

Avant-propos

Introduction

- 1. Introduction 5
- 2. Zoom sur la loi Informatique et Libertés 6
- 3. Zoom sur le RGPD 13
 - 3.1 Rappel du contexte du RGPD 14
 - 3.2 La nécessité de maîtriser ses données 20
- 4. Applicabilité de la loi Informatique et Libertés 21
 - 4.1 Applicabilité matérielle de la Loi Informatiques et Libertés ... 21
 - 4.2 Qui contrôle le respect de la loi Informatique et Libertés ? ... 22
 - 4.3 Qu'est-ce que je risque si je ne respecte pas la loi Informatique et Libertés ? 23
 - 4.3.1 Procédure de sanction. 24
 - 4.3.2 Typologie des sanctions 25
 - 4.3.3 Sanctions pécuniaires 26
 - 4.3.4 Sanctions pénales 30
 - 4.3.5 Atteinte à l'image 32
 - 4.4 Recours 33
- 5. Qu'est-ce que l'Accountability ? 34
 - 5.1 Documentation et procédure en matière de sécurité 37
 - 5.2 Documentation et procédure en matière de respect des droits des personnes. 39
 - 5.3 Documentation et procédure en matière de formation et de sensibilisation du personnel 39
 - 5.4 Documentation et procédure en matière de conformité des traitements 40
 - 5.5 L'Accountability, nouvel indice de détermination des sanctions 41

2 **Guide juridique du RGPD**

La réglementation sur la protection des données personnelles

Chapitre 1

Identifier les traitements

1. Introduction	43
2. Comment identifier une donnée personnelle ?	44
3. Les cas où la donnée personnelle perd son pouvoir identifiant	47
4. Interdiction de traitement de certaines données personnelles	48
5. Comment identifier un traitement de données personnelles ?	54
6. Les obligations du responsable de traitement de données	55
6.1 Qui est le responsable du traitement ?	55
6.2 La responsabilité	56
6.2.1 La responsabilité du responsable de traitement	58
6.2.2 La responsabilité pénale des dirigeants	61
6.2.3 Les responsables conjoints de traitement	64
7. Le sous-traitant	66
8. Le Délégué à la protection des données	72

Chapitre 2

S'assurer de la licéité de vos traitements

1. Introduction	75
2. Les étapes clés en amont du traitement	76
2.1 Les finalités du traitement	77
2.2 La qualité des données (principes de minimisation, d'exactitude et de mise à jour)	78
2.3 La définition de la durée de conservation des données	81
2.4 Le recensement du traitement dans le registre des activités de traitement	83
3. La mise en œuvre du traitement	83
3.1 Le principe de transparence	83
3.2 L'information des personnes	85
3.3 Le consentement des personnes	90

- 3.4 Le respect des droits des personnes 97
 - 3.4.1 Les droits maintenus et renforcés 97
 - 3.4.2 Les nouveaux droits issus du RGPD 105
- 3.5 Les flux transfrontières. 115

Chapitre 3
Les outils de la Compliance

- 1. Vous avez dit Privacy by design et Privacy by default ? 121
 - 1.1 Privacy by design 121
 - 1.1.1 La genèse du concept 121
 - 1.1.2 L'émergence de la notion 122
 - 1.1.3 La consécration du principe 122
 - 1.2 Privacy by default 123
- 2. Comment respecter le principe de Privacy by design ? 124
 - 2.1 Tenir un registre des activités de traitement 125
 - 2.2 Réaliser une étude d'impact sur la vie privée (PIA) 128
 - 2.2.1 Contenu de la PIA. 129
 - 2.2.2 Description du traitement et de ses finalités 132
 - 2.2.3 Évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités . . . 133
 - 2.2.4 Description des mesures pour faire face aux risques . . . 134
 - 2.2.5 Une évaluation des risques pour les droits et libertés des personnes concernées 135
 - 2.2.6 Les résultats de l'EIVP 136
 - 2.3 Nommer un délégué à la protection des données (DPO). 138
 - 2.3.1 Désignation du DPO 138
 - 2.3.2 Fonctions du DPO 147
 - 2.3.3 Responsabilité du DPO 149
 - 2.3.4 Missions du DPO 151
 - 2.4 Adopter des certifications, labels et codes de conduite 154
 - 2.4.1 La certification 155
 - 2.4.2 Fin des labels CNIL. 157
 - 2.4.3 Les codes de conduite 159

