FICHE PRATIQUE

RGPG / GDPR: are you ready?

Note : cette fiche pratique peut ne pas être exhaustive. Elle ne se substitue pas à la réglementation en vigueur
Date d'actualisation : 1er janvier 2018

1. Explications, définitions

Le RGPG (en français), ou le GDPR (en anglais) : qu'est-ce que c'est ??

→ Il s'agit d'un nouvel arsenal juridique issu du droit européen pour la protection des données personnelles des personnes physiques qui sont « traitées » par les entreprises.

- Par « Données Personnelles » on entend : toute information permettant d'identifier directement ou indirectement une personne physique : nom, prénom, adresse, image (vidéo surveillance par exemple), adresse IP, login et mots de passe, données de localisation…

  Certaines données personnelles sont en outre qualifiées de « *sensibles* » et donnent lieu à des règles spécifiques (état de santé, orientations religieuses par exemple).

- Par « traitement » on entend : collecte, transfert, utilisation, conservation et destruction des données personnelles

Pourquoi ?

→ Parce que les anciennes règles ont été adoptées il y a plus de 20 ans, dans un contexte où le « big data » n'existait pas. Elles ne permettent pas de prendre en compte l'utilisation actuelle des données personnelles faites par les entreprises.

→ Le RGPD s'applique non seulement dans l'UE, mais également dans certains cas, en dehors de l'UE (responsable du traitement dans l'UE même si le traitement à lieu hors UE ; traitement hors UE de données personnelles de personnes en UE)

En quoi suis-je concerné en B to B ?

Le RGPD poursuit essentiellement 2 objectifs qui concernent directement les entreprises, même en B to B :

- Il accroît le droit des personnes à avoir accès à la façon dont sont collectées utilisées conservées et détruites leurs données personnelles, en leur donnant un droit d'agir en justice et de demander des dommages et intérêts si le traitement n'est pas conforme à la loi ;

- Il veut responsabiliser les entreprises qui traitent des données personnelles : des amendes conséquentes sont mises en place en cas de non-respect : **2% du CA mondial ou 10 millions d'euros** pour la première catégorie, jusqu'à **4% du CA ou 20 millions d'euros** pour les plus graves ;

→ Il faut être capable de montrer que l'on a conscience de traiter des données personnelles et qu'on le fait avec respect pour les libertés individuelles, avec une traçabilité et en transparence.

En tant qu'entreprise, vous collectez et traitez des données personnelles :

- RH : le département RH collecte, détient et transfère un très grand nombre de données personnelles ;
- Fournisseurs, contacts professionnels : les emails pro contiennent souvent dans leur signature, des données personnelles des interlocuteurs physiques de l'entreprise qui les envoie ;
- Formulaires de contact sur site internet : la encore toutes sortes de données personnelles sont collectées, conservées et traitées.

2. Concrètement que faut-il faire ?

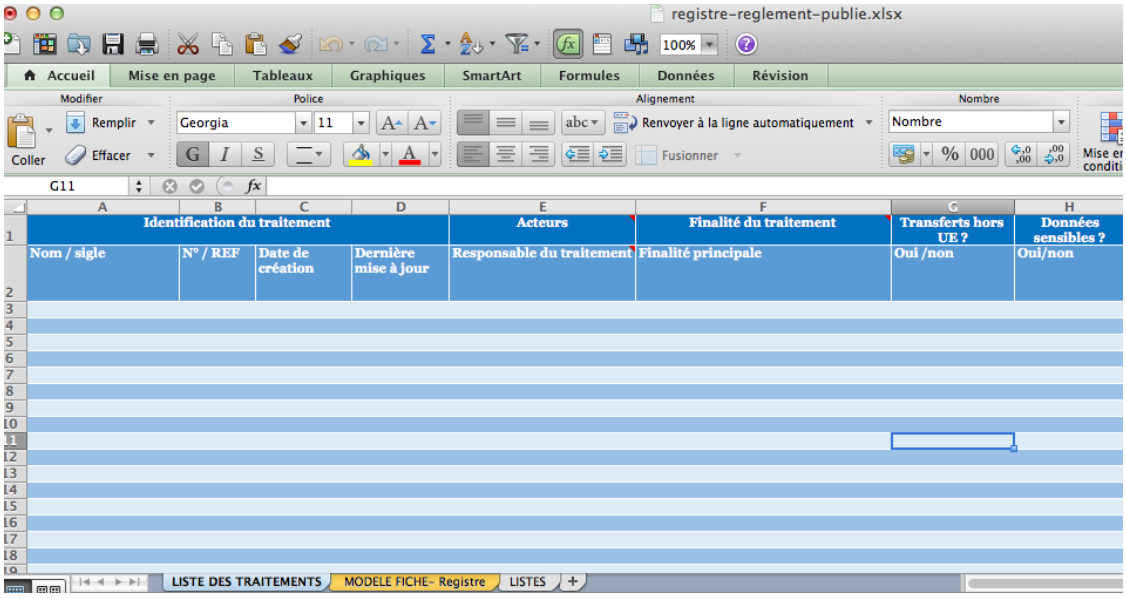
D'abord, il faut **s'assurer que le traitement des données personnelles effectué par l'entreprise est licite**. Le traitement est licite (article 6 du RGPD), notamment :

- si la personne a donné son consentement pour la finalité en cause ;
- si le traitement des données est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie

Les nouvelles dispositions nécessitent ensuite dans certains cas d'adopter des mesures concrètes qui sont principalement :

- ✓ **Mise en place et tenue, pour certaines entreprises (plus de 250 salariés, ou traitement en nombre de façon habituelle de données personnelles par exemple), d'un registre des activités de traitement** qui doit comporter des informations précises (article 30 du RGPD).

