

Compte-rendu de Réunion RGPD

Date	17/04/2018
Réseau Mesure	Estelle DUFLOT – Claire ONFRAY
Lieu	MITUTOYO - Roissy
Objet	Le RGPD - Le nouveau règlement européen sur la protection des données personnelles

Le nouveau règlement européen sur la protection des données personnelles

Intervenant : **Philippe PRADAL**

Avocat WYSER LAW
ppradal@wyzerlaw.com
06.80.24.92.39

CF Présentation ci-jointe

Présentation générale :

- Qui est concerné ?
- Sur quoi est-ce que cela porte ?
- Comment le mettre en place ?

Le règlement européen sur la protection des données ou RGPD est un texte unique pour tous les états membres qui oblige toutes les entreprises et les administrations à respecter certaines règles concernant le traitement des données à caractère personnel (qui permet d'identifier une personne : nom, prénom ...). Le degré de précaution est bien supérieur pour des données dites sensibles : ex : médicales, orientations politiques.

Les données anonymisées sont exclues du RGPD. Pour tout partage de données vers des pays hors union Européenne il faut mettre en place un cadre contractuel.

Il sera **applicable le 25 mai 2018** (pas de report possible car il a été voté le 25 mai 2016 avec mise en application 2 ans plus tard, justement pour laisser le temps aux entreprises de s'adapter)

1^{er} changement fondamental :

La charge de la preuve : avant c'était la CNIL qui faisait les vérifications, maintenant la CNIL demandera à l'entreprise directement de prouver qu'elle est en conformité.

2^{ème} changement :



Principe de co-responsabilité entre les entreprises et les sous-traitants. Les sous-traitants devront justifier leur conformité au RGPD.

Le risque de conformité concerne le traitement des données mais aussi la collecte.

Risque PENAL : jusqu' a 5 ans d'emprisonnement

Risque ADMINISTRATIF : amende, mise en demeure ...

Traitement des e-mailings :

En B to C : Quand on parle d'e-mailing on parle de OPT IN pour leur consentement de manière positive

L'opt-in, c'est obtenir l'accord du destinataire de la communication (publicité, lettre d'information).

Cet accord s'obtient le plus souvent par une mention comme celle-ci : "Si vous souhaitez recevoir des propositions commerciales de nos partenaires par voie électronique, merci de cocher cette case" ;

En B to B : dans l'e-mailing on doit uniquement indiquer la possibilité de se désinscrire : OPT OUT et la source du contact.

« Vos coordonnées nous ont été transmises par un de nos adhérents dans le but de promouvoir le salon.... »

Si on a une adresse professionnelle d'un prospect : OPT OUT

Si l'e-mailing s'inscrit dans un service que l'on poursuit : pas besoin de consentement clairement exprimé.

L'adresse professionnelle : des lors que vous êtes apte à justifier que c'est une adresse utilisée dans le cadre professionnel.

- ➔ Si l'entreprise utilise une base données de personnes non professionnelles, elle doit recevoir leur consentement explicite, en revanche pour le traitement de données professionnelles, il est simplement nécessaire de permettre à la personne de s'exclure de cette base.

Obligation de sécurité :

Il faut sécuriser les données par des moyens proportionnels à votre entreprise.

Obligation d'information si votre base de données se fait hacker.

Droit à la portabilité :

Une personne peut récupérer les données la concernant traitées par un organisme, pour son usage personnel et peut les transférer d'un organisme à un autre.

Pour être conforme :

Il est nécessaire de désigner un responsable du traitement des données, s'il n'est pas désigné, c'est le mandataire social de l'entreprise qui joue ce rôle (le mandataire est dans tous les cas responsable pénalement).

1 - Etablir un registre des traitements:

- Dire d'où viennent les données
- Quelles sont les données
- Pourquoi je les collecte, l'utilisation
- Pour combien de temps je les collecte



La notion de traitement de données : l'utilisation de ces données

- Les données du personnel : bulletin de salaire, les contrats
- Un fichier de prospects : action commerciale, E -mailing

Une base de données peut servir pour plusieurs traitements

Il faut recevoir le consentement de la personne pour la liceité des traitements de données.

Les données du client peuvent être gardées 3 ans sans activité. Si nous envoyons une news letter a un prospect qui accepte de la recevoir sans même répondre, cela renouvelle le délais de conservation de 3 ans.

2 - Tenir un guide de procédure

3 - Nommer un délégué des données personnelles (non obligatoire pour les entreprises qui ne traitent pas un gros volume de données)

Il tient les registres, s'assure de la maintenance du guide de procédure.

Il peut être extérieur à l'entreprise : exemple un avocat spécialisé.

Il n'est pas responsable pénalement.

La CNIL PRECONISE UN PLAN EN 6 ETAPES

- Designner un pilote pas obligatoire sauf pour ceux qui traitent un fort volume de données
- Cartographier les risques : faire du recensement des données
- Prioriser : en fonction des différents traitements prioriser les actions à mettre en place
- Gérer les risques
- Processer : guide de procédure
- Documenter : pour pouvoir démontrer ce qu'on a fait

Ce cabinet d'avocats ici présent propose une prestation de mise en conformité au RGPD, pour les entreprises qui le souhaitent, sur une base de 3 jours.

Etape 1 : faire un diagnostic et plan d'actions

Etape 2 : formation

Etape 3 : mise en place de la documentation de conformité, mise à jour des formulaires

Tarifs MUTUALISES à partir de 10 sociétés.

[A ce jour plusieurs entreprises adhérentes du Réseau Mesure seraient intéressées pour ce service mutualisé.](#)

[Le Réseau Mesure va faire la demande auprès de 2 autres prestataires afin de disposer de plusieurs propositions.](#)