Règlement Général Protection des Données

RGPD 2020
RESUME DES DIFFERENTES ACTIONS

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
RGPD (source CNIL) (Cliquez ici)

Qui est concerné ?

Le RGPD est obligatoire pour toute organisation (Entreprise, TPE, PME, commerce, association, collectivité, publique et privée) qui traite des données personnelles. Toute organisation est concernée dès lors qu'elle a des clients, sous-traitants, salariés, site internet, géolocalisation, vidéosurveillance, badges etc…

Quelles sont les actions à mener pour une mise en conformité RGPD ?

(Ces actions doivent perdurer dans le temps pour être efficaces).

1-Registres des activités de traitements (ils sont la base, le socle de départ) (obligatoire)

-La mise en conformité du RGPD (entrée en vigueur le 25 Mai 2018) consiste en premier lieu et de façon obligatoire à mettre en œuvre et à réaliser les « Registres des activités de traitements » de l'entreprise.

-Il s'agit de mettre en application les préconisations juridiques et techniques de la CNIL.

-Pour chaque ensemble d'opérations traitant des données personnelles, différents registres doivent être réalisés (clients, sous-traitants, salariés, site internet, géolocalisation, vidéosurveillance, badges, etc…).

-A titre d'information, un seul registre représente environ une cinquantaine de pages, ce n'est donc pas quelque chose de simple, facile et rapide à réaliser.

-La réalisation des registres consiste à cartographier les activités principales de l'entreprise qui nécessitent la collecte et le traitement de données.

-Dans les différents registres, il s'agit de déterminer les acteurs, le responsable de traitement, l'entreprise, les sous-traitants, les catégories de données utilisées (pour la paie : nom, prénom, date de naissance, salaire, etc.), descriptif du risque (vol, piratage, pertes de données), l'objectif poursuivi ou la

finalité (Gestion du personnel, obligations légales, paiement des salaires), déterminer le flux de données (PC, disques dur externes, cloud, supports papier), qui a accès aux données (le destinataire, service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs), la durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive), données nécessitant la mise en place d'une analyse d'impact (PIA), mesures de sécurité (Mises en œuvre et préventions pour protéger les données à caractère personnel, identification et priorisation des actions à mener).

2-Documentation (obligatoire)

-Pour prouver la conformité au règlement, il est nécessaire de 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.

-Cette documentation est constituée par exemple des registres de traitements mais également de tous les dossiers et documents réalisés lors de la mise en conformité. C'est ce que demande la CNIL.

3-Registre sous-traitant (obligatoire)

-En tant que sous-traitant, vous devez tenir un registre des catégories d'activités de traitement que vous effectuez pour le compte de vos clients.

-Ce registre doit contenir : le nom et les coordonnées de chaque client pour le compte duquel vous traitez des données, le nom et les coordonnées de chaque sous-traitant ultérieur, le nom et les coordonnées du délégué à la protection des données, les catégories de traitements effectués pour le compte de chaque client, une description générale des mesures de sécurité techniques et organisationnelles que vous mettez en place.

4-Prestations complémentaires obligatoires et optionnelles (sous condition)

-A ce stade l'entreprise est en mesure de déterminer les besoins de mise en place complémentaires de certains dossiers, documents ou certaines prestations selon qu'elle est concernée ou non.

-C'est à cette étape également qu'elle est en mesure de définir si son **prestataire informatique** doit intervenir pour renforcer la sécurité informatique.

5-Création et mise en place d'une charte informatique (optionnelle)

-Elle permet de définir les règles de sécurité, d'utilisation et de protection informatiques dans l'entreprise, elle n'est pas nécessairement liée à un site internet.

6-Avenants aux contrats de travail (obligatoire)

-Le Règlement Européen sur la Protection des Données Personnelles renforce le droit des salariés.
Il est par conséquent impératif pour l'employeur de mettre à jour les contrats de travail sur deux points :

- La définition des missions du salarié pour lesquelles ce dernier va traiter ou collecter des données personnelles ;
- La définition des nouveaux droits du salarié (droit d'accès, rectification, etc…).

