

efcse.eu

## Règlement général sur la protection des données [RGPD] : mise en application aujourd'hui

Auteur : Corinne France, General Secretary EFCSE  
25 Mai 2018

### Garder le contrôle de ses données

Rappelons que le RGPD est un texte émis par l'Union Européenne qui oblige toutes les organisations, sociétés et autres entreprises, à clarifier leurs pratiques concernant le traitement qu'elles réservent aux données de leurs employés, de leurs clients et de leurs fournisseurs.

L'affaire Cambridge Analytica<sup>1</sup> a certainement renforcé l'impact de communication de la mise en application du RGPD.

Si nous y ajoutons une forme d'avantage collatéral, nous pouvons dire que ce type d'événement participe pleinement à la prise de conscience collective et individuelle de l'importance de garder (ou de reprendre) le contrôle de ses données.

#### *Données personnelles, de quoi s'agit-il ?*

Le règlement européen de 2016 abrogeant la directive de 1995 sur la protection des données définit la donnée personnelle comme *"toute information se rapportant à une personne physique identifiée ou identifiable [...] directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale"*.

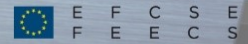
Concrètement, il peut s'agir d'un prénom, d'un nom, d'un email, d'une photo, d'empreintes digitales ou autre donnée biométrique, d'un numéro de carte bancaire, d'une géolocalisation ou encore de « cookies », ces petits modules informatiques qui traquent l'activités de tout internaute sur le Web, etc.

#### *Concernant les entreprises*

La mise en conformité avec le règlement (inventaire des fichiers, adoption de nouvelles procédures, garanties de transparence, etc.) représente pour les entreprises européennes une démarche assez « consommatrice » en ressources financières, humaines, techniques ou juridiques pour ne citer qu'elles.

---

<sup>1</sup> Cambridge Analytica : société spécialisée dans l'analyse des données à grande échelle et de conseil en communication, médiatiquement exposée en ce printemps 2018 suite à l'usage indu de données personnelles de dizaines de millions d'Américains.



efcse.eu

Les ETI, PME et TPE sont elles aussi concernées, dès lors qu'elles collectent ou qu'elles traitent de la donnée personnelle (leurs employés, leurs clients), elles disposent généralement de moins de moyens que les grandes entreprises, ce qui les met en situation contraignante pour assumer la mise en conformité avec le RGPD.

L'exemple de petites start up dont l'activité est centrée sur la collecte de données (production d'objets connectés et de capteurs) est significatif, ces entreprises voient en effet « circuler » des données parfois très sensibles, certaines liées au domaine de la santé, ce qui les met aux premières loges de l'obligation d'investir dans la gestion desdites données.

Au-delà de la contrainte apparente, cela permet aux entreprises de prendre pleinement conscience des règles de protection de l'information, quelle qu'elle soit, et de l'importance que cela revêt pour le maintien et le développement de leur activité dans une conjoncture économique qui ne peut plus guère s'arrêter aux frontières d'un pays, transition numérique oblige.

Dans ce contexte, pour les ETI, PME et TPE, plutôt qu'une simple contrainte, la mise en conformité avec le RGPD peut s'avérer être l'opportunité de s'interroger sur sa stratégie de gestion des DATA, tant en interne - amélioration de la sécurité et de la protection des données de l'entreprise, renforcement de la confiance et de la maîtrise des risques, ... - qu'en externe - renforcement de la confiance des clients, création de nouveaux services, ...

C'est un ensemble de facteurs pouvant concourir à une valorisation de l'image de l'entreprise, à un enrichissement de son champ d'actions commerciales et à sa capacité de se mettre en marche pour réussir cette transition numérique en cours et dont les perspectives d'évolutions n'en sont encore qu'à leurs prémices.

Mais... rappelons que début avril 2018 des chiffres issus de divers sondages donnaient encore quasi 60% des entreprises de l'Union Européenne "à risques" ou "en difficulté" d'être prêtes pour ce vendredi 25 mai.

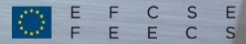
Même s'il existe de nombreux guides pour accompagner les entreprises dans leur démarche de mise en conformité RGPD, il semble que le « chantier » soit encore en œuvre. De plus, dans certains pays où il existait une réglementation forte en la matière, certaines entreprises se pensaient, à tort, déjà en conformité avec le règlement européen, il s'avère que sur certains points (informations sur les partenaires commerciaux, application du droit à l'oubli, ...), le RGPD est plus fort que les législations nationales et a obligé ces entreprises à travailler à marche forcée, mais sont-elles au rendez-vous à ce jour ?

### *Que se passe-t-il à partir du 25 mai 2018 ?*

Le Règlement est « obligatoire dans tous ses éléments et directement applicable dans tout État membre » à partir de ce 25 mai 2018.

C'est un règlement, il entre donc en vigueur directement, ce qui a pour conséquence pour les entreprises en tant que responsable de traitement pénalement responsable, de devenir amendable et soumis aux sanctions prévues, à savoir, pécuniaires - la plus grande valeur entre 4% du chiffre d'affaire mondial ou 20 millions d'euros - voire même des peines de prison (article 226-17 du Code pénal).

Concrètement, il faut montrer à l'autorité administrative indépendante de contrôle que le processus est en cours dans l'organisation, ceci via au minimum la désignation officielle d'une personne (interne ou externe à l'entreprise) pour cette démarche réglementaire, ou via une formation en cours. Il est également bienvenu de dresser dès maintenant la liste des traitements et des risques inhérents à la vie privée et aux libertés fondamentales des propriétaires des données à caractère personnel, en ajoutant si possible la liste des mesures correctives en cours et à venir.



efcse.eu

Dans les faits, les contrôles sur les nouvelles exigences du règlement ne devraient pas commencer avant cette fin d'année 2018. Il ne s'agit pas pour autant de laisser filer le temps sachant que les entreprises qui ont démarré la mise en conformité bien avant ce 25 mai se trouvent encore, à ce jour, dans les phases de mutations profondes.

Il est bien évidemment sous entendu qu'aucune fuite de données de la part de l'entreprise ne doit intervenir avant la mise en conformité totale avec le RGPD.

Nous savons que certaines organisations et associations de clients, consommateurs ou usagers sont d'ores et déjà en ordre de bataille pour entreprendre des actions collectives contre les entreprises non conformes au RGPD, avec le risque médiatique associé pour le contrevenant.

Il est donc plus qu'important de traiter en priorité, dès à présent, les grandes lignes directrices de la réglementation et de structurer un plan d'action moyen et long terme en suivant. C'est une véritable démarche d'amélioration continue qui doit se mettre en place, c'est un des rôles du DPO, sachant que certaines petites organisations n'en disposeront pas, il s'agit d'inscrire au plan stratégique de l'entreprise les actes pour rester en conformité avec le RGPD de façon pérenne.

EFCE invite les entreprises, spécialement les ETI, PME et TPE, à se joindre à ses Working Groups sur les thèmes ci-dessous afin de bénéficier d'un axe complémentaire d'accompagnement pour être au rendez-vous du RGPD sans tarder :

- GOUVERNANCE DE L'INFORMATION - Gouvernance / sectorielle - Création de valeur
- CONTEXTE REGLEMENTAIRE & JURIDIQUE EUROPEEN, STANDARD & LABELLISATION
- CYBERSECURITY : EDUCATION, FORMATION, COACHING

Contact via <https://www.efcse.eu/fr-fr/contact>