LE RGPD
POUR LES NOVICES

spigraph

LE RGPD C'EST QUOI ? C'EST POUR QUI ?

Défini par l'Union européenne, le règlement général sur la protection des données gouverne le traitement des données à caractère personnel des individus.
Depuis le 25 mai 2018, il s'applique à toute organisation, publique et privée, dès lors :

- qu'elle est établie sur le territoire de l'Union européenne,
- ou que son activité cible directement des résidents européens.

QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

C'est une information, ou une combinaison d'informations, relative à une personne physique susceptible d'être identifiée, directement ou indirectement.

Identité : nom, prénom, adresse, date et lieu de naissance, photographie, vidéo,...

Situation familiale : habitudes de vie, situation familiale,...

Situation professionnelle : CV, profession, scolarité, formation,...

Économique et financière : revenus, situation financière, données bancaires,...

Données de connexion : adresses IP, logs, identifiants de connexion,...

Données de localisation : déplacements, données GPS, GSM,...

Internet : cookies, traceurs, données de navigation,...

C'EST QUOI LE TRAITEMENT DE DONNÉES ?

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).

LES 7 PRINCIPES CLÉS DU RGPD

1. **Licéité*, loyauté, transparence du traitement**
2. **Limitation des finalités du traitement**
3. **Minimisation des données : adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités**
4. **Exactitude : données exactes et, si nécessaire, tenues à jour**

QU'EST-CE QU'UN DPO ?

Le délégué à la protection des données (Data Protection Officer ou DPO) dont la désignation est parfois obligatoire, mais toujours recommandée, doit cumuler des compétences juridiques et techniques. Il peut être un collaborateur de l'entreprise ou un prestataire. Soumis au secret professionnel ou à une obligation de confidentialité, il doit, dans tous les cas, agir avec indépendance.

Le DPO est chargé de contrôler le respect de la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné, en l'informant et le conseillant à ce sujet à chaque fois que c'est nécessaire.

En pratique, il pilote le projet de mise en conformité, recense les traitements, assure la liaison entre les responsables de traitement et les personnes concernées (salariés, clients, usagers, etc.) notamment en cas de demande d'accès ou de suppression, aide à effectuer les analyses d'impact et à définir les politiques et diverses procédures de protection des données.

QU'EST-CE QU'UN RESPONSABLE DE TRAITEMENT ?

C'est l'entreprise, l'association, l'établissement public ou l'autorité publique ou, plus généralement, l'organisme qui détermine les finalités et les moyens du traitement.

En pratique, l'organisme responsable de traitement détermine les moyens essentiels et les finalités du traitement seul ou conjointement avec un autre ou plusieurs autres organismes (responsables conjoints) et confie fréquemment le traitement à un prestataire extérieur, lequel doit présenter des garanties suffisantes sur les plans techniques et organisationnels (sous-traitant).

Le contrôle des sous-traitants est l'un des points fondamentaux de la mise en conformité, la CNIL sanctionnant fréquemment les responsables de traitement pour des manquements (dont failles de sécurité) dont les sous-traitants sont à l'origine.

QUELS SONT LES RISQUES, SI JE NE SUIS PAS EN CONFORMITÉ ?

La formation restreinte de la CNIL peut imposer des sanctions si des manquements au RGPD ou à la loi sont constatés :

- Prononcer un rappel à l'ordre
- Limiter temporairement ou définitivement un traitement
- Suspendre les flux de données
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte
- Prononcer une amende administrative.
- Dans le cas d'infractions plus graves, une amende peut s'élever de 2 à 4 % du chiffre d'affaires mondial ou de 10 à 20 millions d'euros (montant le plus élevé) selon les cas.

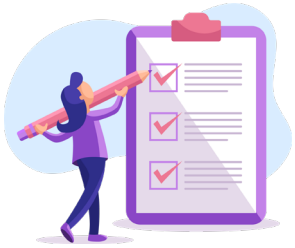
GOOGLE
Amende record
50 000 000 €

Rappel :
Les petites entreprises sont aussi concernées par ces **sanctions.**

5. **Limitation de la conservation des données (au regard de leurs finalités)**
6. **Intégrité et confidentialité des données (sécurité)**
7. **Le principe de responsabilité «accountability»**

***Licéité :** Le traitement est licite si la personne concernée a consenti au traitement de ses données pour une ou plusieurs finalités spécifiques. Sous certaines conditions énoncées dans l'article 6 du RGPD, le consentement peut ne pas être requis (ex. : traitement nécessaire à l'exécution d'un contrat auquel la personne est concernée, traitement nécessaire au respect d'une obligation légale, à la sauvegarde d'intérêts vitaux de personnes physiques, ...).

LES ❹ ACTIONS ESSENTIELLES À MENER POUR ÊTRE CONFORME AU RGPD



❶ LA CARTOGRAPHIE DES TRAITEMENTS

Cela consiste à créer un registre des traitements de données afin d'avoir une vision d'ensemble. Il doit contenir une fiche pour chaque activité recensée en precisant : l'objectif poursuivi (finalité), les catégories de données utilisées (nom, prénom..), qui a accès aux données, la durée de conservation de ces données.

❷ LE TRI DES DONNÉES

Il sert a vérifier que les données qu'une entreprise traite sont nécessaires à ses activités. Ce tri permet aussi de vérifier que seules les personnes habilitées ont accès aux données dont elles ont besoin et que l'entreprise ne conserve pas de donnée au-delà de ce qui est nécessaire.

❸ LE RESPECT DES DROITS DES PERSONNES

Au-delà de leur droit à la transparence, les personnes concernées ont des droits renforcés sur leurs données : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.
Une entreprise peut mettre en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts.

❹ LA SÉCURITÉ DES DONNÉES

Il est de la responsabilité de l'entreprise de garantir l'intégrité, la disponibilité et la confidentialité des données personnelles de ses salariés et de ses clients ou usagers.

spigraph