Comprendre le RGPD et ses conséquences

RÈGLEMENT GÉNÉRAL POUR LA PROTECTION DES DONNÉES

Le Règlement Général pour la Protection des Données est un règlement européen applicable à partir du 25 mai 2018. Ce règlement a pour but de protéger les personnes physiques de toute utilisation abusive de données les concernant.

Il va remplacer la loi « Informatique et Liberté » en application depuis 1978.

MÉDIA DATA SERVICES - Avenue des Censives - TILLÉ - BP 50333 - 60026 BEAUVAIS
SAS au capital de 1 500 000 € 829 606 599 RCS Beauvais N° CCPAP 0319W92243

Les principes majeurs de ce règlement

CHAQUE ENTREPRISE TRAITANT DES DONNÉES DE RESSORTISSANTS EUROPÉENS DOIT SE METTRE EN CONFORMITÉ POUR L'ENSEMBLE DES DONNÉES PERSONNELLES QU'ELLE MANIPULE.

Une donnée personnelle c'est :

Ce qui permet d'identifier précisément une personne : nom, prénom, téléphone, email, numéros d'identification pour l'administration, la sécurité sociale …

Toute donnée attachée à une personne identifiable : adresse personnelle, donnée physique, physiologique, économique, culturelle, voix, image …

Chaque entreprise, quelle que soit sa taille et son métier, doit s'engager à :

Identifier toutes les données personnelles qu'elle détient et tenir un registre des objectifs ou finalités qui en justifient la conservation : *registre des données personnelles, registre des traitements et des finalités des durées de conservation nécessaires, et suppression de toutes les données ou traitements non justifiables.*

Sécuriser ces données pour éviter qu'elles ne soient utilisées à d'autres fins ou diffusées à d'autres que les utilisateurs légitimes : *sécurisation technique et sécurisation des procédures, y compris des sous-traitants (outils ou structures qui traitent des données personnelles pour le compte de l'entreprise).*

Informer les personnes concernées de ces finalités et des données en question, et être capable de rectifier, supprimer ou restituer les données personnelles à la demande de ces personnes : *droit à l'oubli, droit à la rectification, portabilité.*

Informer rapidement la CNIL et toutes les personnes concernées en cas d'incident générant une diffusion non contrôlée de ces données (piratage …) : *devoir d'information en moins de 72 heures.*

Pour mener à bien ce projet, dans l'entreprise, il faut au minimum désigner un référent qui gèrera ce projet, et éventuellement un DPO (Data Protection Officer = responsable des données personnelles) si le métier de l'entreprise consiste à traiter à grande échelle des données personnelles ou des données sensibles.

Pourquoi collecter ces données ?

La collecte, le traitement et le stockage de données s'inscrit dans une démarche de connaissance du marché agricole et de ciblage pour, au travers de nos différents portails d'informations, produits et services à destination des agriculteurs, campagnes de marketing direct et communication ciblée, développer l'activité de nos clients agrofournisseurs, coopératives, et distributeurs et proposer à l'agriculteur l'offre à plus forte valeur ajoutée pour son métier.

CHARTE DES ENGAGEMENTS NGPA POUR LE RGPD

Pour la conformité de Média Data Services, et pour faciliter la mise en conformité de nos clients, nous nous engageons à mettre en oeuvre et garantir dans la durée les pratiques suivantes :

1. Actualiser la cartographie de nos propres bases de données personnelles.

2. Mettre à jour les registres des traitements dans notre entreprise.

3. Respecter nos engagements contractuels de responsable des traitements ou sous-traitant liés au traitement des données personnelles dans le cadre du RGPD.

4. Collecter les données personnelles dans le cadre légal.

5. Notifier toute violation de données, une fois le périmètre impacté identifié.

6. Prendre les mesures nécessaires pour vous garantir un niveau de sécurité des données et des traitements adaptés aux risques.

7. Permettre aux personnes dont les données personnelles sont collectées de faire valoir leurs droits (accès, rectification, portabilité).

8. Veiller à ce que les personnes autorisées à traiter des données personnelles soient engagées contractuellement à une obligation de confidentialité.

9. Informer et contractualiser tout recours à un sous-traitant ultérieur en nous assurant qu'il présente des garanties suffisantes pour la protection des données personnelles. Respecter le cadre légal imposé en cas de recours à un sous-traitant.

Je suis client NGPA : que dois-je faire ?

