

Table des matières

Préface	9
ALEXANDRA JASPAR	
Avant-propos	15
AXEL BEELEN	
Retour d'expérience : interview de Jean-Pierre Heymans	19
Le DPO	25
STÉPHANIE GOLINVAUX et HANNAH TACHENY	
Section 1	
Désignation du DPO	25
§ 1. Origines de la fonction de DPO	25
§ 2. Obligation ou faculté de désignation	27
A. Désignation obligatoire au sein des autorités ou organismes publics	27
B. Autres hypothèses de désignation obligatoire en vertu du RGPD	29
C. Désignation obligatoire en application de la législation nationale	29
D. Désignation facultative	31
E. Sanctions en cas de non-respect des règles relatives à la désignation d'un DPO	32
§ 3. Qualités professionnelles du DPO et certifications	35
§ 4. DPO interne ou DPO externe ?	38
Section 2	
Fonctions du DPO	38
§ 1. L'indépendance du DPO	38
§ 2. Association du DPO à toutes les questions relatives à la protection des données à caractère personnel	43
§ 3. Les ressources nécessaires	45
§ 4. Le secret professionnel ou l'obligation de confidentialité du DPO	47
ANTHEMIS	245

Section 3	
Les missions du DPO	49
Section 4	
Responsabilité du DPO	52
§ 1. Responsabilité du DPO mis en cause par l'autorité compétente et les tiers	52
A. Sanctions administratives	53
B. Sanctions pénales	56
§ 2. Responsabilité du DPO à l'égard de son employeur ou de son client	57
Section 5	
Assurabilité des risques liés à la fonction du DPO	59
§ 1. Dispositions communes aux DPO internes et externes	60
§ 2. L'assurabilité des risques liés au DPO interne	62
§ 3. L'assurabilité des risques liés au DPO externe	62
Les obligations du responsable de traitement	65
LAURENTIA VANELVEN	
Introduction – La mise en place du RGPD au sein des institutions locales, entre obligations nouvelles et opportunités	65
Section 1	
Le délégué à la protection des données	67
§ 1. Une désignation obligatoire	67
§ 2. Qui désigner au sein de son institution ?	67
§ 3. Le positionnement du délégué à la protection des données au sein de l'institution	68
§ 4. Les missions du délégué à la protection des données – Particularités inhérentes aux CPAS	68
A. Rôle d'auditeur et de conseiller	68
B. La sensibilisation et la formation	69
C. Faire tenir le registre des traitements	70
D. Devoir de documentation de la mise en conformité et démonstration d'amélioration des processus	70

E.	Créer et tenir à jour le journal des incidents	70
F.	Veiller à ce que les analyses d'impact soient réalisées	70
G.	Suivre les projets impliquant des données à caractère personnel – Privacy by design	71
H.	Préparer un plan catastrophe en cas de fuite de données à caractère personnel	71
I.	Répondre aux demandes de l'Autorité de protection des données et collaborer	72
J.	Quelle(s) responsabilité(s) pour le DPD ?	72
K.	Le délégué à la protection des données, l'instigateur de nouvelles procédures internes	72
 Section 2		
	Le registre de traitement – Un outil dynamique de gestion	73
§ 1.	Principe – Un exercice inédit	73
§ 2.	La multiplicité des traitements effectués et la nécessité de communiquer efficacement dans le travail social	74
§ 3.	Quelques exemples de finalités au regard des missions du CPAS	74
§ 4.	L'impact de l'article 9 de la loi du 30 juillet 2018	75
 Section 3		
	Le responsable de traitement et les sous-traitants	76
§ 1.	La notion de responsable de traitement	76
§ 2.	La notion de sous-traitant	77
§ 3.	L'analyse des contrats de sous-traitance existants	77
§ 4.	La désignation de futurs sous-traitants	78
§ 5.	Les responsabilités	79
 Section 4		
	Le respect des droits de la personne concernée – Équilibre entre conformité, attentes légitimes du citoyen et obligations du responsable de traitement	82
§ 1.	Les principes	82
§ 2.	De l'information au droit d'accès	82
A.	Le droit à l'information et à la transparence versus l'obligation d'informer en termes clairs et précis	82
B.	Le droit d'accès versus l'obligation pour le responsable de traitement de répondre à toute demande	83

