

Avant-propos

Chapitre 1
Introduction

- 1. Le RGPD 11
- 2. Le RGPD et la loi de 1978 13
- 3. Approche(s) du RGPD 15
- 4. Objet et sujets du RGPD 16
- 5. Application dans le temps du RGPD..... 17
- 6. Application dans l'espace du RGPD 17
- 7. Impact du RGPD 18
- 8. RGPD : obligations et opportunités 19
- 9. Retours d'expérience : 10 constats et propositions 21
 - 9.1 Identifier les rôles des acteurs du RGPD 21
 - 9.2 Régulariser les relations « responsable/sous-traitant » 22
 - 9.3 Désigner un gestionnaire d'activité de traitement 23
 - 9.4 Ajuster les processus « métier » 23
 - 9.5 Conserver, archiver, détruire 23
 - 9.6 Intégrer la fonction de référent à la sécurité
du système d'information 24
 - 9.7 Assurer la gouvernance du RGPD dans le temps 25
 - 9.8 Impliquer les éditeurs de solutions logicielles..... 26
 - 9.9 Mieux gérer les violations de données à caractère personnel. . . 26
 - 9.10 Sensibiliser : une démarche essentielle 27
- 10. 5 ans de RGPD : témoignages 27

Chapitre 2
Une première approche du RGPD

- 1. Structure du document officiel 47
 - 1.1 Considérants..... 47
 - 1.2 Articles..... 48

2. Principaux termes et définitions	50
3. Les deux piliers du règlement.	59
4. Principes fondamentaux juridiques.	60
4.1 Principes fondamentaux relatifs aux traitements de DCP.	60
4.1.1 Licéité, loyauté et transparence	61
4.1.2 Finalité	64
4.1.3 Proportionnalité des données	65
4.1.4 Exactitude des données	66
4.1.5 Conservation des données	66
4.1.6 Sécurité des données	69
4.1.7 Responsabilité (accountability)	71
4.2 Principes fondamentaux relatifs aux droits des personnes concernées.	77
4.2.1 Information et communication	78
4.2.2 Droit d'accès aux DCP.	79
4.2.3 Droit de rectification.	80
4.2.4 Effacement (droit à l'oubli).	80
4.2.5 Droit d'opposition à un traitement	81
4.2.6 Droit à la formulation de directives « décès ».	82
4.2.7 Droit à la limitation du traitement	83
4.2.8 Droit à la portabilité des données.	84
5. Le pilier "sécurité des DCP"	85
6. Du droit au management.	85

Chapitre 3

Un système de management

1. Introduction	87
2. Le système de management	88
2.1 Qu'est-ce qu'un système?.	88
2.2 Qu'est-ce qu'un système de management ?	89
2.3 Caractéristiques d'un système de management	90

3.	Conception du SMDCP	91
3.1	Finalité du système.....	91
3.2	Interaction du système avec son environnement.....	91
3.3	Objectifs du système	93
3.4	Éléments qui le composent	93
3.5	Autres caractéristiques.....	94
4.	Processus du SMDCP.....	94
4.1	Définition	94
4.2	Déterminer le nombre et l'intitulé des processus	95
4.3	Objectifs, activités, éléments de sorties et mesures techniques et organisationnelles attachées aux 12 processus.....	98
4.3.1	Processus - Accountability	99
4.3.2	Processus - Traitements et transferts de données	100
4.3.3	Processus - Droits des personnes concernées.....	102
4.3.4	Processus - Sous-traitants	103
4.3.5	Processus - Privacy by design	104
4.3.6	Processus - Privacy by default.....	106
4.3.7	Processus - Privacy Impact Assessment (PIA)	107
4.3.8	Processus - Sensibiliser, former et communiquer	108
4.3.9	Processus - Exigences, sollicitations, violations, poursuites.....	109
4.3.10	Processus - Évaluer et auditer	111
4.3.11	Processus - Gérer la documentation et les preuves	112
4.3.12	Processus - Piloter le SMDCP	113
5.	Outils du SMDCP.....	115
6.	Ressources humaines	116
7.	Autres caractéristiques du SMDCP.....	120
7.1	Fonction de contrôle ou de feedback.....	120
7.2	Politiques du système.....	122
7.2.1	Politique générale de protection des données à caractère personnel.....	122
7.2.2	Politique de gestion des données à caractère personnel	123
7.3	Les référentiels du système de gestion	123