1/ PRENDRE CONNAISSANCE DE LA RÉGLEMENTATION.

Des documents simples et clairs sont publiés par la CNIL pour faciliter la compréhension de cette réglementation.

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

https://www.cnil.fr/rgpd-notions-cles-et-bons-reflexes

https://www.cnil.fr/rgpd-passer-a-laction

2/ CRÉER VOTRE REGISTRE DES TRAITEMENTS

L'essentiel est d'identifier les données personnelles détenues sur les salariés et les clients/prospects, dans toutes les formes possibles :

1. Dossiers papiers.

2. Logiciels bureautiques (notamment les tableurs) ou professionnels.

3. Base de données informatisées (CRM, listes de diffusion, fichier clients, adhérents,…).

et les documenter dans un registre des traitements (le plus facile est d'utiliser un tableur). La CNIL fournit un modèle de registre (https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx). Ce modèle n'est pas obligatoire et pourrait être simplifié dans le cas d'une TPE n'ayant que quelques salariés et un fichier de ses prospects/clients/fournisseurs, souvent sans autres informations que des données de contacts (adresses, téléphone, email).

LES RISQUES LES PLUS ÉLEVÉS POUR LES DONNÉES PERSONNELLES.

Garantir une méthode efficace de conservation / protection des données.

Les risques les plus élevés sont souvent dans des fichiers tableurs disséminés sur des postes non sauvegardés et peu sécurisés (le mot de passe d'un tableur est aisément contournable). **C'est pour ce type de fichiers qui contiennent des données RH ou des données clients/prospects, que le risque de divulgation est le plus élevé** car il suffit d'une copie ou d'un envoi par mail, au contraire d'une base de données souvent sécurisée qui nécessite l'accès au logiciel. Un inventaire exhaustif est indispensable, et aboutit souvent à la détection d'un grand nombre de données personnelles, souvent inutiles, qui néanmoins sont réparties sur les postes de l'entreprise.

Pour les logiciels professionnels, les éditeurs de logiciels sont sensibilisés et vont généralement renforcer la sécurité ou le cryptage des données. Mais tout cela est inutile si les utilisateurs de l'entreprise se transmettent leurs mots de passe, ou bien laissent leurs postes non verrouillés en cas d'absence, ou bien si la gestion des droits utilisateurs n'est pas rigoureusement définie dans les logiciels.

L'établissement du registre des traitements peut être un gros travail selon l'activité de l'entreprise, mais c'est l'occasion de se poser un grand nombre de bonnes questions qui **amèneront de la sécurité à votre entreprise**, et pas uniquement vis-à-vis des données personnelles.

3/ ÉVALUER LES RISQUES ET LES PROCÉDURES A METTRE EN PLACE

Une fois le registre établi, il est souhaitable d'identifier les principaux risques pour l'entreprise en cas de perte ou fuite de données personnelles. Pour chacun des risques identifiés, il faudra décider de la réponse qui sera mise en oeuvre le cas échéant.

Au minimum, il faut définir la procédure pour deux situations :

1. Une personne demande la modification ou la suppression des données personnelles la concernant : à qui s'adresse-t-elle ?

2. Un incident provoque la diffusion non souhaitée de données personnelles : Comment en informer les personnes concernées en moins de 72 heures ?

4/ FAUT-IL NOMMER UN DPO ?

(DATA PROTECTION OFFICER = RESPONSABLE DES TRAITEMENTS DE DONNEES PERSONNELLES)

Nommer un DPO est obligatoire pour :