C. Le droit de rectification versus l'obligation d'intégrité des données traitées	84
D. Le droit à l'effacement (droit à l'oubli)	84
E. Le droit à la limitation du traitement versus l'obligation pour le service public d'avoir une base légale lui permettant de procéder à un traitement de données	84
§ 3. Une mise en pratique pas si évidente...	85
Section 5	
Mener une analyse d'impact sur la protection des données (AIPD) au sein de son institution	85
§ 1. Définition	85
§ 2. Qui doit mener l'analyse d'impact ?	87
§ 3. Dans quels cas l'analyse d'impact doit-elle être menée ?	87
§ 4. Concrètement	88
Section 6	
L'obligation de minimisation	88
Section 7	
Les mesures techniques et organisationnelles de protection des données à caractère personnel – Une base déjà existante pour les institutions connectées au réseau BCSS par l'application des normes minimales	90
Section 8	
Les zones d'ombre	94
§ 1. La protection sociale du délégué à la protection des données	95
§ 2. La révision des délais de conservation des archives	95
§ 3. L'Autorité de protection des données face aux pouvoirs locaux	95
Conclusion	96

Droits des personnes concernées	99
SABA PARSA et NICOLAS ROLAND	
Introduction	99
Section 1	
Les modalités d'exercice des droits	100
§ 1. Les bénéficiaires des droits et les débiteurs d'obligations	100
A. Les bénéficiaires	100
B. Les débiteurs	102
§ 2. Les modalités d'exercice de tous les droits	102
A. Comment ?	102
B. Dans quels délais ?	105
§ 3. La limitation des droits	105
A. Que prévoit le RGPD ?	105
B. Qu'a-t-on prévu en Belgique ?	106
Section 2	
Les droits des personnes concernées	108
§ 1. Le droit à l'information et le droit d'accès	108
A. De quoi est-il question ?	108
B. Qu'est-ce le droit à l'information ?	109
C. Qu'est-ce le droit d'accès ?	116
§ 2. Le droit de rectification	119
A. De quoi est-il question ?	119
B. <i>Quid si ces données furent déjà transmises à d'autres personnes ?</i>	119
C. Comment comprendre la dérogation à cette obligation de notification ?	120
§ 3. Le droit à l'effacement (« droit à l'oubli »)	120
A. De quoi est-il question ?	120
B. Dans quels cas est-ce possible ?	120
C. <i>Quid si ces données furent déjà transmises à d'autres personnes ?</i>	123
D. <i>Quid si le responsable du traitement a rendu publiques ces données et les a transmises à d'autres responsables du traitement ?</i>	123
E. Ce droit à l'effacement est-il absolu ?	123
F. Qu'en est-il en pratique ?	125
§ 4. Le droit à la portabilité	125
A. De quoi est-il question ?	125
B. De quelles données s'agit-il ?	126

