Le RGPD, nouvelle révolution de la gouvernance de l'information

Auteur : Isabelle CARRIO – Directrice Commerciale, Everteam.
Janvier 2018

Le Règlement Général sur la Protection des Données (RGPD) entrera en vigueur le 25 mai 2018 sur tout le territoire européen. Texte fondateur d'un nouveau rapport aux données personnelles, il fixe de nouvelles obligations aux entreprises en matière de gouvernance de l'information. Fruit de longues années de négociation entre les acteurs économiques et les législateurs, comptant quelque 99 articles et 173 considérants, il doit aider l'Europe et les entreprises à s'adapter aux nouvelles réalités du numérique. Le RGPD constitue un document de référence, certes contraignant mais aussi protecteur, redonnant aux citoyens le contrôle sur leurs données. Il fait ainsi évoluer la composition même des entreprises, créant des métiers inédits et incitant à l'utilisation de nouveaux outils, au service du nouveau « référent » que devient le DPO.

Le RGPD en bref

RGPD va permettre de tourner la page de la directive européenne de 1995 (95/46/CE). Elle régissait jusque-là l'accès des entreprises aux données personnelles, et présentait deux problèmes majeurs :

– D'une part, elle avait l'objet d'une transposition dans les différents droits nationaux, créant de fait des disparités et des inégalités entre les pays et entre les entreprises ;

– D'autre part, elle n'était pas assez dissuasive.

En tant que règlement européen (et non directive), le RGPD s'appliquera tel quel sur l'ensemble du territoire de l'Union. Il octroie de nouveaux droits aux consommateurs, et en renforce certains qui existaient déjà : le droit d'accès aux données, le droit d'être informé sur le traitement des données utilisées, le droit de rectification, le droit d'opposition, le droit de portabilité des données, dans certains cas, et le droit à l'oubli.

Imposant également une certaine réactivité aux entreprises, il s'apprête à chambouler l'organisation de celles-ci. Faisant naître, de fait, de nouveaux métiers et de nouvelles responsabilités.

Un nouveau métier, le DPO …

Parmi ces nouveaux métiers, celui de DPO (Data protection officer, ou Délégué à la protection des données, DPD) est le plus important. Il devient le chef d'orchestre du respect du RGPD en entreprise, étant tout à la fois juriste, pédagogue, porte-parole et informaticien. Sa nomination est ainsi obligatoire dans certains cas :

– Les autorités ou les organismes publics (les administrations, les ministères…) ;

– Les organismes (les entreprises, pour être plus clair) dont les activités imposent de réaliser un suivi régulier (c'est-à-dire « continu ou ponctuel », « récurrent ou itératif », « en cours ou se produisant pendant des périodes données ») et systématique (» prévu, organisé ou méthodique »), à grande échelle (selon le nombre de personnes concernées, mis en rapport avec le volume des données collectées, la durée de traitement et le périmètre géographique), des personnes

– Les organismes dont les activités de base leur imposent de traiter « à grande échelle » des données considérées comme sensibles (les données génétiques, biométriques, afférentes à la santé, à la religion, aux opinions politiques ou à l'appartenance syndicale…) ou des données en lien avec des condamnations pénales et/ou des infractions.

S'il peut être interne comme externe, le DPO est l'héritier du CIL (Cf article RGPD | CIL et DPO, ce n'est pas (vraiment) la même chose !). Selon le RGPD, il doit être désigné « sur la base de ses qualités professionnelles et, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir [ses] missions. » Conséquence ? Tous les CIL ne peuvent devenir DPO. En effet, une étude menée pour la CNIL en 2015 a démontré que ceux-ci proviennent de domaines d'expertise très variés (profil technique à 47 %, profil juridique à 19 % et profil administratif à 10 %). Lesquels ne collent pas forcément tous avec les exigences liées à l'exercice du métier de DPO !

Le DPO idéal possède des compétences dans de nombreux domaines :

Une expertise en matière de législation et de pratiques sur la protection des données ;

Une connaissance solide des opérations de traitement, des systèmes d'information et des logiciels utilisés dans l'entreprise, alliée à une sensibilité aux questions éthiques, morales et légales soulevées par ces pratiques ;

Une compréhension des risques légaux et judiciaires encourus par l'entreprise en cas de manquement aux exigences du RGPD…

… et de nouvelles pratiques pour les autres

Le RGPD n'a pas uniquement un impact sur l'organisation de l'entreprise, avec l'arrivée d'un DPO chargé de la tenue d'un registre d'activité. Il modifie aussi les activités d'autres professionnels.

Citons, par exemple, les avocats. Ils devront accompagner leurs clients dans la mise en place du RGPD, fournissant conseils et formations, permettant une application sereine du texte. Ils pourront également réaliser des audits et des études d'impact, un document clé dans le cadre de la gestion des risques, qui concerne les entreprises responsables de traitements de données comme les sous-traitants fournisseurs de solution qui permettent de mettre en œuvre ces traitements.

La DSI, elle aussi, voit ses activités changer. Et ce pour permettre au DPO d'appliquer les grands principes du RGPD :

- L'accountability. Soit « l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données ».
- Le Privacy by design. C'est-à-dire que chaque nouvelle application, chaque nouveau process, respecte bien les principes de l'accountability, dès la phase de conception.
- Le Privacy by default. Soit une limitation des traitements de données à ce qui est strictement nécessaire. Ni plus, ni moins !

Des outils pour les DPO et les DSI

DPO et DSI doivent s'appuyer sur un logiciel automatisé de gestion des données personnelles. Il leur permettra :

- De lister les traitements automatisés ;
- De créer une base documentaire mise à jour en temps réel ;

- D'identifier là où se trouvent les données sensibles dans les ensembles non-structurés, pour y accéder plus facilement et mener les éventuelles opérations correctives ;
- De cartographier l'ensemble des traitements ;
- De tenir le registre des traitements ;
- D'éditer un bilan annuel, qui pourrait être demandé par la CNIL en cas de contrôle ;
- De gérer l'ensemble des tâches demandées par les consommateurs (consultation, suppression, modification, anonymisation) …

Des conséquences dans tous les secteurs d'activité

Le RGPD s'appliquant à toutes les entreprises, et non pas uniquement celles concernées par la nomination d'un DPO, il imposera de nouveaux réflexes à des structures de tous les secteurs :

- Les assurances, où les échanges avec les clients constituent une mine de données personnelles exploitables ;
- La banque, où les données sensibles sont nombreuses ;
- Le e-commerce, où les goûts et moyens des consommateurs sont décryptés, analysés, exploités…

Le RGPD doit être vu comme une chance de renouveler la confiance entre les entreprises et les consommateurs, les premières « rendant » aux seconds le contrôle de leurs données personnelles. À condition, bien sûr, d'adopter les bons réflexes et les bons outils.

EFCSE a en son sein des compétences permettant d'accompagner ces transformations, son organisation en working groups, ouverts à tous ses membres, offre une approche concrète en adéquation avec la mise en conformité avec la réglementation européenne sur la protection des données personnelles.