7-Politique de Confidentialité pour site internet (obligatoire)

-La Politique de Confidentialité d'un site internet doit comporter certaines dispositions pour satisfaire au Règlement Européen sur la Protection des Données :

- Définition d'une donnée à caractère personnel ;
- Identité du responsable de traitement ;
- Objectif de la Politique de Confidentialité ;
- Les données collectées ;
- La durée de conservation des données ;
- La base juridique que laquelle se fonde le traitement ou la collecte de données ;
- Etc.

8-Conditions générales de vente (obligatoire)

-Pour être en conformité avec le Règlement Européen sur la Protection des Données, les Conditions Générales de Vente doivent disposer de différentes clauses spécifiques comprenant :

- Identité de la société et du responsable de traitement ;
- L'éventuelle transmission des données à un sous-traitant/tiers ;
- La mention du droit d'accès, de rectification, de limitation, et d'effacement des données ;
- La possibilité de s'opposer au traitement et à la portabilité des données ;
- La possibilité de retirer son consentement au traitement effectué ;
- La possibilité d'effectuer une réclamation auprès de l'autorité de contrôle.
- Etc.

9-Conditions générales d'utilisation (Données à caractère personnel site internet) (obligatoire)

-Le Règlement Européen sur la Protection des Données impose une mise à jour des sites internet.

A ce titre, les mentions égales et Conditions Générales d'utilisation doivent désormais intégrer une clause RGPD qui doit notamment préciser :

- Le renvoi à une Politique de Confidentialité (via un lien hypertexte) ;
- Le droit d'accès, rectification, effacement, portabilité de vos données ou limitation du traitement de ces dernières ;
- Identité et coordonnées du responsable de traitement.

10-Clauses contractuelles de sous-traitance (obligatoire)

-Lors de l'utilisation d'un sous-traitant, le Règlement Européen sur la Protection des Données **impose aux entreprises dans son article 28-1 de faire uniquement appel à des sous-traitants qui présentent des garanties suffisantes** quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

Par conséquent, chaque entreprise doit veiller à mettre à jour les contrats passés avec ses sous-traitants afin de se mettre en conformité avec le Règlement Européen.

A noter de ces contrats constitueront une partie de la documentation RGPD que doit mettre en place chaque entreprise afin de justifier de sa conformité au Règlement Européen.

L'avenant au contrat comprend :

- L'objet du contrat
- La description du traitement faisant l'objet de la sous-traitance
- La durée du contrat
- Les obligations du sous-traitant vis-à-vis du responsable de traitement
- Les obligations du responsable de traitement vis-à-vis du sous-traitant

11-Clause d'information en cas d'utilisation de badges (obligatoire)

-L'utilisation de badges pour règlementer l'accès aux locaux constitue un registre de traitements. Plusieurs données sont effectivement susceptibles d'être collectées (nom, prénom, numéro de matricule interne, numéro de badge, date d'entrée et de sortie, etc…).

12-Clause d'information en cas de géolocalisation des véhicules des salariés (obligatoire)

-L'utilisation d'un système de géolocalisation des véhicules constitue un registre de traitements. Plusieurs données sont effectivement susceptibles d'être collectées (nom, prénom, coordonnées professionnelles, matricule interne, numéro de plaque d'immatriculation du véhicule, etc…).

13-Clause d'information en cas de vidéosurveillance sur les lieux de travail (obligatoire)

-L'utilisation d'un système de vidéosurveillance constitue un registre de traitements. L'image d'un salarié, visiteur, client est une donnée et doit faire l'objet de plusieurs actions

14-Engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel (obligatoire)

-Le responsable de traitement devant prendre toutes les mesures nécessaires pour sécuriser la collecte et le traitement des données personnelles, il est impératif de sensibiliser les personnes amenées à traiter ou collecter lesdites données.

15-Modèle de clause pouvant être utilisée en cas de maintenance par un tiers (obligatoire)

-Les opérations de maintenance réalisées par des tiers doivent faire l'objet d'un encadrement pour maîtriser l'accès aux données par des tiers.

16-Bandeau d'information préalable si existence site internet (obligatoire)

-Tout internaute se rendant sur un site internet doit être informé : des finalités précises des cookies utilisés, de la possibilité de s'opposer à ces cookies et de changer les paramètres en cliquant sur le lien présent dans le bandeau, du fait de sa validation de l'utilisation des cookies en poursuivant sa navigation sur le site internet.

