TPE/PME : LES POINTS CLES POUR REUSSIR SA MISE EN CONFORMITE AU RGPD

Le Règlement Général sur la Protection des Données (RGPD) est entré en vigueur le 25 mai 2018. Il renforce l'obligation de protéger et de sécuriser le traitement des données personnelles et institue, à cet effet, une obligation de transparence et de licéité dans la collecte et le traitement des données personnelles par les entreprises. Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels.

La Commission Nationale de l'Informatique et des Libertés (CNIL) est l'autorité de contrôle pour la protection des données personnelles, chargée de veiller, d'accompagner les entreprises à la bonne application du RGPD et d'en sanctionner les manquements.

ATTENTION
Dans un communiqué « Alerte vigilance » publié le 24 novembre 2017, la CNIL a annoncé avoir constaté l'émergence d'une pratique frauduleuse au sujet de la mise en conformité avec le RGPD. Le message, alarmiste et pouvant faire penser à une mise en demeure administrative, insiste sur les sanctions financières encourues.

Selon la CNIL ces messages peuvent avoir pour but de faire appeler un numéro de téléphone surtaxé, de faire signer un engagement frauduleux pour une « mise en conformité Informatique et Libertés (ou RGPD) » ou de collecter des informations sur une organisation pour préparer une escroquerie ou une attaque informatique.
Elle signale ne pas être à l'origine de ces messages et invite les entreprises qui ont des doutes sur certains messages qu'elles ont reçus à la contacter au 01 53 73 22 22.

https://www.cnil.fr/fr/vigilance-mise-en-conformite-rgpd

Qui est concerné?

Toute entreprise, organisme public ou privé quel que soit sa taille, son pays d'implantation et son activité qui traite des données personnelles pour son compte. Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte de leurs clients.

Qu'est-ce qu'une donnée personnelle?

Toute information se rapportant à une personne physique identifiée ou identifiable. Une personne peut être identifiée directement (nom, prénom) ou indirectement (identifiant, n°client, n° de téléphone, la voix, l'image…)

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

Opération ou ensemble d'opérations portant sur des données personnelles quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, extraction, consultation…).
Ex: tenue d'un fichier de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs…
Un traitement de données personnelles n'est pas nécessairement informatisé.
Le traitement doit avoir un objectif, une finalité c'est-à-dire que l'on ne peut pas collecter ou traiter des données personnelles simplement au cas où cela serait utile.

Ex: l'édition de factures, la mise en place d'un programme de fidélité constituent des traitements de données personnelles ayant pour objectif la gestion de la clientèle.

La désignation d'un Délégué à la Protection des Données (DPD) ou Data Protection Officer (DPO) est-elle obligatoire ?

Oui, dans certains cas limitativement énumérés par le RGPD.

La désignation du DPD est obligatoire pour :

-Les autorités ou les organismes publics,

-Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle (prise en compte du nombre de personnes concernées, le volume de données, durée et permanence du traitement…) ex: banques, assurances, opérateurs téléphoniques, réseaux sociaux…

-Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » (*concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes)* ou relatives à des condamnations pénales et infractions *(ex: hôpitaux, laboratoires….)*

En dehors de ces cas, la désignation d'un DPD est vivement encouragée. Elle permet en effet de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données personnelles.

Le RGPD impose que le délégué soit désigné « *sur la base de ses qualités professionnelles et, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir ses missions* ».

Le DPD doit être déclaré auprès de la CNIL.

https://www.cnil.fr/fr/designation-dpo

Quelles sont les obligations pour les entreprises qui collectent des données personnelles ?

Chaque entreprise qui collecte des données personnelles a l'obligation de constituer **un dossier dit « RGPD »**.

La constitution de ce dossier permettra à l'entreprise, à l'occasion d'un contrôle de la CNIL, de démontrer efficacement et rapidement que le traitement de données personnelles est conforme au règlement.

Le dossier devra notamment contenir les éléments suivants :

- Le registre des activités de traitement,

https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

Des modèles de registres sont disponibles sur le site de la CNIL : https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

- Dans certains cas, les analyses d'impact sur la protection des données ou Privacy Impact Assessment (PIA),

L'analyse d'impact relative à la protection des données (PIA) est obligatoire pour tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées.

C'est une étude aidant à construire des traitements de données respectueux de la vie privée et permettant de démontrer la conformité de son traitement au RGPD.

