

Remerciements

Les autrices tiennent à remercier les personnes suivantes pour leur précieuse contribution à cet ouvrage.

- M. Michel Bazet, Délégué à la protection des données, AG2R La Mondiale
- Mme Céline Bigoy, Documentaliste, chargée de veille au Service Information Documentation de la Commission nationale de l'informatique et des libertés (CNIL)
- M. Gerome Billois, Partner, Wavestone
- Mme Isaure de Châteauneuf, Directrice juridique Technologies de l'information et Déléguée à la protection des données, Compagnie de Saint-Gobain
- Mme Sophie Eveno, Chargée des affaires juridiques, Groupe Crédit social des fonctionnaires (CSF)
- M. Hervé Fortin, Délégué à la protection des données, Servier
- M. Florent Gastaud, Délégué à la protection des données externe, Mon DPO externe
- M. Paul-Olivier Gibert, Président de l'Association française des correspondants à la protection des données à caractère personnel (AFCDP)
- M. Jean-Marc Grémy, Président du Club de la Sécurité de l'information français (CLUSIF)
- Mme Isabelle Holié, Responsable Achats et *Executive Coaching*, IFCAM (entité du Groupe Crédit Agricole)
- Mme Mylène Jarossay, Présidente du Club des experts de la sécurité de l'information et du numérique (CESIN)
- Mme Dominique Jeanne, Déléguée à la protection des données, Banque de France
- Mme Émilie Kerdelhué, Déléguée à la protection des données par intérim, en charge du ministère de l'Éducation nationale, de la Jeunesse et des Sports

- Mme Brigitte Lafond, Directeur juridique, Groupe Crédit social des fonctionnaires (CSF)
- Mme Claire Levallois-Barth, Coordinatrice de la Chaire Valeurs et Politiques des informations personnelles de l'Institut Mines-Télécom, enseignant-chercheur en droit à Télécom Paris
- M. Fabrice Mattatia, Délégué à la protection des données, ministère de l'Intérieur
- Mme Myriam Quéméner, Avocat général près la cour d'appel de Paris, Docteur en droit
- Mme Delphine de Saint Cyr, Déléguée à la protection des données et RSSI, Bourse Direct
- Mme Albine Vincent, Cheffe du service des délégués à la protection des données, Direction de la Conformité à la Commission nationale de l'informatique et des libertés (CNIL)

Des mêmes autrices

Dans la même collection

Le Délégué à la Protection des Données Clé de voûte de la conformité

Aline Alfer, Amandine Kashani-Poor et Garance Mathias, 2017.

Hors collection

Valoriser une entreprise par la propriété intellectuelle Des *fintech* aux grands groupes, quelle stratégie de gestion des actifs immatériels ?

Charlène Gabillat et Garance Mathias, 2017.

ISBN : 978-2-86325-966-5

Code Géodif : G0070839

Diffusé par les Éditions d'Organisation, 1, rue Thénard, 75240 Paris Cedex 05.

Copyright © 2020. RB Édition, 18, rue La Fayette – 75009 Paris.

www.revue-banque.fr

Toute reproduction, totale ou partielle, de la présente publication est interdite sans autorisation écrite de RB Édition ou du CFC, conformément aux dispositions du Code de la propriété intellectuelle.

SOMMAIRE

PRÉFACE	15
INTRODUCTION	17
PARTIE I. Le DPO : un acteur au cœur de la conformité	19
A. Pourquoi désigner un DPO ?	20
1. Quand doit-on désigner un DPO ?.....	20
2. Est-il pertinent de désigner un DPO même si l'on n'est pas soumis à cette obligation ?	21
3. Peut-on confier la gestion de la protection des données à un collaborateur interne ou externe sans le désigner DPO ?	22
B. Qui est le DPO ?	23
1. Quelles sont les différentes typologies de DPO ?.....	24
2. Quelles sont les compétences du DPO ?.....	26
3. Quels sont les marqueurs de l'indépendance du DPO ?	28
C. Comment le DPO exerce-t-il ses missions ?	32
1. Quelles sont les démarches à effectuer en cas de désignation d'un DPO et en cas de fin de mission ?.....	32
2. Quelles sont les ressources allouées au DPO dans l'exercice de ses missions ?.....	34
3. Qui sont les alliés du DPO en interne ?	36
PARTIE II. Les missions du DPO : cas pratiques	43
Cas pratique n°1 : Les missions de sensibilisation et de formation du DPO	44
Cas pratique n°2 : La visibilité du DPO.....	47
Cas pratique n°3 : La qualification des parties.....	49

Cas pratique n°4 :	
Le casse-tête du DPO pour qualifier les responsabilités dans un groupe de sociétés.....	53
Cas pratique n°5 :	
Le rôle du DPO dans un appel d'offres	56
Cas pratique n°6 :	
La tenue du registre.....	59
Cas pratique n°7 :	
L'autonomie des équipes métiers.....	62
Cas pratique n°8 :	
L'accompagnement par le DPO dans la détermination des durées de conservation	64
Cas pratique n°9 :	
Le rôle du DPO dans la gestion des demandes d'exercice de droits	68
Cas pratique n°10 :	
Le rôle du DPO dans le cadre d'une AIPD.....	71
Cas pratique n°11 :	
La relation DPO – RSSI	74
Cas pratique n°12 :	
Le rôle du DPO dans la gestion d'une violation de données	80
Cas pratique n°13 :	
Le rôle du DPO dans le cadre d'une gestion de crise.....	84
Cas pratique n°14 :	
Les démarches du DPO en cas d'évolution du cadre réglementaire.....	86
Cas pratique n°15 :	
Les contrôles du DPO	89
Cas pratique n°16 :	
Les contrôles de la CNIL.....	92
CONCLUSION	97
POSTFACE	99

