Table des matières

AVANT-PROPOS V

PRÉSENTATION DES CONTRIBUTEURS VII

PRÉFACE IX

PRINCIPALES ABRÉVIATIONS XI

1. LA DÉSIGNATION D'UN DPO 1

1.1. Le caractère obligatoire de la désignation d'un DPO et ses conséquences 2

1.1.1. Les critères de désignation 2

1.1.2. Les conséquences de la non-désignation d'un DPO obligatoire 7

1.2. Qui désigner, comment et quand ? 8

1.2.1. Qui désigner ? 8

1.2.2. Comment désigner un Cil ? 11

1.2.3. Quand désigner le DPO ? 14

1.2.4. Où désigner le DPO ? 14

1.2.5. La désignation est-elle possible si elle n'est pas obligatoire ? 15

2. LE PORTRAIT D'UN DPO 17

2.1. Le profil du DPO 17

2.1.1. Du Cil au DPO 17

2.1.2. La désignation en interne 19

2.1.3. La désignation sur la base d'un contrat de service 19

2.2. La formation du DPO 20

2.2.1. Le niveau d'expertise exigé 20

2.2.2. Une expertise en droit indispensable 21

2.3. Le rattachement du DPO 22

2.3.1. L'implication 22

2.3.2. L'indépendance 23

2.3.3. Les conflits d'intérêts 24

2.4. Les moyens 25

2.4.1. Les ressources nécessaires pour exercer ses missions 25

2.4.2. Le coût estimé de la mise en conformité 26

3. Les missions du DPO 27
3.1. Les premières missions du DPO 28
3.2. La conformité des traitements 29
3.3. La cartographie des traitements 30
3.4. Le DPO, point de contact 32
3.5. Le DPO, pédagogue et conseil 34
3.6. Le DPO et les missions d'audit 35
3.7. Le DPO et la sécurité des traitements 36
3.8. Le DPO et les études d'impacts 36
3.9. La certification du DPO 38

4. La réforme du droit de la protection des données 41
4.1. Le DPO et la minimisation des données collectées 41
4.1.1. Le principe de minimisation 42
4.1.2. Le rôle du DPO dans la minimisation de la collecte 42
4.2. Le DPO et l'application du consentement donné pour des finalités spécifiques 43
4.2.1. Le principe du consentement donné pour des finalités spécifiques 43
4.2.2. Le rôle du DPO dans la protection du consentement 44
4.3. Le DPO et la protection des données dès la conception 45
4.3.1. Le principe de protection des données dès la conception 45
4.3.2. Le rôle du DPO dans la protection des données dès la conception 45
4.4. Le DPO et la protection des données par défaut 47
4.4.1. Le principe de protection des données par défaut 47
4.4.2. Le rôle du DPO dans la protection des données par défaut 47
4.5. Le DPO et le principe d'*accountabilty* 48
4.5.1. Le principe d'accountabilty 48
4.5.2. Le rôle du DPO au regard du principe d'accountability 49

5. Les outils de conformité à mettre en place 51
5.1. Le DPO et la conformité 51
5.1.1. L'utilité de se doter d'outils de conformité 51
5.1.2. Les procédures complémentaires 52
5.2. Les outils de conformité 53
5.2.1. La formation, la sensibilisation et l'information 53
5.2.2. Le registre des activités de traitements 56

5.2.3. La méthode fondée sur une liste des systèmes d'information de l'entreprise ... 58
5.2.4. La méthode fondée sur les métiers exercés dans l'entreprise ... 60
5.2.5. L'outil de tenue du registre des activités de traitement ... 61
5.3. Le contrat conforme aux exigences de l'article 28 du RGPD ... 62
5.3.1. L'état de lieux des contrats en cours ... 62
5.3.2. La qualification des acteurs ... 63
5.4. Les outils de gouvernance ... 64
5.4.1. Les politiques de gouvernance des données à caractère personnel ... 64
5.4.2. Les règles d'entreprise contraignantes ... 65
5.4.3. Les codes de conduite ... 65
5.4.4. La certification ... 66
5.5. Les outils de contrôle ... 67
5.5.1. L'autoévaluation continue ... 67
5.5.2. Le contrôle interne permanent ... 68
5.5.3. L'audit ... 69
5.6. Les outils d'évaluation et les indicateurs ... 69

6. L'organisation de la fonction ... 71
6.1. La gouvernance des données personnelles ... 71
6.2. Les grandes tendances de la gouvernance des données personnelles ... 73
6.3. Les modèles possibles de gouvernance des données personnelles ... 75
6.4. Les mesures organisationnelles ... 76

7. Les sanctions applicables ... 79
7.1. La mise en place d'un régime européen de réponse aux violations ... 79
7.1.1. Le RGPD : un régime européen ... 79
7.1.2. Les aménagements réalisés en France ... 83
7.2. Les sanctions dans le RGPD ... 85
7.2.1. Le large pouvoir d'adoption de mesures correctrices par les autorités de contrôle ... 85
7.2.2. Les conditions générales d'imposition des amendes administratives ... 87

