

PRÉFACE

L'exploitation et la valorisation des données personnelles sont au cœur de l'activité bancaire et financière, au-delà des exigences fortes en matière de connaissance client propre à ce secteur. Le respect du Règlement Général sur la Protection des Données Personnelles (RGPD) constitue donc un enjeu capital, impliquant un changement de culture et une véritable responsabilisation de chaque acteur. Si l'élévation considérable du montant des sanctions à hauteur d'un maximum de 4 % du chiffre d'affaires a engagé une prise de conscience du secteur, les outils introduits par la réglementation offrent l'opportunité de mieux maîtriser cet actif que constitue la « donnée personnelle ». Le défi pour les banques est, aujourd'hui, de l'insérer dans un plan de gouvernance plus global, alliant maîtrise du risque et préservation de la confiance des clients.

Une intégration réussie de ces nouvelles règles nécessite de comprendre l'esprit de la réglementation, d'identifier les acteurs impliqués et les mesures à adopter tout en les articulant avec le contexte et les spécificités du secteur concerné ; tant d'étapes à franchir que cet ouvrage explique avec clarté.

Rédigé par des praticiens expérimentés et à destination des professionnels du secteur bancaire et financier, ce *vade-mecum* apporte un éclairage global sur le RGPD tout en donnant du sens aux mécanismes mis en place par une explication de contexte et une mise en perspective avec les besoins des entreprises. Pour mieux guider les professionnels, les auteurs ont émaillé leur exposé d'exemples démontrant que l'intégration des principes de protection des données, dès la conception, suppose d'organiser un processus itératif et dynamique. Il est, en effet, essentiel d'éviter l'écueil consistant à établir une simple grille de mesures à appliquer de manière isolée, le RGPD s'inscrivant, pour les banques, dans un contexte réglementaire complexe et contraignant, mis en perspective dans cet ouvrage.

En passant d'un mécanisme de formalités préalables à un principe général d'*accountability*, le RGPD impose d'intégrer la conformité dans toutes les strates de l'entreprise et de démontrer de manière proactive

le respect des principes de protection des données. Il s'agit d'un exercice pluridisciplinaire nécessitant d'être articulé avec les autres processus de conformité interne et de maîtrise des risques propres au secteur bancaire, voire de s'appuyer sur ces derniers. Afin de préserver la confiance des clients et de limiter l'exposition aux risques, les auteurs offrent un panorama des obligations des professionnels, décliné sous forme de plan d'action associant aspects organisationnels, techniques, de sensibilisation, dont la réalité et la robustesse, dans le temps, appellent un système d'évaluation dynamique et proactif, permettant de garantir l'effectivité des mesures déployées.

En résumé, voici un *vade-mecum* à garder près de soi, en tant que référence pour orchestrer de manière complète et effective la mise en place d'une meilleure gouvernance en matière de protection des données personnelles ou, tout simplement, pour mieux comprendre les évolutions de l'écosystème bancaire visant à mieux maîtriser l'actif stratégique que constitue la donnée.

Clémence Scottez

*Chef du Service des Affaires économiques
Commission Nationale de l'Informatique et des Libertés*

TABLE DES MATIÈRES

Préface de Clémence Scottez

Chef du Service des Affaires économiques Commission Nationale de l'Informatique et des Libertés.....	7
---	---

Introduction	13
---------------------------	----

PARTIE I

L'Accountability au service de la protection des données	21
---	----

Chapitre 1

Les obligations des responsables de traitement et des sous-traitants	23
§1 L'obligation d'apporter la preuve et de documenter la conformité	23
§2 Une approche par les risques.....	28

Chapitre 2

La coresponsabilité de traitement et le nouveau rôle des sous-traitants	39
§1 La coresponsabilité de traitement	39
§2 Le nouveau rôle du sous-traitant	43

PARTIE II

Les droits des personnes concernées 51

Chapitre 1

Des droits historiques renforcés 55

§1 Le droit à l'information 55

§2 Le droit d'accès, de rectification et d'opposition..... 59

§3 Le profilage 62

Chapitre 2

De nouveaux droits 65

§1 Le droit à l'oubli 65

§2 Le droit à la portabilité des données 67

§3 Droit à la limitation du traitement 71

Chapitre 3

De nouveaux moyens pour assurer l'effectivité des droits des personnes 75

§1 L'élargissement du périmètre des personnes susceptibles d'engager un recours 75

§2 L'élargissement du périmètre des personnes susceptibles de voir leur responsabilité engagée 78

PARTIE III

Mettre en place un système de management de la protection des données 83

Chapitre 1

Mettre en place une gouvernance de la protection des données 87

§1 Le choix d'une autorité chef de file 87

§2 Le Délégué à la Protection des Données..... 91

Chapitre 2

Diffuser la culture Informatique et Libertés au sein de l'organisme 97

§1 La conduite du changement 97

§2 La *Privacy* au quotidien 100

Chapitre 3

Mesurer l'efficacité du système de management de la protection des données..... 105

§1 Mettre en place des contrôles de conformité 105

§2 La reconnaissance de la conformité
du système par un tiers externe 110

Conclusion 115

Annexe

Cartographie des principales finalités de traitement 119

Liste des encadrés 121