4 **Guide juridique du RGPD**

La réglementation sur la protection des données personnelles

Chapitre 4

Sécuriser les traitements

1. Introduction	161
2. Qui est concerné par l'obligation de sécurité ?	162
3. Pourquoi mettre en place des mesures de sécurité ?	164
4. Que dois-je faire pour sécuriser mon traitement ?	167
4.1 Mener un audit de sécurité complet	169
4.2 Mettre en place des mesures techniques	169
4.2.1 Sécuriser l'accès physique aux locaux	170
4.2.2 Sécuriser les postes de travail	171
4.2.3 Sécuriser le réseau local	175
4.2.4 Sécuriser les données sauvegardées	176
4.2.5 La pseudonymisation	176
4.3 Mettre en place des mesures organisationnelles	181
4.3.1 Élaborer un référentiel de sécurité complet	181
4.3.2 Adopter une logique Privacy by design	185
4.3.3 Mener des études d'impact et des tests d'intrusion	185
4.3.4 Tenir un registre des failles de sécurité	186
4.3.5 Sécuriser la confidentialité et la sécurité des données avec les prestataires et sous-traitants	189
4.3.6 Former son personnel au travers d'actions de sensibilisation	190
4.3.7 Nommer un RSSI	191
Conclusion	193

Annexes

1. Quiz : Avez-vous le profil compliance ?	197
2. Bibliographies, liens utiles	200

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

Chapitre 2**Une première approche du RGPD**

1. Structure du document officiel	29
1.1 Considérants	29
1.2 Articles	30
2. Principaux termes et définitions	32
3. Les deux piliers du règlement.	41
4. Principes fondamentaux juridiques.	42
4.1 Principes fondamentaux relatifs aux traitements de DCP.	42
4.1.1 Licéité, loyauté et transparence	43
4.1.2 Finalité.	46
4.1.3 Proportionnalité des données.	47
4.1.4 Exactitude des données	48
4.1.5 Conservation des données	48
4.1.6 Sécurité des données.	51
4.1.7 Responsabilité (accountability)	53
4.2 Principes fondamentaux relatifs aux droits des personnes concernées	59
4.2.1 Information et communication.	60
4.2.2 Droit d'accès aux DCP	61
4.2.3 Droit de rectification	62
4.2.4 Effacement (droit à l'oubli)	62
4.2.5 Droit d'opposition à un traitement	63
4.2.6 Droit à la formulation de directives « décès »	64
4.2.7 Droit à la limitation du traitement	65
4.2.8 Droit à la portabilité des données	66
5. Le pilier "sécurité des DCP"	67
6. Du droit au management.	67

Chapitre 3
Un système de management

- 1. Introduction 69
- 2. Le système de management 70
 - 2.1 Qu'est-ce qu'un système? 70
 - 2.2 Qu'est-ce qu'un système de management ? 71
 - 2.3 Caractéristiques d'un système de management 72
- 3. Conception du SMDCP 73
 - 3.1 Finalité du système. 73
 - 3.2 Interaction du système avec son environnement. 73
 - 3.3 Objectifs du système 75
 - 3.4 Éléments qui le composent 75
 - 3.5 Autres caractéristiques 76
- 4. Processus du SMDCP 76
 - 4.1 Définition 76
 - 4.2 Déterminer le nombre et l'intitulé des processus 77
 - 4.3 Objectifs, activités, éléments de sorties et mesures techniques et organisationnelles attachées aux 12 processus 80
 - 4.3.1 Processus - Accountability 81
 - 4.3.2 Processus - Traitements et transferts de données 82
 - 4.3.3 Processus - Droits des personnes concernées 84
 - 4.3.4 Processus - Sous-traitants. 85
 - 4.3.5 Processus - Privacy by design 86
 - 4.3.6 Processus - Privacy by default 88
 - 4.3.7 Processus - Privacy Impact Assessment (PIA). 89
 - 4.3.8 Processus - Sensibiliser, former et communiquer 90
 - 4.3.9 Processus - Exigences, sollicitations, violations, poursuites 91
 - 4.3.10 Processus - Évaluer et auditer. 93
 - 4.3.11 Processus - Gérer la documentation et les preuves. 94
 - 4.3.12 Processus - Piloter le SMDCP. 95
- 5. Outils du SMDCP. 97