La CNIL (Commission Nationale Informatique et Libertés) fournit un modèle sous forme de tableau Excel : https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx



✓ **Information des salariés amenés à traiter des données personnelles :**

- Mise en place de clauses particulières dans le contrat de travail pour autoriser le traitement des données personnelles des salariés ;
- Mise en place et signature par les salariés amenés à traiter des données personnelles d'une Charte relative aux données personnelles (à inclure éventuellement dans la charte informatique de l'entreprise).

✓ **Procédure de notification des violations :**

- En cas de violation des données personnelles (par exemple en cas de hakeurs), le RGPD impose de le notifier à la CNIL dans les 72 heures après qu'on en ait connaissance.
- Il impose aussi de tenir un registre des violations de manière suffisamment détaillée.

✓ **Procédures permettant l'exercice des droits des personnes concernées :**

- Recueil et preuve du consentement des personnes concernées : lorsque le traitement est autorisé suite à un consentement de la personne concernée, il faut un acte positif du consentement. Les cases pré remplies ne sont plus suffisantes
- Portabilité des données : lorsqu'une personne demande à ce que ses données lui soient restituées, il faut le faire dans un format permettant l'interopérabilité : que ce soit facile pour la personne de re-transférer ses données à un autre interlocuteur
- Mise à jour régulière des données personnelles

Il faut pouvoir à tout moment identifier les données collectées, leur utilisation, leur mise à jour, leur destruction, pour pouvoir en justifiant à la personne concernée qui en fait la demande.

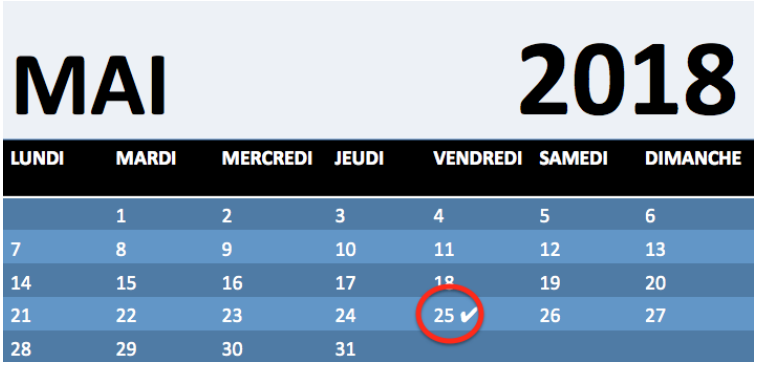
✓ **Désignation d'un Délégué à la Protection des Données (Data Protection Officer):**

- Pour certaines entreprises elle est obligatoire (article 37 du RGPD. Si l'entreprise réalise un suivi régulier et systématique de personnes à grande échelle par exemple cf. webmarketing). Pour les autres, elle peut être un moyen de s'assurer de la conformité au RGPD.
- Pour plus d'information : https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees

✓ **Mise à jour des contrats avec les sous-traitants :**

- La loi impose une obligation directe et une responsabilité propre des sous-traitants qui traitent des données personnelles pour le compte du responsable du traitement. Il faut donc s'assurer que le sous-traitant respecte et est en conformité avec le RGPD au moyen notamment, de clauses contractuelles le lui imposant.
    - ex : hébergeur, fournisseur email, logiciels de facturation, coursiers, partenaire chèques restaurant etc.

3. Entrée en vigueur :



4. Des outils pour m'aider :

La CNIL a mis en place **une méthodologie pour aider les entreprises** à se mettre en conformité.

Elle repose sur **6 étapes :**

- **https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes**

ETAPE 1 DÉSIGNER UN PILOTE

DÉSIGNER UN PILOTE

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

ETAPE 2 CARTOGRAPHIER

CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES

Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

ETAPE 3 PRIORISER

PRIORISER LES ACTIONS À MENER

Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

ETAPE 4 GÉRER LES RISQUES

GÉRER LES RISQUES

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA).

ETAPE 5 ORGANISER

ORGANISER LES PROCESSUS INTERNES

Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

ETAPE 6 DOCUMENTER

DOCUMENTER LA CONFORMITÉ

Pour prouver votre conformité au règlement, vous devez 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.

5. Pour une assistance personnalisée

Les avocats peuvent vous accompagner sur ce projet.

POPAI a mis en place un partenariat avec le cabinet d'avocats de Maître Tamara BOOTHESRTONE pour un accompagnement personnalisé suivant la méthode recommandée par la CNIL, à savoir :

→ Formation des équipes dans l'entreprise : sensibilisation au RGPD, présentation des mesures et réflexes à adopter dès à présent, présentation de la méthode pour cartographier les données.

- Cette formation peut être réalisée dès maintenant et tout au long de l'année.
- **TARIF : 600 € HT – Formation de 9h à 12h**

→ Analyse des résultats et recommandations.

- Cette étape intervient après la réalisation par l'entreprise de la cartographie de ses données. Idéalement, pour être prêt pour le 25 mai 2018, la cartographie des données devrait être terminée d'ici la mi-février pour permettre l'analyse courant mars.
- **TARIF : 900 € HT – Livrable : Rapport d'analyse**

→ Mise à jour de la documentation juridique.

- Cette étape devrait être réalisée courant avril pour être en ordre au 25 mai 2018.
- **TARIF : 1.000 € HT - Livrable : Documentation juridique conforme**

Pour tout renseignement contactez Maître Tamara BOOTHERSTONE, BK Conseil par email à tb@bkconseil.fr en indiquant dans l'objet « RGPD POPAI ».