- les entreprises du domaine public,

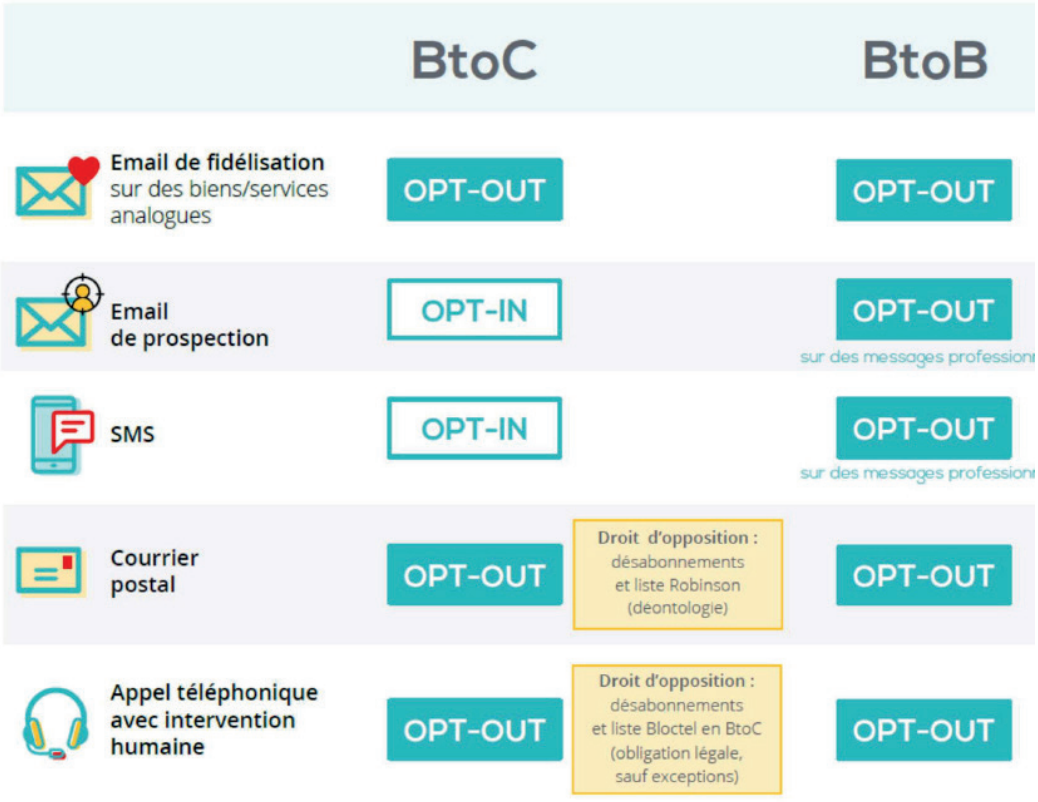
- les entreprises privées dont une activité majeure est de traiter des données personnelles à grande échelle, (vente à distance aux particuliers, compagnies d'assurance, sites de rencontre …)

- les entreprises qui traitent des données « sensibles » (santé, judiciaire, ...).

Pour la plupart des petites entreprises, il n'est donc pas obligatoire de nommer un DPO. Cependant, et même si la nomination d'un DPO n'est pas impérative pour votre entreprise, il est recommandé de désigner un référent pour la protection des données personnelles qui tiendra à jour ses connaissances sur le sujet et gèrera les principales obligations évoquées ci-dessus.

5/ FAUT-IL OBTENIR LE CONSENTEMENT DES AGRICULTEURS POUR LEUR ADRESSER UNE COMMUNICATION OU UNE OFFRE COMMERCIALE ?

Le RGPD ne change pas les règles applicables en prospection. Dans une relation B to B (de professionnel à professionnel) c'est donc le principe de l'opt out qui prévaut. Il n'est pas nécessaire de demander la permission à l'agriculteur avant de le contacter, par contre il est indispensable de l'informer du devenir de ses informations personnelles au moment de la collecte et de lui donner les moyens de se désabonner des listes d'envois.



(source SNCD mai 2018)

6/ ET SI JE NE SAIS PAS COMMENT DEMARRER ?

Garantir une méthode efficace de conservation / protection des données.

Dans certains cas, il est difficile d'évaluer le travail ou les démarches à réaliser. Il est préférable alors de prendre contact avec vos conseillers habituels qui sauront vous orienter. De nombreuses propositions vont vous parvenir pour vous vendre des prestations d'accompagnement estampillées « RGPD ». Assurément elle ne se valent pas toutes, et, sur ce sujet sensible, la confiance est le premier critère de choix d'un partenaire.

En tant que personnes, nous sommes tous attachés à ce que nos données personnelles soit protégées. En cohérence, il faut engager cette démarche dans toutes les entreprises qui en détiennent, afin de contribuer, chacun à son niveau, à la protection de tous.

RÉFÉRENT RGPD :

Christophe SEMONT

csemont@hyltel.fr

TÉL. 06 78 73 01 67.

RGPD Ready

MÉDIA DATA SERVICES - Avenue des Censives - TILLÉ - BP 50333 - 60026 BEAUVAIS
SAS au capital de 1 500 000 € 829 606 599 RCS Beauvais N° CCPAP 0319W92243