

RGPD - Le comprendre et le mettre en oeuvre

(pour les DPO, responsables d'entreprise, responsables informatique, chef de projet...)

Introduction

1. Définition du RGPD	11
2. Approche(s) du RGPD	13
3. Objet et sujets du RGPD	14
4. Application dans le temps du RGPD	15
5. Application dans l'espace du RGPD	16
6. Genèse et portée du RGPD	16
7. RGPD : obligations et opportunités	19

Une première approche du RGPD

1. Structure du document officiel	23
1.1 Considérants	23
1.2 Articles	24
2. Principaux termes et définitions	26
3. Les deux piliers du règlement	34
4. Principes fondamentaux juridiques	35
4.1 Principes fondamentaux relatifs aux traitements de DCP	35
4.1.1 Licéité, loyauté et transparence	36
4.1.2 Finalité	39
4.1.3 Proportionnalité des données	39

RGPD - Le comprendre et le mettre en oeuvre

(pour les DPO, responsables d'entreprise, responsables informatique, chef de projet...)

4.1.4 Exactitude des données	40
4.1.5 Conservation des données	41
4.1.6 Sécurité des données	43
4.1.7 Responsabilité (accountability)	45
4.2 Principes fondamentaux relatifs aux droits des personnes concernées	51
4.2.1 Information et communication	52
4.2.2 Droit d'accès aux DCP	53
4.2.3 Droit de rectification	53
4.2.4 Effacement (droit à l'oubli)	54
4.2.5 Droit d'opposition à un traitement	55
4.2.6 Droit à la limitation du traitement	56
4.2.7 Droit à la portabilité des données	57
5. Le pilier "sécurité des DCP"	58
6. Du droit au management	58

Un système de management

1. Introduction	59
2. Le système de management	60
2.1 Qu'est-ce qu'un système ?	60
2.2 Qu'est-ce qu'un système de management ?	61
2.3 Caractéristiques d'un système de management	62
3. Conception du SMDCP	63
3.1 Finalité du système	63
3.2 Interaction du système avec son environnement	63
3.3 Objectifs du système	65
3.4 Éléments qui le composent	65
3.5 Autres caractéristiques	66

RGPD - Le comprendre et le mettre en oeuvre

(pour les DPO, responsables d'entreprise, responsables informatique, chef de projet...)

4. Processus du SMDCP	66
4.1 Définition	66
4.2 Déterminer le nombre et l'intitulé des processus	67
4.3 Objectifs, activités et éléments de sorties des 12 processus	70
4.3.1 Processus - Accountability	71
4.3.2 Processus - Traitements et transferts de données	72
4.3.3 Processus - Droits des personnes concernées	73
4.3.4 Processus - Sous-traitants	73
4.3.5 Processus - Privacy by design	74
4.3.6 Processus - Privacy by default	75
4.3.7 Processus - Privacy Impact Assessment (PIA)	76
4.3.8 Processus - Sensibiliser, former et communiquer	76
4.3.9 Processus - Exigences, sollicitations, violations, poursuites	77
4.3.10 Processus - Évaluer et auditer	78
4.3.11 Processus - Gérer la documentation et les preuves	78
4.3.12 Processus - Piloter le SMDCP	79
5. Outils du SMDCP	80
6. Ressources humaines	81
7. Autres caractéristiques du SMDCP	85
7.1 Fonction de contrôle ou de feedback	85
7.2 Politiques du système	87
7.2.1 Politique générale de protection des données à caractère personnel	87
7.2.2 Politique de gestion des données à caractère personnel	88
7.3 Les référentiels du système de gestion	88
7.4 Propriétés	89
7.4.1 Il est transversal	89
7.4.2 Il est décrit	89
7.4.3 Il est en amélioration constante	90
7.4.4 Il fournit des preuves	93
8. Gouvernance du SMDCP	93

RGPD - Le comprendre et le mettre en oeuvre

(pour les DPO, responsables d'entreprise, responsables informatique, chef de projet...)

8.1 Qu'est-ce que la gouvernance ?	93
8.2 Principes de la gouvernance	94
8.2.1 Collégialité	95
8.2.2 Transparence du cheminement décisionnaire	95
8.2.3 Gestion des risques et des conflits	95
8.2.4 Communication	96
8.3 Acteurs de la gouvernance	97
8.4 Structure de gouvernance et rythme	98
8.5 Tableau de bord de la gouvernance	98
9. Intégration du SMDCP avec des systèmes de management existants	101
9.1 Juxtaposition	103
9.2 Harmonisation	104
9.3 Mutualisation	105
10. En résumé	106
 Mise en œuvre du système de management	
1. Introduction	107
2. Choix de la méthode	107
3. Phase de conception	109
3.1 Étape 1 : Définir	110
3.1.1 Objectifs	110
3.1.2 Activités	110
3.1.3 Livrables	115
3.2 Étape 2 : Collecter	115
3.2.1 Objectifs	115
3.2.2 Activités	116
3.2.3 Livrables	119
3.3 Étape 3 : Organiser	120

RGPD - Le comprendre et le mettre en oeuvre

(pour les DPO, responsables d'entreprise, responsables informatique, chef de projet...)

