GOUVERNANCE DES DONNÉES

LE *DATA PROTECTION OFFICER* : UNE CHANCE À SAISIR POUR LE SECTEUR BANCAIRE

Paul-Olivier Gibert

Président
Association française des correspondants à la protection des données à caractère personnel (AFCDP)

Président fondateur
Digital & Ethics

Dans moins d'un an, avec l'entrée en vigueur du RGPD, la protection des données personnelles sera nécessairement un élément essentiel de l'activité des établissements bancaires et financiers, au même titre que la maîtrise des risques prudentiels ou des impératifs de sécurité financière. Ainsi, la nomination d'un *Data Protection Officer* deviendra obligatoire dans bon nombre d'établissements financiers.

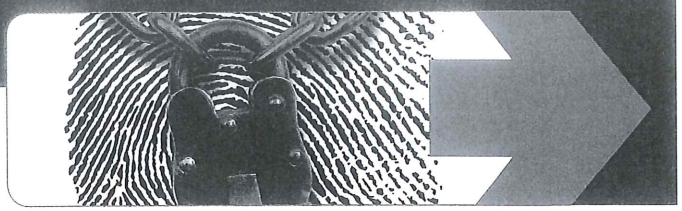
Si le numérique a changé nos sociétés, nos habitudes et nos économies de manière durable, les développements technologiques, et en particulier la multiplication des données personnelles, continuent à être sujet à débat. Le contexte actuel suscite craintes et questionnements chez nos concitoyens quant au respect de leurs données. Le règlement européen, la loi pour une République numérique et la négociation d'accords de transferts transfrontaliers de données tentent d'apporter des réponses à ces enjeux sociétaux majeurs.

L'architecture générale du règlement européen repose sur deux grands principes : la responsabilisation des organismes traitant des données personnelles et l'affirmation de la souveraineté des individus sur leurs données. En outre, ce texte va rendre la présence d'un *Data Protection Officer* (DPO) obligatoire dans un nombre considérable d'entreprises et d'administrations. D'ici un an, l'essentiel des établissements financiers auront désigné un DPO dans le cadre de leur programme de mise en conformité avec le RGPD.

LE RGPD CHANGE L'UNIVERS DE LA PROTECTION DES DONNÉES

Le règlement européen est certes fondé sur un cadre conceptuel peu différent de celui de la directive de 1995, qui elle-même ne faisait qu'actualiser les textes rédigés à la fin des années 1970 en Europe et en France de la loi Informatique et Libertés. Ses racines communes peuvent laisser penser que nous restons dans le même univers. Cette impression est trompeuse pour deux raisons : le RGPD installe des acteurs plus autonomes et plus responsables et octroie un pouvoir accru aux individus sur leurs données. En premier lieu, l'architecture de cette réglementation est profondément remaniée : à une logique de contrôle *a priori*, soit par des déclarations, soit par des autorisations, se substitue une logique de responsabilisation. Par ailleurs, le règlement allège considérablement les formalités préalables mais impose une responsabilisation des entreprises : les acteurs gagneront en souplesse et en simplification au prix d'une forte responsabilisation, avec le principe d'*accountability*, qui se décline en de nouvelles obligations (notification des violations de données, d'impact...), qui sont largement analysées par d'autres contributions de ce numéro de la Revue Banque. Cette responsabilisation est également marquée par les montants des sanctions susceptibles d'être appliquée en cas de manquement : celles-ci cesseront d'être symboliques pour atteindre des montants de mêmes niveaux que ceux appliqués pour les infractions aux réglementations financières et au droit de la concurrence.

En deuxième lieu, les législateurs européens ont souhaité que le RGPD porte l'affirmation de la souveraineté



des individus sur leurs données à caractère personnel. Le texte réaffirme tout d'abord les droits et principes figurant dans la directive de 1995, consolidés autour du principe de transparence :
– une information concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ;
– un exercice des droits des personnes facilité par le responsable de traitement ;
– l'encadrement du profilage ;
– la communication à la personne concernée de la violation de ses données.
Mais le texte prévoit aussi de nouveaux droits pour les personnes :
– le droit à la portabilité des données, c'est-à-dire la possibilité pour les personnes de gérer eux-mêmes leurs données personnelles et de pouvoir les récupérer pour les transférer vers un autre ;
– le droit à la limitation du traitement ;
– la consécration du droit à l'oubli.

UN TEXTE DE PORTÉE GÉNÉRALE

Enfin, il s'agit d'un texte applicable à l'ensemble des acteurs économiques, quels que soient leur secteur d'activité et leur localisation, puisque le règlement européen s'applique à tout organisme traitant de données ressortissant de l'Union européenne.
Du point de vue des établissements bancaires, si la mise en œuvre du RGPD peut sembler proche des différents chantiers réglementaires qu'ils doivent conduire pour être conformes aux exigences des différents régulateurs financiers, il existe des différences significatives : considérer que la conformité au RGPD est un sous-projet de la conformité BCBS 239 serait une importante erreur.