7.4	Propriétés.	124
7.4.1	Il est transversal	124
7.4.2	Il est décrit	124
7.4.3	Il est en amélioration constante	125
7.4.4	Il fournit des preuves.	128
8.	Gouvernance du SMDCP.	128
8.1	Qu'est-ce que la gouvernance ?	128
8.2	Principes de la gouvernance	129
8.2.1	Collégialité	130
8.2.2	Transparence du cheminement décisionnaire	130
8.2.3	Gestion des risques et des conflits	130
8.2.4	Communication	131
8.3	Acteurs de la gouvernance	132
8.4	Structure de gouvernance et rythme.	133
8.5	Tableau de bord de la gouvernance	133
9.	Intégration du SMDCP avec des systèmes de management existants	135
9.1	Juxtaposition	138
9.2	Harmonisation	139
9.3	Mutualisation	140
10.	En résumé	141

Chapitre 4

Mise en œuvre du système de management

1.	Introduction	143
2.	Choix de la méthode	143
3.	Phase de conception	145
3.1	Étape 1 : Définir	146
3.1.1	Objectifs	146
3.1.2	Activités	146
3.1.3	Livrables	151

3.2	Étape 2 : Collecter	151
3.2.1	Objectifs	151
3.2.2	Activités	152
3.2.3	Livrables	155
3.3	Étape 3 : Organiser	156
3.3.1	Objectifs	156
3.3.2	Activités	156
3.3.3	Livrables	164
3.4	Étape 4 : Protéger	164
3.4.1	Objectifs	164
3.4.2	Activités	165
3.4.3	Livrables	167
3.4.4	Focus sur la rédaction de la politique de gestion des données à caractère personnel	167
3.5	Étape 5 : Clôturer la phase	177
3.5.1	Objectifs	178
3.5.2	Activités	178
3.5.3	Livrables	179
4.	Phase de réalisation	180
4.1	Les trois étapes de la phase de réalisation	180
4.2	Étape 1 : Exécuter	181
4.2.1	Objectif	181
4.2.2	Activités	181
4.2.3	Livrables	188
4.3	Étape 2 : Mesurer	188
4.3.1	Objectif	188
4.3.2	Activités	189
4.3.3	Livrables	190
4.4	Étape 3 : Clôturer le projet	190
4.4.1	Objectif	190
4.4.2	Activités	190
4.4.3	Livrables	191

5. Organisation du projet	192
5.1 Échéancier du projet	192
5.2 Ressources du projet	193
6. Cycle de vie du SMDCP	194
7. Facteurs clés de succès du projet	195

Chapitre 5

La sécurité des DCP et PIA

1. Système d'information et sécurité	197
1.1 Rappel sur le système d'information	197
1.2 Sécurité des systèmes d'information	198
1.3 Normes et référentiels de sécurité des systèmes d'information	201
2. Sécurité des DCP : que dit le règlement ?	204
3. Privacy by default	206
4. Analyse d'impact relative à la protection des données	213
5. Traitements et facteurs de déclenchement d'un PIA	214
6. Déroulement d'un PIA	217
6.1 PIA et respect des principes fondamentaux	218
6.2 PIA et mesures de sécurité	219
6.2.1 Prise en compte du contexte	220
6.2.2 Appréciation des risques	220
6.2.3 Traitement des risques	222
6.2.4 Consultation préalable	224
6.2.5 Acceptation des risques	225
6.2.6 Outillage	225
7. Privacy by design	225

Chapitre 6

Le(s) responsable(s) et le(s) sous-traitant(s)

1. Introduction	229
2. Notion de responsable	230
2.1 Interprétation de la notion	230
2.2 Personnes responsables.	232
3. Notion de responsable conjoint.	234
4. Contrat entre responsables conjoints	237
5. Sous-traitant	238
5.1 Définition	238
5.2 Choix du sous-traitant	241
5.3 Contrat de sous-traitance et sous-traitance de données à caractère personnel.	243
5.4 Sous-traitance initiale et sous-traitances successives.	245
6. Formalisation des relations entre responsable de traitement et sous-traitant	246
7. Aspects internationaux	247
8. Contenu du contrat	248
9. Résolution du contrat.	250

Chapitre 7

Les transmissions de données

1. Distinction entre les transmissions, les transferts européens et les transferts internationaux de données	253
2. Transmission de données en France	257
3. Traitements transfrontaliers	259
3.1 Définition	259
3.2 Particularité de ces traitements	259
3.3 Détermination de la loi applicable en cas de traitement transfrontalier	261
3.4 Compétence en cas de recours	266

4. Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales.	267
4.1 Principe général applicable aux transferts.	268
4.2 Transferts fondés sur une décision d'adéquation	268
4.3 Transferts moyennant des garanties appropriées.	271
4.4 Règles d'entreprise contraignantes	274
4.4.1 Généralités	274
4.4.2 Exemples de règles d'entreprise contraignantes (BCR).	277
4.5 Transferts ou divulgations non autorisés par le droit de l'Union.	277
4.6 Dérogations pour des situations particulières	278
4.6.1 Autorisation de la personne concernée	278
4.6.2 Transferts nécessaires	279
4.6.3 Transferts réalisés à partir d'un registre public	279
4.6.4 Transferts à portée limitée	280
4.7 Limites au transfert de catégories spécifiques de données à caractère personnel.	281
5. Traitement d'un responsable ou sous-traitant de pays tiers vers l'UE.	281
5.1 Applicabilité du règlement.	282
5.2 Désignation d'un représentant	283
5.3 Modalités et portée de la désignation	283

Chapitre 8

Le contrôle de l'autorité, la CNIL

1. Introduction	285
2. Traitement des réclamations	286
3. Enquête	287
4. Accès aux locaux du responsable du traitement ou du sous-traitant.	287
5. Notification d'une violation	289
6. Mise en demeure.	289

7. Rappel à l'ordre	290
8. Injonctions diverses	290
9. Mesures coercitives.	291
10. Caractère contradictoire des procédures	291
11. Publicité des mesures	292
12. Coopération entre autorités centrales.	292

Chapitre 9 Les sanctions

1. Diversité des sanctions.	293
1.1 Sanctions prononcées par l'autorité de contrôle.	294
1.1.1 Mesures correctrices	294
1.1.2 Amendes administratives	298
1.2 Sanctions pénales	302
1.3 Condamnation à des dommages-intérêts	306
1.4 Sanctions liées au caractère illicite du traitement	308
1.4.1 Nullité des contrats.	308
1.4.2 Licenciement non fondé	309
2. Représentation de la personne concernée	310
3. Détermination des responsables	312
3.1 Un responsable du traitement	313
3.2 Plusieurs responsables du traitement	314
3.3 Un ou plusieurs sous-traitants.	315
3.4 L'action en cas de pluralité de responsables	315
3.5 Action récursoire.	317
4. Appréciation de la responsabilité.	317
4.1 Limitation ou exclusion de responsabilité	317
4.2 Responsabilité, certifications et codes de conduites.	318
4.3 Règlement amiable	319

4.4	Responsabilité et délégué à la protection des données.	320
4.4.1	Un recours parfois obligatoire	320
4.4.2	Un recours recommandé ?	322
4.4.3	Responsabilité	323

Chapitre 10

Marché unique numérique et RGPD

1.	Introduction	327
2.	Règlements DSA et DMA	328
2.1	Présentation du règlement DSA	328
2.2	Présentation du règlement DMA.	332
2.3	Relations avec le RGPD	336
3.	Règlements sur la gouvernance des données et sur les données . . .	340
3.1	Règlement sur la gouvernance des données	341
3.2	Règlement sur les données.	344
4.	Législation sur l'intelligence artificielle.	348
4.1	Objectifs de la législation.	348
4.2	Présentation de la législation	351
4.3	Cohérence de la législation sur l'IA avec le droit des données à caractère personnel.	358
5.	Données à caractère personnel dans les communications électroniques (ePrivacy)	359
	Glossaire	363
	Index	367

Préface

Avant-propos

Chapitre 1

Définitions de références sur le métier

1. Définition DPO (explication du terme anglais et français)	7
2. La fonction du DPO (selon les textes officiels, RGPD, CNIL, CEPD) . .	8
3. La désignation du délégué à la protection des données (selon les textes officiels)	10
4. Les missions (selon les textes officiels)	12
5. Les définitions en termes de fiche métier (registre des métiers, référentiels de certification...)	14
5.1 Registre des métiers	14
5.2 Référentiel de certification de la CNIL	16
5.3 Référentiel de certification du RNCP 34776	18
5.4 Référentiel de certification du RNCP 36448	18
6. Le rôle du DPO au regard des livrables de la mise en conformité . .	19
6.1 Registre des activités de traitements	21
6.2 Sensibilisation/communication	23
6.3 Privacy by design	25
6.4 Analyses de risques (PIA/AIPD)	26
6.5 Politique de protection des données	28
6.6 Procédure sur les durées de conservation	28
6.7 Procédure sur l'exercice des droits	29
6.8 Procédure sur la violation de données	29
6.9 Procédure d'alerte du responsable de traitement	30
6.10 Procédure d'accompagnement du contrôle CNIL	31
6.11 Indicateurs/audits/bilan annuel	32
6.11.1 Matrice de maturité	33
6.11.2 Matrice de suivi de la conformité	34
6.11.3 Le bilan annuel	35