3.3.1 Objectifs	120
3.3.2 Activités	120
3.3.3 Livrables	128
3.4 Étape 4 : Protéger	128
3.4.1 Objectifs	128
3.4.2 Activités	129
3.4.3 Livrables	130
3.5 Étape 5 : Clôturer la phase	131
3.5.1 Objectifs	131
3.5.2 Activités	131
3.5.3 Livrables	133
4. Phase de réalisation	133
4.1 Les trois étapes de la phase de réalisation	133
4.2 Étape 1 : Exécuter	134
4.2.1 Objectif	134
4.2.2 Activités	134
4.2.3 Livrables	142
4.3 Étape 2 : Mesurer	142
4.3.1 Objectif	142
4.3.2 Activités	143
4.3.3 Livrables	144
4.4 Étape 3 : Clôturer le projet	144
4.4.1 Objectif	144
4.4.2 Activités	144
4.4.3 Livrables	145
5. Organisation du projet	146
5.1 Échéancier du projet	146
5.2 Ressources du projet	147
6. Cycle de vie du SMDCP	148
7. Facteurs clés de succès du projet	149

RGPD - Le comprendre et le mettre en oeuvre

(pour les DPO, responsables d'entreprise, responsables informatique, chef de projet...)

La sécurité des DCP et PIA

1. Système d'information et sécurité	151
1.1 Rappel sur le système d'information	151
1.2 Sécurité des systèmes d'information	152
1.3 Normes et référentiels de sécurité des systèmes d'information	155
2. Sécurité des DCP : que dit le règlement ?	158
3. Privacy by default	159
4. Analyse d'impact relative à la protection des données	166
5. Traitements et facteurs de déclenchement d'un PIA	167
6. Déroulement d'un PIA	170
6.1 PIA et respect des principes fondamentaux	171
6.2 PIA et mesures de sécurité	172
6.2.1 Prise en compte du contexte	173
6.2.2 Appréciation des risques	173
6.2.3 Traitement des risques	175
6.2.4 Consultation préalable	177
6.2.5 Acceptation des risques	178
7. Privacy by design	178

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

1. introduction	181
2. Relations entre le responsable du traitement et le sous-traitant	181
2.1 Définition du sous-traitant	182

RGPD - Le comprendre et le mettre en oeuvre

(pour les DPO, responsables d'entreprise, responsables informatique, chef de projet...)

2.2 Choix du sous-traitant	183
2.3 Droit applicable à la sous-traitance	185
2.4 Dispositions du RGPD relatives au contrat	186
2.4.1 Obligation de limitation du traitement par le sous-traitant	187
2.4.2 Obligation de confidentialité du sous-traitant	188
2.4.3 Obligation de sécurité du traitement	188
2.4.4 Obligation de coopération avec le responsable	188
2.4.5 Obligations en fin de contrat	189
2.4.6 Clauses contractuelles types	189
2.5 Sous-traitance initiale et sous-traitances successives	189
3. Relations entre les responsables conjoints	190

Les transmissions de données

1. Distinction entre les transmissions, les transferts européens et les transferts internationaux de données	193
2. Transmission de données en France	194
3. Traitements transfrontaliers	196
3.1 Définition	196
3.2 Particularité de ces traitements	196
3.3 Détermination de la loi applicable en cas de traitement transfrontalier	198
3.4 Compétence en cas de recours	201
4. Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales	202
4.1 Principe général applicable aux transferts	203
4.2 Transferts fondés sur une décision d'adéquation	203
4.3 Transferts moyennant des garanties appropriées	205
4.4 Règles d'entreprise contraignantes	206

RGPD - Le comprendre et le mettre en oeuvre

(pour les DPO, responsables d'entreprise, responsables informatique, chef de projet...)

4.4.1 Généralités	206
4.4.2 Exemples de règles d'entreprise contraignantes (BCR)	209
4.5 Transferts ou divulgations non autorisés par le droit de l'Union	210
4.6 Dérogations pour des situations particulières	210
4.6.1 Autorisation de la personne concernée	210
4.6.2 Transferts nécessaires	211
4.6.3 Transferts réalisés à partir d'un registre public	211
4.6.4 Transferts à portée limitée	212
4.7 Limites au transfert de catégories spécifiques de données à caractère personnel	213
5. Traitement d'un responsable ou sous-traitant de pays tiers vers l'UE	213
5.1 Applicabilité du règlement	213
5.2 Désignation d'un représentant	215
5.3 Modalités et portée de la désignation	216

Le contrôle de l'autorité, la CNIL

1. Introduction	217
2. Traitement des réclamations	218
3. Enquête	218
4. Accès aux locaux du responsable du traitement ou du sous-traitant	219
5. Notification d'une violation	220
6. Mise en demeure	220
7. Rappel à l'ordre	221
8. Injonctions diverses	221

RGPD - Le comprendre et le mettre en oeuvre

(pour les DPO, responsables d'entreprise, responsables informatique, chef de projet...)

9. Mesures coercitives 222

10. Caractère contradictoire des procédures 222

11. Publicité des mesures 222

Les sanctions

1. Diversité des sanctions 223

1.1 Sanctions prononcées par l'autorité de contrôle 224

1.1.1 Mesures correctrices 224

1.1.2 Amendes administratives 225

1.2 Les sanctions pénales 227

1.3 Condamnation à des dommages-intérêts 232

1.4 Sanctions liées au caractère illicite du traitement 233

1.4.1 Nullité des contrats 233

1.4.2 Licenciement non fondé 233

2. Représentation de la personne concernée 234

3. Détermination des responsables 235

3.1 Un responsable du traitement 236

3.2 Plusieurs responsables du traitement 237

3.3 Un sous-traitant 238

3.4 Une pluralité de responsables 238

3.5 Action récursoire 240

4. Appréciation de la responsabilité 240

4.1 Limitation ou exclusion de responsabilité 240

4.2 Responsabilité, certifications et codes de conduites 241

4.3 Responsabilité et délégué à la protection des données 242

4.3.1 Un recours parfois obligatoire 242

RGPD - Le comprendre et le mettre en oeuvre

(pour les DPO, responsables d'entreprise, responsables informatique, chef de projet...)

4.3.2 Un recours recommandé ?	244
4.3.3 Responsabilité	244