C.	Comment ces données doivent-elles être transmises ?	126
D.	Portabilité ne signifie pas effacement	128
E.	Ce droit de portabilité est-il absolu ?	128
F.	Comment ce droit est-il perçu en pratique ?	129
§ 5.	Le droit d'opposition au traitement	130
A.	De quoi est-il question ?	130
B.	Quels traitements peuvent faire l'objet d'une opposition ?	131
C.	Quelles sont les limites de ce droit ?	132
D.	Qu'en est-il en pratique ?	133
§ 6.	Le droit à la limitation du traitement	133
A.	De quoi est-il question ?	133
B.	Quels traitements peuvent faire l'objet d'une limitation ?	133
C.	Quelles sont les conséquences de ce droit ?	134
D.	Qu'en est-il en pratique ?	135
§ 7.	Le droit de ne pas être soumis à une décision automatisée	135
A.	De quoi est-il question ?	135
B.	Quels traitements peuvent faire l'objet d'une limitation ?	136
C.	Quelles sont les limites de ce droit ?	137
D.	Qu'en est-il en pratique ?	138
§ 8.	Le droit à la notification des fuites et brèches dans le système d'information	138
A.	De quoi est-il question ?	138
B.	Quelles sont les limites à ce droit ?	138
C.	Qu'en est-il en pratique ?	139
Conclusion		139
Sécurité des données personnelles		141
PHILIPPE CORNETTE		
Section 1		
Les implications du RGPD pour la sécurité des données		141
§ 1.	Introduction	141
§ 2.	Pourquoi devrions-nous nous préoccuper de la sécurité de l'information ?	142
§ 3.	Que doivent protéger les mesures de sécurité ?	143
§ 4.	Quel est le niveau de sécurité requis ?	143

Section 2	
Introduction à la sécurité de l'information	145
Section 3	
Gestion des risques de sécurité pour le traitement des données à caractère personnel	147
Section 4	
Aperçu des étapes méthodologiques	152
§ 1. Description du processus	152
§ 2. Établissement du contexte	152
§ 3. Évaluation des risques	152
§ 4. Identification des risques	153
§ 5. Analyse des risques	154
§ 6. Évaluation des risques	154
§ 7. Traitement des risques	154
§ 8. Acceptation des risques	155
§ 9. Communication et consultation sur les risques	155
§ 10. Surveillance et examen des risques en matière de sécurité de l'information	156
Section 5	
Choisir les mesures les plus adaptées	156
§ 1. L'état de la technique	156
§ 2. Les coûts de mise en œuvre des mesures pertinentes	156
Section 6	
Mesures organisationnelles	157
§ 1. Politiques de sécurité de l'information et procédures	157
§ 2. Continuité des activités	158
§ 3. Évaluation des risques	159
§ 4. Information et rapports de gestion	159
§ 5. Sensibilisation et formation	159
§ 6. Audits	159
§ 7. Évaluation de la sécurité d'entreprises tierces	159
ANTHEMIS	251

§ 8.	Plan de cybersécurité	160
§ 9.	Établir un budget pour la cybersécurité	160
§ 10.	Trois lignes de défense	161
A.	La première ligne de défense : les fonctions qui possèdent et gèrent les risques	161
B.	La deuxième ligne de défense : les fonctions qui supervisent ou qui sont spécialisées dans la conformité ou la gestion des risques)	162
C.	La troisième ligne de défense : les fonctions qui fournissent une assurance indépendante	162
Section 7		
Mesures techniques recommandées		163
§ 1.	Inventoriez vos actifs (logiciels et matériels)	163
§ 2.	Sauvegardez vos données	163
§ 3.	Évitez les dommages causés par les logiciels malveillants (<i>malware</i> , virus <i>ransomware</i>)	164
§ 4.	Utilisez des mots de passe complexes pour protéger vos données	165
§ 5.	Protégez vos smartphones (et vos tablettes)	166
§ 6.	Prévenez les attaques de <i>phishing</i>	166
§ 7.	Gérez les accès de vos employés	166
§ 8.	Protégez vos réseaux	167
§ 9.	Protégez votre réseau Wifi	167
§ 10.	Installez les correctifs et mettez à jour vos systèmes d'exploitation et logiciels	167
§ 11.	Sensibilisez les employés aux cybermenaces	168
§ 12.	Contrôlez l'accès physique aux ordinateurs et aux composants du réseau	168
§ 13.	Faites appel à des experts et consultez les standards et modèles existants	169
Section 8		
Utilisation du <i>cloud computing</i> en toute sécurité		169
§ 1.	Définitions	169
§ 2.	Responsabilités partagées en matière de sécurité dans les nuages	170