Annexe 1 :	
La veille RGPD pour les DPO.....	101
Annexe 2 :	
Exemple de lettre de mission du DPO	111
Annexe 3 :	
Exemple de note de service de nomination d'un relais informatique et libertés.....	113
Annexe 4 :	
Points clés de conformité autour de la fonction de DPO.....	117
Annexe 5 :	
Exemple de grille d'analyse du DPO	119
Annexe 6 :	
Gouvernance de la conformité dans le temps	123

PRÉFACE

Les professionnels qui évoluent dans l'univers de la protection des données personnelles vivent leur quotidien avec intensité depuis le 25 mai 2018, date d'entrée en application du Règlement général sur la protection des données (RGPD).

Alors qu'auparavant certains d'entre eux pouvaient se considérer comment isolés sur une « planète lointaine », l'exposition dont ils font l'objet désormais est sans commune mesure ! Ne doutons pas que c'est en particulier la capacité de sanction de l'autorité de contrôle prévue par le législateur européen qui a rendu la matière sensiblement plus crédible pour de nombreuses gouvernances. Naturellement, celles-ci se tournent vers leur délégué à la protection des données (ou *data protection officer* – « DPO ») pour bénéficier de ses conseils appropriés. En effet, les sujets et projets de l'entreprise qui s'appuient sur des données personnelles sont omniprésents dans nos activités professionnelles, à l'instar de nos vies privées.

C'est dans ce contexte qu'il apparaît indispensable à ces acteurs de la conformité que sont les DPO en devenir, ou DPO désignés auprès de la CNIL, de maîtriser parfaitement les exigences réglementaires de la fonction et ses pratiques métiers, tel que cet ouvrage ambitionne de vous faire découvrir.

Albine VINCENT

Cheffe du service des délégués à la protection des données
Direction de la Conformité à la Commission nationale de l'informatique
et des libertés (CNIL)

INTRODUCTION

Plus de deux ans après l'entrée en application du Règlement général sur la protection des données¹, le métier de Délégué à la protection des données (ou DPO)² n'a pas fini de révéler ses multiples facettes. Nous nous sommes ainsi interrogées sur le rôle du DPO et sur l'intérêt que pouvait représenter une telle fonction pour un organisme. Cet ouvrage s'adresse donc aux praticiens de la protection des données, qu'ils exercent depuis plusieurs années – avant l'avènement du DPO – ou qu'ils soient nouveaux venus dans la profession. Il est également destiné à tous ceux qui se veulent les alliés du DPO.

Quelle posture adopter en cas de désaccord sur la qualification des parties ? Comment le DPO peut-il intervenir dans le cadre d'un appel d'offres ? Quel est le rôle du DPO dans la détermination des durées de conservation des données ? Quelle méthodologie adopter dans la conduite d'une analyse d'impact relative à la protection des données ? Comment le DPO peut-il diffuser les bonnes pratiques en matière de protection des données ? Est-ce au DPO de notifier une violation de données ? Autant de questions qui nous permettent d'appréhender les missions du DPO à travers des situations concrètes et le retour d'expérience de professionnels. Parce que l'ouvrage porte davantage sur le DPO que sur les règles qu'il applique, nous avons choisi de ne pas revenir sur les grands principes consacrés par le RGPD³, mais plutôt de présenter au lecteur des pistes de réflexion sur sa pratique quotidienne, notamment dans le secteur bancaire et financier.

Nous nous sommes intéressées aux pratiques de celles et ceux que nous avons pu interroger et dont les contributions servent à illus-

-
- 1 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
 - 2 À l'instar du site de la CNIL, l'acronyme « DPO » pour « Data Protection Officer » sera utilisé.
 - 3 Voir l'Essentiel *Le délégué à la protection des données – Clé de voûte de la conformité*, Aline Alfer, Amandine Kashani-Poor et Garance Mathias, RB Édition, 2017.

trer nos propos tout au long de l'ouvrage. Les échanges que nous avons quotidiennement avec les personnes, DPO ou non, dans l'exercice de nos professions respectives ont aussi contribué à enrichir notre point de vue. Nous nous sommes également appuyées sur les lignes directrices du groupe de l'article 29 (G29) reprises par le Comité européen de la protection des données (CEPD), les décisions rendues par les autorités de contrôle et les juridictions.

Le DPO : un acteur au cœur de la conformité

Le RGPD institutionnalise le DPO en lui consacrant une section à part entière⁴. Il apparaît donc clairement que les institutions européennes ont souhaité faire du DPO un acteur clé de la conformité et de la démarche d'*accountability*⁵. Sa fonction doit être connue et reconnue au sein de l'entité en l'intégrant notamment de manière opportune dans les processus internes décisionnels. Comme a pu le rappeler l'autorité de contrôle belge : « Réduire l'association du DPO à sa simple information (*a posteriori*) concernant une décision [au sein de l'entité qui l'a désigné] vide sa fonction de son contenu »⁶.

4 RGPD, Chapitre 4, Section 4.

5 RGPD, article 5-2 (principe de responsabilité en langue française).

6 Autorité de protection des données, Chambre contentieuse, Décision quant au fond 18/2020 du 28 avril 2020, Numéro de dossier : AH-2019-0013, p. 14.