

La Présidente

Monsieur Jean-Louis BANCEL
Président
OFFICE DE COORDINATION BANCAIRE ET
FINANCIERE
116 BOULEVARD HAUSSMANN
75008 - PARIS

Paris, le 20 SEP. 2017

N/Réf. : IFP/MBI/CS171150
A rappeler dans toute correspondance

Monsieur le Président,

L'Union européenne s'est dotée en 2016 d'un nouveau cadre juridique visant à renforcer et à harmoniser les règles et principes qui régissent la protection des données à caractère personnel des citoyens de ses Etats membres. Les profondes modifications introduites par le règlement européen 2016/679 du 27 avril 2016, seront applicables dès le 25 mai 2018.

Ce nouveau cadre repose sur une logique de responsabilisation des acteurs, qu'ils soient « responsables de traitements » de données à caractère personnel (donneurs d'ordres) ou sous-traitants. Tout organisme qui traite des données personnelles devra ainsi pouvoir justifier à tout moment de sa conformité aux obligations posées par le règlement (logique d'« *accountability* »). Le non-respect de ces obligations pourra faire l'objet de sanctions pécuniaires prononcées par les autorités de contrôles (les « CNIL » européennes) et pouvant s'élever pour les entreprises, selon le Règlement, jusqu'à 4% du chiffre d'affaires annuel mondial total ou à 20 millions d'euros, le plafond le plus élevé étant retenu.

Ces exigences auront une résonance particulière dans le secteur bancaire compte tenu des enjeux forts existant au regard de la législation « informatique et libertés », qui ont d'ailleurs conduit la CNIL, en lien avec les professionnels, à engager des travaux sur un « pack de conformité banque » et à mettre à jour dans ce cadre plusieurs de ses référentiels.

Vos membres devront ainsi prendre, dans le cadre du nouveau Règlement, les mesures techniques et organisationnelles propres à garantir le respect des principes « Informatique et Libertés » (finalité des traitements, minimisation et sécurisation des données collectées, effectivité des droits des personnes concernées, etc.), en s'appuyant sur une large gamme d'instruments de conformité (en particulier études d'impact sur la vie privée, registre des activités de traitement, codes de bonne conduite et certification).

Cette nouvelle gouvernance interne de la protection des données reposera sur un acteur clé : le délégué à la protection des données, dont la désignation sera dans certaines hypothèses obligatoire selon l'activité de vos membres et/ou les catégories de données qu'ils traitent. La désignation de ce délégué pourra en tout état de cause être recommandée, y compris en dehors des cas de désignation obligatoire, compte tenu du rôle que cet acteur est appelé à jouer.

Ce délégué, qui succède au Correspondant Informatique et Libertés (CIL) dont il reprend les attributions, sera en effet le véritable « chef d'orchestre » de la démarche permanente de mise en conformité. Ses missions consisteront notamment à informer et conseiller l'organisme ainsi que ses employés ; à contrôler le respect du règlement européen, du droit national et des règles internes en matière de protection des données, via l'organisation d'audits en particulier ; à coopérer avec l'autorité de contrôle et à être le point de contact pour celle-ci.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Dans ce contexte, **il m'apparaît essentiel que l'OCBF sensibilise ses membres sur la nécessité de se préparer à ce nouvel environnement juridique**, sur les outils existant pour les accompagner dans cette démarche et sur les enjeux de gouvernance interne de la protection des données. Il est en particulier important de déterminer le caractère obligatoire ou non de la désignation d'une personne chargée de veiller au respect des dispositions légales applicables.

Pour leur permettre d'identifier au mieux les actions à mettre en œuvre, et de s'assurer ainsi une sécurité juridique optimale, je vous recommande d'inviter vos membres à consulter les rubriques «Banques – Assurances» et «Règlement européen» du site de la CNIL. Ils y trouveront en effet beaucoup d'informations sur la réglementation en cause et ses évolutions, ainsi que des liens vers les nombreux outils proposés par la Commission, en «avance de phase» par rapport au nouveau cadre juridique, aux fins d'accompagner les professionnels dans leurs démarches de mise en conformité.

Mes services (service des Correspondants Informatique et Libertés – correspondants@cnil.fr / 0153732222, touche 3) restent à votre disposition pour apporter tout renseignement complémentaire et soutenir votre organisme dans les actions qu'il décidera d'engager.

Je vous prie d'agréer, Monsieur le Président, l'expression de mes salutations distinguées.



Isabelle FALQUE-PIERROTIN