LE DPO, PIVOT DE LA MISE EN ŒUVRE DU RÈGLEMENT EUROPÉEN

Rappelons que le DPO, ce « CIL 2.0 », est le véritable pivot du règlement européen et qu'il devra être le garant de la conformité au règlement européen de l'organisation.
Ses missions sont nombreuses et exigeantes : veiller à la réalisation des analyses de risques et des études d'impacts, être l'interlocuteur privilégié en cas de violation de données personnelles (il devra veiller à ce que cette violation soit documentée) et le point de contact des personnes concernées, veiller à ce que les demandes de droit d'accès soient satisfaites en un mois, etc.
Le Correspondant informatique et libertés (CIL) qui préfigure largement le DPO a été selon les retours d'expériences perçus au sein de l'AFCDP, très bénéfique pour les organismes qui les ont désignés [1]. C'est de fait une fonction qui ne s'improvise pas : le DPO devra connaître le règlement, savoir communiquer, comprendre le fonctionnement d'un SI. C'est ainsi que l'AFCDP préconise une « clause du grand-père », qui permet aux CIL qui le souhaitent d'être confirmés en tant que DPO.
L'Association a réalisé de nombreux outils permettant aux organisations et aux futurs DPO de structurer et formaliser cette fonction avec notamment une fiche de poste et une lettre de mission. Au-delà de ces aspects techniques, il faut bien saisir les enjeux sous-jacents de la mise en conformité avec le RGPD : ce texte vise notamment à rééquilibrer les relations entre les individus et les responsables de traitement et leurs sous-traitants. Il convient ainsi de considérer les nouvelles attentes sociétales : la bonne gouvernance des données personnelles sera, dans les prochaines années, un enjeu central de la relation entre les organisations et les individus. Le nouveau droit à la portabilité des données illustre cette volonté de rééquilibrage portée par le règlement européen.
Pour que la profession bancaire puisse pleinement profiter de la désignation des DPO pour renforcer ses relations avec ses clients, les DPO du secteur devront être clairement positionnés pour permettre ce nouvel équilibre sur l'utilisation des données personnelles entre les individus et les responsables de traitement porté par le RGPD. ■

« L'architecture générale du règlement européen repose sur deux grands principes : la responsabilisation des organismes traitant des données personnelles et l'affirmation de la souveraineté des individus sur leurs données. »

[1] Cf. « "J'ai désigné un CIL et je m'en félicite" – Dix responsables de traitement témoignent » : https://www.afcdp.net/J-ai-designe-un-CIL-et-je-m-en.

REPÈRES

Appréhender le changement profond dans l'utilisation des données à caractère personnel

■ Créée en 2004, l'AFCDP (Association française des correspondants à la protection des données à caractère personnel) regroupe tous les professionnels concernés par la protection des données personnelles et la conformité aux lois relatives à la protection de la vie privée dans les entreprises, les établissements publics, les collectivités territoriales, les associations, etc. Elle compte plus de 750 membres (dont 600 personnes morales) et regroupe plus de 2 000 professionnels de la conformité. Ses adhérents ont des profils divers : correspondants informatique et Libertés (CIL), délégués à la protection des données, *Data Privacy-Protection Officers* (DPO), juristes, avocats, spécialistes des ressources humaines, informaticiens, professionnels du *marketing* et du e-commerce, RSSI et experts en sécurité, *Risk Managers*, qualiticiens, archivistes et *Record Managers*, déontologues, consultants, universitaires et étudiants. L'association encourage la discussion et les échanges d'informations en matière de protection des données personnelles, dans le but de faciliter la communication entre ses membres et de promouvoir les meilleures pratiques. L'AFCDP entretient un dialogue avec la CNIL et d'autres autorités concernées au niveau français et européen par la protection des données personnelles. En 2011, en compagnie de la GDD (Allemagne), la NGFG (Pays-Bas) et l'APEP (Espagne), l'AFCDP a fondé la CEDPO (Confédération européenne des associations de DPO). L'Irlande, la Pologne et l'Estonie ont rejoint la confédération courant 2014. Cette confédération porte au niveau de Bruxelles la voix des professionnels concernés par le futur règlement européen sur les données.
Pour l'association, la protection des données est la réponse concrète qu'il faut apporter au contraste créé entre des pratiques technologiques de plus en plus capables d'affecter la vie privée des citoyens, et la protection légitime des droits et libertés fondamentaux, et en premier lieu du droit à la vie privée.