RGPD

FOIRE AUX QUESTIONS : LES QUESTIONS LES PLUS FRÉQUENTES

Juin 2022

LE RGPD ME CONCERNE-T-IL ?

Le RGPD s'applique à toute organisation, publique et privée, quelle que soit sa taille et activité (entreprise, administration, collectivités et associations), 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 personnes qui se trouvent sur le territoire de l'UE.

Autrement dit, que vous soyez un professionnel de santé ayant son cabinet médical, président d'une association de quartier avec 10 membres, artisan travaillant seul, maire d'une commune de 500 habitants ou encore PDG d'une grosse PME, vous devez vous conformer au RGPD.

LA DÉSIGNATION D'UN DPO EST-ELLE OBLIGATOIRE ?

Le Délégué à la protection des données (DPO) est le chef d'orchestre de la conformité. Sa nomination n'est pas obligatoire dans toutes les structures. En effet, seuls les autorités ou les organismes publics (collectivité, syndicat, notaire, huissier, etc.) et les autres structures amenées à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions sont contraints de désigner un DPO. Les autres structures n'y sont pas obligées, même si c'est fortement recommandé.

Le DPO peut être interne à la structure ou externalisé par l'intermédiaire d'un prestataire.

Le DPO est chargé d'informer, conseiller, auditer et accompagner le représentant de la structure dans sa mise en conformité.

Le DPO n'est pas personnellement responsable en cas de non-conformité de son organisme avec le règlement. Celle-ci incombe au responsable de traitement ou le sous-traitant qui doit être en mesure de démontrer que le traitement est effectué conformément à la règlementation.

QU'ENTEND-T-ON PAR RESPONSABLE DE TRAITEMENT ?

Le responsable de traitement est la personne morale (entreprise, commune, association, etc.) ou physique qui détermine les finalités et les moyens d'un traitement des données à caractère personnel, c'est à dire l'objectif et la façon de le réaliser. En pratique, il s'agit de la personne morale incarnée par son représentant légal (président, gérant, maire, etc.).

Le responsable de traitement est légalement responsable de la conformité de ses opérations de traitement avec le RGPD et est responsable vis-à-vis des personnes et des autorités qui peuvent l'auditer et le sanctionner en cas de violation du règlement.

Le responsable de traitement est soumis à une série d'obligations (obligation d'information, obligation de sécurité, etc.). S'il ne s'y conforme pas, sa responsabilité peut être engagée.

Le responsable du traitement peut agir seul ou conjointement avec d'autres.

Il y a responsabilité conjointe de traitement lorsque l'entreprise s'associe à une ou plusieurs organisations pour déterminer conjointement « pourquoi » et « comment » les données à caractère personnel devraient être traitées. Dans ce cas, un accord doit définir précisément les obligations et le partage de responsabilité de chacun.

QU'ENTEND-T-ON PAR SOUS-TRAITANT ?

Le sous-traitant des données traite les données à caractère personnel uniquement pour le compte du responsable du traitement.

Le sous-traitant est généralement un tiers extérieur à l'entreprise. Toutefois, dans le cas des groupes d'entreprises, une des entreprises peut être le sous-traitant d'une autre.

Les devoirs du sous-traitant envers le responsable du traitement doivent être précisés dans un contrat. Par exemple, le contrat doit préciser ce que deviennent les données personnelles quand le contrat prend fin.

QUE RISQUE-T-ON EN CAS DE NON-CONFORMITÉ ?

En cas de violation des normes RGPD de la part des organismes, les sanctions peuvent être très importantes :

- *Amendes administratives* : amende pouvant aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires mondial pour le non-respect des obligations administratives et amende pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial pour le non-respect des droits des personnes
- *Risque pour la réputation de l'entreprise* : mauvaise image de l'entreprise, perte de la confiance des collaborateurs et des clients
- *Dénonciation* : suite à une insatisfaction, dénonciation auprès de la CNIL, d'un client mécontent, prospect ou ancien collaborateur

Attention, ça ne touche pas que les grandes entreprises, la CNIL sanctionne régulièrement les « petites structures ».

Exemples : Société de traduction (TPE – 9 personnes) : Uniontrad Company a été condamnée à 20 000 euros d'amende pour avoir mis en place un dispositif de vidéosurveillance qui plaçait ses salariés sous surveillance constante (juin 2019)

Médecins : deux médecins libéraux condamnés à 3000 et 6000 euros pour insuffisance de protection des données de santé des patients et pour absence de notification d'une violation de données à la CNIL (décembre 2020)

QUELLES SONT LES OPPORTUNITÉS LIÉES AU RGPD ?

- *Meilleure protection des données* : le RGPD est un règlement nécessaire pour protéger les données personnelles de chaque citoyen. Il responsabilise les entreprises quant à leur utilisation afin d'éviter de nouvelles dérives. Elles doivent adopter les mesures de sécurité adéquates afin de renforcer la vie privée des personnes
- *Gestion renforcée des données personnelles* : le RGPD impose aux entreprises de revoir leur système de collecte et de gestion des données par la mise en œuvre de mesures comme par exemple la mise en place de procédures internes, l'amélioration des pratiques ou une meilleure information des équipes sur le respect de la vie privée
- *Se conformer au RGPD est un gage de confiance et de qualité* : les clients ont une meilleure maîtrise de leurs données personnelles car ils sont informés sur le traitement des données et les droits dont ils disposent (accès, rectification, suppression, opposition, etc.). Les entreprises améliorent leur image aux yeux des tiers et inspirer confiance va vous permettre de fidéliser votre clientèle existante, d'attirer de nouveaux clients et de gagner de nouveaux marchés
- *Amélioration de la sécurité au sein de l'entreprise* : face aux attaques de plus en plus nombreuses, la protection des données est devenue un atout majeur. Le RGPD vous permet en cas de fuite de données par un tiers malveillant de faire face aux demandes de vos clients ou de vos salariés.

QU'EST-CE QUE LA CNIL ?

La Commission Nationale de l'Informatique et des Libertés (CNIL) a été créée par le loi Informatique et Libertés du 6 janvier 1978. Elle assure une veille et contrôle les usages informatiques afin qu'ils demeurent en conformité avec la loi française. Il s'agit notamment de protéger la vie privée et les libertés individuelles ou publiques, et de veiller également à la protection des données personnelles qui font l'objet de traitements. Cela inclut tous les traitements qu'ils soient informatiques ou papiers, et qu'ils soient le fait d'organismes publics aussi bien que privés.

La CNIL a des missions de conseil et d'information vis-à-vis de tous les publics (particuliers et organisations), mais elle dispose aussi d'un pouvoir de contrôle et de sanction :

- Dans le cadre de sa mission d'information, elle répond aux demandes des particuliers et des professionnels. Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits en lui adressant une plainte
- La mission d'accompagnement de la conformité constitue son objectif prioritaire
- Dans sa mission de contrôle et de sanction, la CNIL peut contrôler les organismes et, en cas de manquements constatés, elle peut décider de les mettre en demeure ou de les sanctionner