6. Ressources humaines	98
7. Autres caractéristiques du SMDCP	102
7.1 Fonction de contrôle ou de feedback	102
7.2 Politiques du système	104
7.2.1 Politique générale de protection des données à caractère personnel	104
7.2.2 Politique de gestion des données à caractère personnel	105
7.3 Les référentiels du système de gestion	105
7.4 Propriétés	106
7.4.1 Il est transversal	106
7.4.2 Il est décrit	106
7.4.3 Il est en amélioration constante	107
7.4.4 Il fournit des preuves	110
8. Gouvernance du SMDCP	110
8.1 Qu'est-ce que la gouvernance ?	110
8.2 Principes de la gouvernance	111
8.2.1 Collégialité	112
8.2.2 Transparence du cheminement décisionnaire	112
8.2.3 Gestion des risques et des conflits	112
8.2.4 Communication	113
8.3 Acteurs de la gouvernance	114
8.4 Structure de gouvernance et rythme	115
8.5 Tableau de bord de la gouvernance	115
9. Intégration du SMDCP avec des systèmes de management existants	117
9.1 Juxtaposition	120
9.2 Harmonisation	120
9.3 Mutualisation	121
10. En résumé	122

Chapitre 4
Mise en œuvre du système de management

- 1. Introduction 125
- 2. Choix de la méthode..... 125
- 3. Phase de conception 127
 - 3.1 Étape 1 : Définir 128
 - 3.1.1 Objectifs 128
 - 3.1.2 Activités 128
 - 3.1.3 Livrables 133
 - 3.2 Étape 2 : Collecter..... 133
 - 3.2.1 Objectifs 133
 - 3.2.2 Activités 134
 - 3.2.3 Livrables 137
 - 3.3 Étape 3 : Organiser 138
 - 3.3.1 Objectifs 138
 - 3.3.2 Activités 138
 - 3.3.3 Livrables 146
 - 3.4 Étape 4 : Protéger 146
 - 3.4.1 Objectifs 146
 - 3.4.2 Activités 147
 - 3.4.3 Livrables 149
 - 3.4.4 Focus sur la rédaction de la politique de gestion
des données à caractère personnel 149
 - 3.5 Étape 5 : Clôturer la phase..... 159
 - 3.5.1 Objectifs 160
 - 3.5.2 Activités 160
 - 3.5.3 Livrables 161
- 4. Phase de réalisation..... 162
 - 4.1 Les trois étapes de la phase de réalisation 162
 - 4.2 Étape 1 : Exécuter 163
 - 4.2.1 Objectif 163
 - 4.2.2 Activités 163

4.2.3 Livrables	170
4.3 Étape 2 : Mesurer	170
4.3.1 Objectif	171
4.3.2 Activités	171
4.3.3 Livrables	172
4.4 Étape 3 : Clôturer le projet.....	172
4.4.1 Objectif	173
4.4.2 Activités	173
4.4.3 Livrables	174
5. Organisation du projet	174
5.1 Échéancier du projet.....	175
5.2 Ressources du projet.....	176
6. Cycle de vie du SMDCP.....	177
7. Facteurs clés de succès du projet	178

Chapitre 5

La sécurité des DCP et PIA

1. Système d'information et sécurité.....	179
1.1 Rappel sur le système d'information.....	179
1.2 Sécurité des systèmes d'information.....	180
1.3 Normes et référentiels de sécurité des systèmes d'information	183
2. Sécurité des DCP : que dit le règlement ?	186
3. Privacy by default	187
4. Analyse d'impact relative à la protection des données.....	194
5. Traitements et facteurs de déclenchement d'un PIA.....	195
6. Déroulement d'un PIA	198
6.1 PIA et respect des principes fondamentaux	199