Si le traitement rencontre au moins 2 des 9 critères ci-dessous, alors il est vivement conseillé de faire une analyse d'impact relative à la protection des données (PIA) :

- Evaluation ou notation;
- Décision automatisée avec effet juridique ou effet similaire significatif;
- Surveillance systématique ;
- Données sensibles ou données à caractère hautement personnel ;
- Données personnelles traitées à grande échelle ;
- Croisement d'ensembles de données ;
- Données concernant des personnes vulnérables ;
- Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
- Exclusion du bénéfice d'un droit, d'un service ou contrat.

https://www.cnil.fr/fr/gerer-les-risques

Cette analyse d'impact doit être réalisée avant la mise en œuvre du traitement.

La CNIL a mis en place des outils pour aider les entreprises à mener ce PIA :
https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-pia

- L'encadrement des transferts de données hors UE (notamment les clauses contractuelles types),

- Les mentions d'information,

La personne concernée par un traitement de données doit recevoir une information délivrée de façon concise, transparente, compréhensible et aisément accessible en des termes clairs et simples.

Le support utilisé pour la collecte des données personnelles doit comporter des mentions d'information:
- Finalité de la collecte,
- Le nom de la personne autorisée à traiter les données,
- Le nom de la personne qui a accès aux données,
- La durée de conservation des données,
- Les droits des personnes et les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits,
- L'indication de la transmission des données hors de l'UE (préciser le pays).

Pour éviter des mentions trop longues sur un formulaire, il est possible de donner un premier niveau d'information en fin de formulaire et de renvoyer à une politique de confidentialité complète.

- Les modèles de recueil du consentement des personnes concernées,

Les personnes doivent être informées de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambigüe.

- Les procédures mises en place pour l'exercice des droits des personnes,

Les personnes (clients, salariés, fournisseurs…) ont des droits sur leurs données qui sont renforcés par le RGPD: droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.

- Les contrats avec les sous-traitants qui traitent des données personnelles pour votre compte dans le cadre d'une prestation

https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants

- Les preuves que les personnes concernées ont donné leur consentement.

- Les procédures internes en cas de violation de données,

Le RGPD impose aux entreprises de garantir un niveau de sécurité adapté aux risques numériques.

Pour garantir à tout moment la sécurité et la protection des données personnelles collectées et traitées, chaque entreprise doit prendre toutes les mesures nécessaires pour limiter voire éviter les failles de sécurité, espionnage, piratage, perte, vol de données….et mettre en place des procédures internes.

L'Agence Nationale de la Sécurité des Systèmes Informatiques (ANSSI) publie sur son site un guide des bonnes pratiques de l'informatique pour la sécurité des systèmes d'informations des TPE/PME.

https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/

Ex : mises à jour régulières des logiciels, changement régulier des mots de passe (chaque trimestre) et utilisation de mots de passe complexes, cryptage ou chiffrement des données, mise en place d'une charte informatique, sécuriser l'accès WI-FI de l'entreprise, protéger les données lors des déplacements….

En cas de violation de données personnelles, le RGPD impose à l'entreprise de prévenir immédiatement la CNIL dans les 72 heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Cette notification s'effectue en ligne sur le site de la CNIL : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Si ces risques sont élevés pour ces personnes, il faudra les en informer.
En cas de doute, l'entreprise doit notifier la violation à la CNIL qui lui indiquera s'il est nécessaire d'informer les personnes.

Quelles sont les sanctions en cas de violation des dispositions du RGPD?

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du

règlement. La nature de la sanction varie en fonction de la gravité du manquement aux dispositions du RGPD.

S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Responsabilité civile : réparation du préjudice matériel et moral subi en raison de la violation des dispositions du RGPD.

Responsabilité pénale (article 226-17 du Code pénal) : le fait de procéder ou de faire procéder à un traitement de données en violation des dispositions du RGPD est puni de 5 ans d'emprisonnement et 300 000 euros d'amende.

Par ailleurs, la CNIL et Bpifrance ont élaboré un guide pratique de mise en conformité au RGPD à destination des entrepreneurs. La mise en place du RGPD est aussi l'occasion pour les TPE et PME de progresser dans leur maturité numérique.

https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement

Pour vous aider dans votre mise en conformité RGPD :

- Atelier « RGPD » CCI de Seine-et-Marne