8. La sécurité et le DPO ... 93
8.1. Qu'est-ce que la sécurité en matière de protection des données personnelles ? ... 94
8.1.1. La sécurité du système d'Information ... 94

8.1.2. L'évolution du modèle de sécurité : de la défense périmétrique à un besoin croissant de détection et de prédiction 97
8.2. Les enjeux 98
8.2.1. Le contexte international inquiétant : le patrimoine informationnel comme cible privilégiée 99
8.2.2. Les ambitions du règlement en matière de sécurité : un sujet devenu prioritaire et central 101
8.3. Le DPO confronté à la sécurité des données : nouveaux challenges et opportunités 101
8.3.1. Le concept d'accountability imposant un contrôle de la sécurité pendant tout le cycle de vie des données 102
8.3.2. La place croissante de la gestion des risques dans la mise en œuvre de la sécurité 103
8.3.3. La conception « privacy » et « security by design » 104
8.3.4. Le choix de sous-traitant offrant des garanties suffisantes en matière de sécurité 105
8.3.5. La gestion efficace des failles de sécurité et les relations avec les tiers 106
8.3.6. La sécurité dans le contrat 107

9. Les règles de responsabilité 111
9.1. Le régime de responsabilité 111
9.1.1. La notion de responsable du traitement 111
9.1.2. Le droit à réparation 112
9.2. Le régime de réparation 113
9.2.1. La mise en œuvre de la responsabilité 114
9.2.2. La responsabilité conjointe 115

10. DPO et sous-traitant 119
10.1. Le DPO de l'organisme sous-traitant 120
10.1.1. La désignation du DPO et ses missions 120
10.1.2. Les obligations du DPO du sous-traitant 121
10.1.3. Exemples de mesures et de conseils 123
10.2. Le DPO d'un organisme responsable de traitement face aux sous-traitants 126
10.2.1. Le référencement des sous-traitants 127
10.2.2. Le contrat entre le responsable de traitement et le sous-traitant 127

10.2.3. L'audit 129

11. Le DPO dans le secteur de l'assurance 131
11.1. Le cas particulier des données de santé 131
11.1.1. La donnée relative au handicap d'une personne 132
11.1.2. Les données concernant la santé 132
11.1.3. L'hébergement des données de santé 135
11.1.4. Un droit à l'oubli spécifique 136
11.1.5. Un droit d'accès spécifique 137
11.2. Le cas particulier du NIR 137
11.3. Le cas particulier des traitements d'assurance 139
11.3.1. Le pack de conformité assurance 139
11.3.2. Le pack de conformité véhicules connectés et données personnelles . . 140
11.3.3. Le traitement des données par les agents généraux d'assurance 141
11.3.4. L'obligation d'analyse d'impact 141

12. Le DPO et la cyberassurance 145
12.1. Du cyber-virus à l'hygiène cyber 146
12.2. Des cyber-couvertures initialement plutôt tacites 148
12.3. Des couvertures cyber maintenant souvent plus explicites 150
12.4. Une cyber-assurance mitigée des sanctions administratives 151
12.5. Un prix du cyber-risque encore imprécis 152

13. Le DPO et le droit d'accès 155
13.1. Cerner et comprendre le droit à l'information et le droit d'accès 156
13.1.1. La définition du droit à l'information 157
13.1.2. Les questions pratiques de compréhension du droit à l'information . . 157
13.1.3. La définition du droit d'accès 161
13.1.4. Les questions pratiques 162
13.1.5. Les limites du droit d'accès 165
13.2. La réponse du DPO à une demande de droit d'accès 169
13.2.1. La réception de la demande 169
13.2.2. Le traitement de la demande 171
13.2.3. La réponse au demandeur 173
13.2.4. Les difficultés pratiques auxquelles un organisme peut être confronté 175

14. Le DPO dans le secteur bancaire et financier 177
14.1. La désignation d'un DPO : une quasi-obligation 177
14.1.1. La notion d'activités de base dans le secteur bancaire 177
14.1.2. La notion de traitements à grande échelle dans le secteur bancaire .. 179
14.1.3. La notion de traitements exigeant un suivi régulier et systématique dans le secteur bancaire 179
14.2. Le rôle du DPO dans le secteur bancaire 180
14.2.1. La tenue du registre des activités 181
14.2.2. La réalisation d'analyses d'impact (PIA) 181
14.2.3. Le respect du principe de minimisation 184
14.2.4. La limitation de la durée de conservation des données 184
14.3. Le DPO et la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) 185

Liste des annexes 187

Annexe 1 : Référentiel de certification des compétences du DPO 189

Annexe 2 : Référentiel d'agrément d'organismes de certification pour la certification des compétences du DPO 191

Annexe 3 : Mesures d'évaluation du niveau de sécurité des données personnelles préconisées par la Cnil 193

Annexe 4 : Principales durées de conservation des données bancaires selon leurs finalités 195

Annexe 5 : Lexique 197

Annexe 6 : Bibliographie 201

Annexe 7 : Liste des figures et schémas 205

Annexe 8 : Index 207