- 6.2 PIA et mesures de sécurité 200
 - 6.2.1 Prise en compte du contexte 201
 - 6.2.2 Appréciation des risques 201
 - 6.2.3 Traitement des risques 203
 - 6.2.4 Consultation préalable 205
 - 6.2.5 Acceptation des risques 206
- 7. Privacy by design 206

Chapitre 6

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

- 1. Introduction 209
- 2. Notion de responsable 209
 - 2.1 Interprétation de la notion 209
 - 2.2 Les personnes responsables 211
- 3. Notion de responsable conjoint 213
- 4. Sous-traitant 215
 - 4.1 Définition 215
 - 4.2 Choix du sous-traitant 216
 - 4.3 Contrat de sous-traitance et sous-traitance de données à caractère personnel 218
 - 4.4 Sous-traitance initiale et sous-traitances successives 220
- 5. Formalisation des relations entre responsable de traitement et sous-traitant 221
- 6. Aspects internationaux 221
- 7. Contenu du contrat 222
- 8. Résolution du contrat 224
- 9. Contrat entre responsables conjoints 225

Chapitre 7**Les transmissions de données**

1. Distinction entre les transmissions, les transferts européens et les transferts internationaux de données	227
2. Transmission de données en France	230
3. Traitements transfrontaliers	232
3.1 Définition	232
3.2 Particularité de ces traitements	232
3.3 Détermination de la loi applicable en cas de traitement transfrontalier	234
3.4 Compétence en cas de recours	239
4. Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales	240
4.1 Principe général applicable aux transferts	240
4.2 Transferts fondés sur une décision d'adéquation	241
4.3 Transferts moyennant des garanties appropriées	242
4.4 Règles d'entreprise contraignantes	244
4.4.1 Généralités	244
4.4.2 Exemples de règles d'entreprise contraignantes (BCR)	247
4.5 Transferts ou divulgations non autorisés par le droit de l'Union	247
4.6 Dérogations pour des situations particulières	248
4.6.1 Autorisation de la personne concernée	248
4.6.2 Transferts nécessaires	248
4.6.3 Transferts réalisés à partir d'un registre public	249
4.6.4 Transferts à portée limitée	249
4.7 Limites au transfert de catégories spécifiques de données à caractère personnel	250
5. Traitement d'un responsable ou sous-traitant de pays tiers vers l'UE	251
5.1 Applicabilité du règlement	251
5.2 Désignation d'un représentant	252

5.3 Modalités et portée de la désignation 253

Chapitre 8
Le contrôle de l'autorité, la CNIL

1. Introduction 255

2. Traitement des réclamations 256

3. Enquête 256

4. Accès aux locaux du responsable
du traitement ou du sous-traitant 257

5. Notification d'une violation 258

6. Mise en demeure 258

7. Rappel à l'ordre 259

8. Injonctions diverses 259

9. Mesures coercitives 260

10. Caractère contradictoire des procédures 260

11. Publicité des mesures 260

12. Coopération entre autorités centrales 261

Chapitre 9
Les sanctions

1. Diversité des sanctions 263

1.1 Sanctions prononcées par l'autorité de contrôle 264

1.1.1 Mesures correctrices 264

1.1.2 Amendes administratives 268

1.2 Les sanctions pénales 271

1.3 Condamnation à des dommages-intérêts 275

1.4 Sanctions liées au caractère illicite du traitement 276

1.4.1 Nullité des contrats 276

1.4.2 Licenciement non fondé 276

2. Représentation de la personne concernée	277
3. Détermination des responsables	278
3.1 Un responsable du traitement	279
3.2 Plusieurs responsables du traitement	280
3.3 Un sous-traitant	281
3.4 Une pluralité de responsables	281
3.5 Action récursoire.	282
4. Appréciation de la responsabilité.	283
4.1 Limitation ou exclusion de responsabilité	283
4.2 Responsabilité, certifications et codes de conduites.	283
4.3 Responsabilité et délégué à la protection des données.	285
4.3.1 Un recours parfois obligatoire	285
4.3.2 Un recours recommandé ?	287
4.3.3 Responsabilité.	287
Glossaire	291
Index	295