2 **Le DPO**

Rôle, fonction et attributs du Délégué à la Protection des Données

Chapitre 2

Compétences nécessaires pour le métier

1. Les compétences	37
2. Les compétences spécifiques à l'international	40
3. Les qualités	52
4. Les formations	54
5. Les différents types de contrats (DPO interne, mutualisé, DPO externe)	58
5.1 DPO interne	58
5.2 DPO mutualisé	60
5.3 DPO externe	63
5.4 Le cas spécifique du DPO au sein de la fonction publique territoriale.	64
6. Les outils (bureautique, outils métier...)	67
6.1 Les outils bureautiques.	67
6.2 Les outils métiers	68

Chapitre 3

Le métier et son environnement

1. Le métier et son environnement	73
2. Le positionnement du DPO dans l'organisation.	74
3. Le positionnement du DPO selon les études récentes	80
3.1 L'étude de la DGEFP en 2022	80
3.2 L'étude du cabinet d'avocats Grant Thornton en 2022 sur 125 DPO	82
4. La relation avec les autres métiers (interne : RT, CIL, RSSI ; externe : CNIL, etc.)	83
4.1 Relations avec les relais internes	85
4.2 Relations avec ses pairs	87
4.3 Relations avec les personnes concernées.	87

4.4	Relations avec la DSI et la SSI	88
4.5	Relations avec la CNIL	91
4.6	Relations avec le CIL ou RIL	92
4.7	Relations avec les métiers du Big Data	94
4.8	Relations entre le responsable de traitement et son sous-traitant	96
4.8.1	Rôle du DPO d'un responsable de traitement	97
4.8.2	Rôle du DPO d'un sous-traitant	99
4.9	Relation avec un sous-traitant ultérieur	102
4.10	Relation avec un sous-traitant dans un pays inadéquat	104
4.11	Relation entre responsables conjoints de traitement	105

Chapitre 4

La perception du métier

1.	Le métier vu par les DPO eux-mêmes (11 interviews)	107
1.1	La gouvernance	108
1.2	Le périmètre d'intervention	112
1.3	Les interactions avec les autres acteurs	117
1.4	Le temps par rapport à la charge de travail	122
1.5	Les compétences/formations	124
1.6	Les évolutions du métier	127
1.7	Les constats/anecdotes	132
2.	Le métier vu par les enquêtes (AFPA-AFCDP/CNIL/APEC...)	136
2.1	Étude DGEFP / AFPA-AFCDP le métier de DPO février à avril 2019	136
2.2	Étude DGEFP / AFPA-AFCDP le métier de DPO avril 2020	139
2.3	Étude DGEFP / AFPA-AFCDP le métier de DPO parue en avril 2022	141
2.4	Enquête SupDPO de 2022	143
2.5	Étude AFCDP-Bruno Rasle «Il faut sauver le soldat DPO»	144
2.6	Synthèse des enquêtes	145

4 **Le DPO**

Rôle, fonction et attributs du Délégué à la Protection des Données

3. Le métier au regard des différentes entreprises.	148
3.1 La conscience numérique est un présupposé si le métier de DPO veut être compris.	148
3.2 L'entreprise «data-centric»	149
3.2.1 L'entreprise et la réglementation européenne post RGPD	150
3.2.2 La gouvernance des données	150
3.3 Le DPO, l'interface qui facilite la lecture des enjeux	151
3.4 Des outils et des hommes pour mettre en œuvre la stratégie de gouvernance de la donnée	151
4. Et si le métier de DPO n'existait pas, il faudrait l'inventer (cartographie des risques et sourcing de l'information).	157

Chapitre 5

Les évolutions possibles du métier

1. Introduction	163
2. Les métiers possibles pour un DPO.	165
3. Les évolutions du métier de DPO au regard de l'évolution des outils numériques et du Big data.	166
3.1 Le métier est-il en ligne avec les mutations liées à la masse de données circulantes ?	167
3.1.1 Le DPO et la gouvernance des données.	172
3.1.2 Où sont stockées les données ? Cartographier et documenter.	172
3.1.3 Le DPO et la Data Science au service de la prise de décision stratégique	173
3.1.4 L'anonymisation des données et le Big Data	174

3.2	Le DPO, la réglementation, la norme, le stockage et la sûreté.	174
3.2.1	La réglementation européenne pour la donnée aux horizons 2025	174
3.2.2	Le stockage et la sûreté.	176
3.2.3	Le stockage dans le cloud	177
3.2.4	La cybersécurité	179
4.	Le métier de DPO et l'approche «éthique»	183
4.1	Le cas des données de santé comme exemple éclairant de l'éthique adaptée au numérique	184
4.2	Le cas de l'évolution du métier pour les DPO Groupe	186
5.	Le métier de DPO et l'approche «internationale».	187
	Glossaire	191
	Acronymes	199
	Bibliographie	201
	Index	209