17-Information du candidat à l'embauche (obligatoire)

Pour être en conformité avec le Règlement Européen sur la Protection des Données, le recrutement d'un salarié doit faire l'objet d'une note informative comprenant :

- Identité de la société et du responsable de traitement ;
- La finalité, la base juridique et le process du traitement de données ;
- L'éventuelle transmission des données à un sous-traitant/tiers ;
- La durée de conservation des données ;
- La mention du droit d'accès, de rectification, de limitation, et d'effacement des données ;
- Etc.

18-Note informative sur la mise en place du RGPD (obligatoire)

-Une note informative concernant la mise en place du RGPD doit être mise à disposition auprès des salariés, clients, fournisseurs, prestataires, sous- traitants. Elle peut être intégrée au site web.

19-Attestation justificative mise en conformité RGPD (obligatoire)

-Depuis le 25 mai 2018 et l'entrée en vigueur du Règlement Européen sur la Protection des Données, toute société ou organisme doit attester auprès de ses clients avoir réalisé cette démarche.

20-Recommandations de la CNIL dans le cas d'une authentification des utilisateurs basée sur des mots de passe

21-Formulaire de notification et violation CNIL

22-A ce stade l'entreprise est en capacité de mettre en place toutes les préventions qui s'imposent et elle capable de répondre à certaines interrogations.

22-1-PIA (analyse d'impact) (optionnelle)

Lorsque le traitement a pour objet ou pour effet : l'évaluation d'aspects personnels ou notation d'une personne (scoring financier), une prise de décision automatisée, la surveillance systématique de personnes (télésurveillance), le traitement de données sensibles (santé, biométrie, etc.), le traitement de données concernant des personnes vulnérables (mineurs), le traitement à grande échelle de données personnelles, le croisement d'ensembles de données, des usages innovants ou l'application de nouvelles technologies (objet connecté), l'exclusion du bénéfice d'un droit, d'un service ou contrat (liste noire).

Si les traitements de données répondent à au moins 1 de ces 9 critères, vous devez, *a priori*, conduire une analyse d'impact sur la protection des données (PIA : Privacy Impact Assesment), avant de commencer les opérations de traitement.

22-2-DPO (délégué à la protection des données) (optionnelle)

Dans certains cas, vous pourrez être conduits à désigner un délégué à la protection des données.

Cette désignation est obligatoire pour certaines entreprises opérant des traitements à grande échelle présentant des risques particuliers.

Dans les autres cas, la désignation d'un délégué (DPO) est recommandée notamment si votre activité vous impose de mener une analyse approfondie du RGPD.

*Le RGPD, source de business supplémentaire !

Alors qu'il est souvent considéré comme une contrainte, le RGPD peut devenir **un véritable avantage concurrentiel**. Comment ? Tout simplement en mettant en avant vos démarches de mises en conformité dans votre communication. Un bon moyen de prendre l'avantage face à vos concurrents qui n'auraient pas encore entamé ces démarches ou qui n'auraient pas eu l'idée de communiquer dessus !

Important : Pour rappel, vos clients, doivent vous demander de justifier et d'attester que vous êtes en conformité avec le RGPD, avant de collaborer avec vous, c'est ce qu'impose la CNIL.

*Contrôles et sanctions

Contrôle en cas de non réalisation du RGPD ? Les contrôles sont réalisés par la CNIL. Le contrôle peut être réalisé de façon inopinée, ou suite à la plainte d'une personne, d'un organisme qui ont constaté une violation de leurs données à caractère personnel. La conformité d'un site internet peut également être contrôlée à distance.

Qui est responsable ? De façon générale, il s'agit de la personne morale (l'entreprise) qui est incarnée par le représentant légal (le dirigeant), lui-même responsable du traitement de données.

Quelles sont les sanctions ? Les sanctions encourues par le représentant légal des personnes morales (sociétés), sont des sanctions administratives prononcées par la CNIL qui peuvent être conséquentes ainsi que des sanctions pénales.

Précision : Lorsqu'une entreprise fait appel à un cabinet extérieur pour réaliser le RGPD (cabinet d'avocat, cabinet spécialisé, autre), en cas de contrôle de la CNIL, seules les responsabilités du représentant légal et de la personne morale peuvent être engagées.