§ 3. Directives générales de sécurité de l'information et protection de la vie privée de la Banque-Carrefour de la sécurité sociale	171
§ 4. Bonnes pratiques de protection des données dans le <i>cloud</i>	172
A. Sachez ce dont vous êtes responsable	172
B. Déterminez quelles sont les données les plus sensibles et le cryptage	172
C. Mettez en place des politiques de suppression des données dans le nuage	172
D. Gérez le contrôle d'accès	173
E. Formez vos employés à vos pratiques de sécurité dans les nuages	173
F. Veillez à l'hygiène de la sécurité	173
G. Respectez la réglementation	173
H. Recherchez des fournisseurs fiables	174
I. Examinez attentivement les contrats et les accords de niveau de service des fournisseurs de services dans le nuage	174
Section 9	
Que faire si vous opérez dans un secteur qui a ses propres exigences en matière de sécurité ?	174
Section 10	
Que faire lorsqu'un sous-traitant de données est impliqué ?	175
Section 11	
Devriez-vous utiliser la pseudonymisation, l'anonymisation et le cryptage ?	176
§ 1. Qu'est-ce que la pseudonymisation ?	177
§ 2. Pseudonymisation ou anonymisation ?	177
§ 3. Cryptage des données personnelles	178
Section 12	
Comment ISO 27001 ou NIST peuvent-elles vous aider à protéger vos données personnelles ?	178
§ 1. ISO 27001	179
§ 2. NIST	180
A. <i>Avantages du NIST ,CSF</i>	181
B. Fonctions	182

Section 13	
Gestion de projet de cybersécurité	184
Section 14	
Plan d'intervention en cas d'incident	185
§ 1. Contenu d'un plan d'intervention	185
§ 2. Le plan de communication en cas de cyberattaque	187
Autres impacts du RGPD sur l'IT	189
PHILIPPE CORNETTE	
Section 1	
Gouvernance des données	189
Section 2	
Les principes de « <i>privacy by design</i> » et « <i>privacy by default</i> »	191
§ 1. Que dit le RGPD sur la protection des données par conception et par défaut ?	191
§ 2. Qu'est-ce que la protection des données par défaut ?	193
Section 3	
Développer en conformité avec le RGPD	193
Section 4	
Minimiser les données collectées	196
Section 5	
Gestion des consentements	197
Section 6	
Gestion des cookies	198
Section 7	
Gérer la durée de conservation des données	201
Section 8	
Analyse d'impact relative à la protection des données	202

Le RGPD : une opportunité de transformation positive pour les organisations ?	205
DOMINIQUE GRÉGOIRE	
Introduction	205
Section 1	
Le RGPD : menace ou opportunité pour les administrations ?	207
§ 1. Une relecture du RGPD	208
§ 2. Le plus grand risque de non-conformité pour les administrations publiques ?	209
§ 3. Le nécessaire changement	209
§ 4. L'opportunité de la transformation	212
Section 2	
Les bienfaits d'une approche positive de la transformation	214
§ 1. Conditions de réussite de la mise en conformité et opportunités	215
§ 2. Maîtrise et sentiment de maîtrise	216
A. Gestion des risques <i>vs</i> gestion des incertitudes : la fin du mythe de la prévisibilité	216
B. L'agilité : plus qu'une mode, une nécessité	220
C. Quand les contrôles engendrent une perte de contrôle	222
D. Les dimensions humaines	225
§ 3. La confiance : une condition indispensable	226
§ 4. La création de valeur	228
Section 3	
Rôle du DPO dans cette démarche	231
Section 4	
Exemples d'opportunités	233
§ 1. Data Protection Management System (<i>DPMS</i>)	233
§ 2. Privacy by design	234
§ 3. Minimisation et conservations des données	236
Section 5	
Synthèse	237
ANTHEMIS	255

Annexe	241
1. Livres compagnons	241
2. Bibliographie	242