déterminer les données dites sensibles qui nécessitent une sécurité accrue et les autres.

Qui est concerné par le RGPD ?

Tout organisme quel que soit sa taille, son pays d'implantation et son activité

Toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non

Dès lors qu'elle est établie sur le territoire de l'Union européenne

ou

que son activité cible directement des résidents européens

RGPD

Sous-traitants également impliqués

- Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organismes.

- Ainsi, si vous traitez ou collectez des données pour le compte d'une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées.

Les TPE et PME face au RGPD

- les petites entreprises sont tout aussi concernées que les grandes

- Il s'agit, pour toute opération ou ensemble d'opérations portant sur des données, de rassembler un certain nombre d'informations dans un registre : quelles informations sont demandées, pour quelle finalité ?

- Les opérations (collecte, enregistrement, conservation, transmission, utilisation, suppression....) devront respecter certaines règles. Par exemple, il sera impossible d'utiliser à des fins commerciales des données récoltées lors d'un évènement, si la personne n'a pas donné son consentement. Le recueil du consentement est plus strictement encadré et doit spécifier l'utilisation qui sera faite des données.

Les risques encourus

- La responsabilité d'une **entreprise peut être engagée au plan civil si les règles fixées par le règlement RGPD n'ont pas été correctement appliquées. Il peut donc** y avoir des conséquences importantes en terme d'image pour le professionnel qui se verrait sanctionné pour non-respect du règlement européen ; mais aussi financière avec des amendes allant jusqu'à 20 millions d'euros ou 4% du CA.

•

Depuis le 25 mai , plus de 3300 sanctions ont été prononcées par la CNIL et ce chiffre est en expansion.

Les 6 points à respecter pour être conforme au RGPD

1- Désigner un pilote : DPO

2- Cartographier vos traitements de données personnelles

3- Prioriser les actions

4- Gérer des risques

5- Organiser les processus internes

6- Vérification des documents

RGPD

Désigner un pilote DPO

- Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exerce une mission d'information,de conseil et de contrôle en interne : le délégué à la protection des données.

RGPD

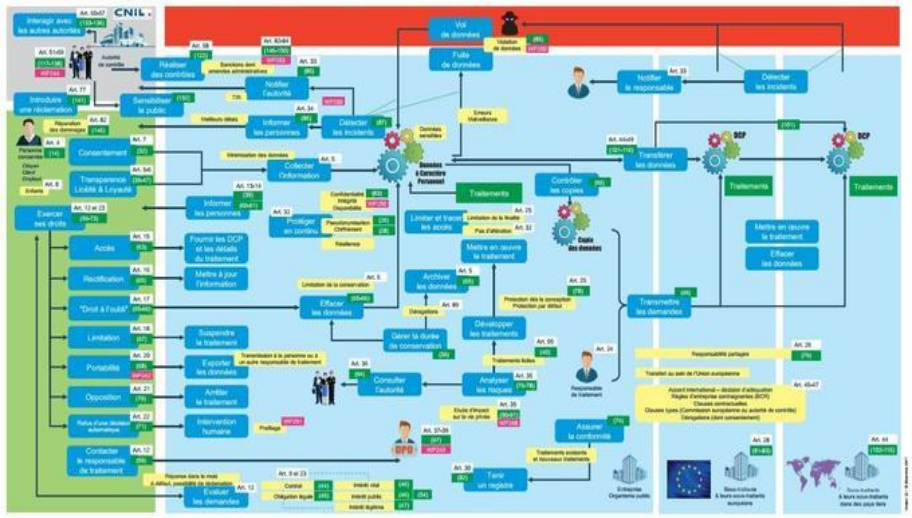
Cartographier vos traitements de données personnelles

- Pour mesurer concrètement l'impact du règlement européen sur la protection des données de votre activité, commencez par recenser de façon précise les traitements de données personnelles que vous mettez en œuvre. La tenue d'un registre des traitements vous permet de faire le point.

RGPD

Prioriser les actions

- Sur la base du registre des traitements de données personnelles, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.



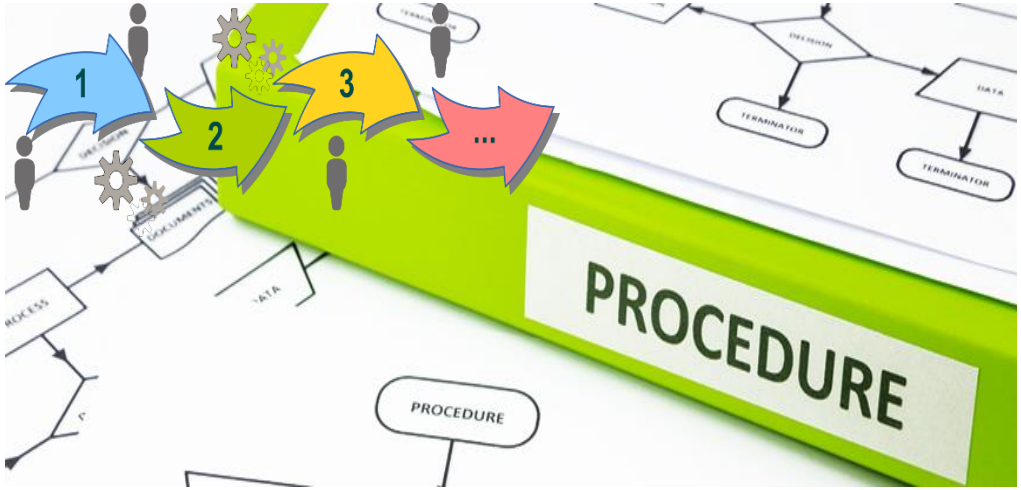
Gérer les risques

- Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une étude d'impact sur la protection des données (en anglais, Privacy Impact Assessment ou PIA).

RGPD

Organiser les processus internes

- Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la protection des données à tout moment ,en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement de données personnelles (par exemple : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire etc.).



Documenter la conformité

- Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire.
- Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

RGPD

Sources documentaires

- Site de la commission européenne

- Site de la CNIL

CNIL.

- Site eur-lex

- Site du service public