

Avant-propos

Introduction

1. Introduction	7
2. Zoom sur la loi Informatique et Libertés	9
3. Zoom sur le RGPD	16
3.1 Rappel du contexte du RGPD	16
3.2 La nécessité de maîtriser ses données	22
4. Applicabilité de la loi Informatique et Libertés	24
4.1 Applicabilité matérielle de la loi Informatique et Libertés	24
4.2 Qui contrôle le respect de la loi Informatique et Libertés ?	25
4.3 Qu'est-ce que je risque si je ne respecte pas la loi Informatique et Libertés ?	26
4.3.1 Procédure de sanction	27
4.3.2 Typologie des sanctions	29
4.3.3 Sanctions pécuniaires	30
4.3.4 Sanctions pénales	34
4.3.5 Atteinte à l'image	37
4.4 Recours	37
5. Qu'est-ce que l'Accountability ?	38
5.1 Documentation et procédure en matière de sécurité	41
5.2 Documentation et procédure en matière de respect des droits des personnes	43
5.3 Documentation et procédure en matière de formation et de sensibilisation du personnel	43
5.4 Documentation et procédure en matière de conformité des traitements	44
5.5 L'Accountability, nouvel indice de détermination des sanctions	45

2 ————— Guide juridique du RGPD

La réglementation sur la protection des données personnelles

Chapitre 1

Identifier les traitements

1. Introduction	47
2. Comment identifier une donnée personnelle ?	48
3. Les cas où la donnée personnelle perd son pouvoir identifiant	52
4. Interdiction de traitement de certaines données personnelles	54
5. Comment identifier un traitement de données personnelles ?	60
6. Les obligations du responsable de traitement de données	60
6.1 Qui est le responsable du traitement ?	61
6.2 La responsabilité	62
6.2.1 La responsabilité du responsable de traitement	63
6.2.2 La responsabilité pénale des dirigeants	67
6.2.3 Les responsables conjoints de traitement	70
7. Le sous-traitant	73
8. Le Délégué à la protection des données	81

Chapitre 2

S'assurer de la licéité de vos traitements

1. Introduction	83
2. Les étapes clés en amont du traitement	84
2.1 Les finalités du traitement	85
2.2 La qualité des données (principes de minimisation, d'exactitude et de mise à jour)	86
2.3 La définition de la durée de conservation des données	89
2.4 Le recensement du traitement dans le registre des activités de traitement	92
3. La mise en œuvre du traitement	93
3.1 Le principe de transparence	93
3.2 L'information des personnes	94
3.3 Le consentement des personnes	99

3.4	Le respect des droits des personnes	107
3.4.1	Les droits maintenus et renforcés	107
3.4.2	Les nouveaux droits issus du RGPD	116
3.5	Les flux transfrontières.	126

Chapitre 3

Les outils de la Compliance

1.	Vous avez dit Privacy by design et Privacy by default ?	135
1.1	Privacy by design	135
1.1.1	La genèse du concept	135
1.1.2	L'émergence de la notion	136
1.1.3	La consécration du principe	136
1.1.4	L'application jurisprudentielle du principe	138
1.2	Privacy by default	138
2.	Comment respecter le principe de Privacy by design ?	139
2.1	Tenir un registre des activités de traitement	140
2.2	Réaliser une étude d'impact sur la vie privée (PIA)	143
2.2.1	Contenu de la PIA.	145
2.2.2	Description du traitement et de ses finalités	148
2.2.3	Évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités . . .	148
2.2.4	Description des mesures pour faire face aux risques . . .	149
2.2.5	Une évaluation des risques pour les droits et libertés des personnes concernées.	150
2.2.6	Les résultats de l'EIVP	152
2.3	Nommer un délégué à la protection des données (DPO). . . .	153
2.3.1	Désignation du DPO	153
2.3.2	Fonctions du DPO	163
2.3.3	Responsabilité du DPO	166
2.3.4	Missions du DPO	168

4 _____ Guide juridique du RGPD

La réglementation sur la protection des données personnelles

2.4	Adopter des certifications, labels et codes de conduite	172
2.4.1	La certification	173
2.4.2	Fin des labels CNIL	175
2.4.3	Les codes de conduite	176

Chapitre 4

Sécuriser les traitements

1.	Introduction	179
2.	Qui est concerné par l'obligation de sécurité ?	181
3.	Pourquoi mettre en place des mesures de sécurité ?	183
4.	Que dois-je faire pour sécuriser mon traitement ?	186
4.1	Mener un audit de sécurité complet	189
4.2	Mettre en place des mesures techniques	190
4.2.1	Sécuriser l'accès physique aux locaux	190
4.2.2	Sécuriser les postes de travail	192
4.2.3	Sécuriser le réseau local	197
4.2.4	Sécuriser les données sauvegardées	199
4.2.5	La pseudonymisation	200
4.3	Mettre en place des mesures organisationnelles	204
4.3.1	Élaborer un référentiel de sécurité complet	204
4.3.2	Adopter une logique Privacy by design	208
4.3.3	Mener des études d'impact et des tests d'intrusion	208
4.3.4	Tenir un registre des failles de sécurité	209
4.3.5	Sécuriser la confidentialité et la sécurité des données avec les prestataires et sous-traitants	212
4.3.6	Former son personnel au travers d'actions de sensibilisation	213
4.3.7	Nommer un RSSI	214

Chapitre 5 Gérer une crise cyber

1. Introduction	217
1.1 Qu'est-ce qu'une crise cyber?	217
1.2 Une intensification de la menace cyber	219
1.3 Du côté de la CNIL : recrudescence des contrôles et des sanctions.	220
2. Prévention du risque cyber et conformité RGPD	221
2.1 Mesures organisationnelles et techniques.	221
2.2 Gouvernance et définition des procédures de gestion de crise.	222
2.3 Sensibilisation de l'organisation au risque cyber	223
2.4 Prévoir le risque cyber dans les contrats	224
3. Le pilotage juridique de la crise cyber	226
3.1 Appliquer les procédures de gestion de crise définies en amont	226
3.2 Qualifier l'incident : qu'est-ce qu'une violation de données?	227
3.3 Notifier une violation de données : quand et comment ?	229
3.4 Documenter l'incident : le registre des violations	230
3.5 Les éventuelles procédures supplémentaires de notification	231
3.6 Déposer plainte : les infractions pénales applicables	232
3.7 Activer sa police d'assurance : connaître les garanties et respecter les délais	233
3.8 Organiser sa communication de crise	235
4. L'après-crise cyber.	235
4.1 Analyser la crise	235
4.2 Tirer les leçons/capitaliser	236
4.3 Mesures de remédiation	237
 Conclusion	 241

6 ————— Guide juridique du RGPD

La réglementation sur la protection des données personnelles

Annexes

1. Quiz : Avez-vous le profil compliance ? 245
2. Bibliographies, liens utiles 248

Remerciements 253

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