

LES OBLIGATIONS LÉGALES DE CYBERSÉCURITÉ ET DE NOTIFICATIONS D'INCIDENTS



CENTRE FOR
CYBER SECURITY
BELGIUM

crids

CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

politeia

Colophon

Les obligations légales de cybersécurité et de notifications d'incidents

Franck Dumortier, Valéry Vander Geeten, Marion Dargent, Benjamin Docquir, Catherine Forget et Manon Knockaert

Sous la coordination de Franck Dumortier et Valery Vander Geeten

ISBN 978-2-509-03578-3

D/2019/8132/161

NUR 820

© Éditions Politeia s.a.

Boulevard de l'Empereur 34

1000 Bruxelles

Tél. (02) 289 26 10

Fax (02) 289 26 19

info@politeia.be

www.politeia.be

Ce livre fait partie de la collection « RGPD, vie privée et données à caractère personnel », éditée par les Éditions Politeia avec la collaboration des experts du CRIDS-UNamur. Cette collection est dirigée par les professeurs Cécile de Terwangne et Élise Degrave.

Aucun extrait de cette édition ne peut, même partiellement, être communiqué au public, reproduit ni traduit ou adapté sous quelque forme que ce soit moyennant photocopie, microfilm, enregistrement ou tout autre moyen sans l'autorisation écrite et préalable de l'éditeur.

TABLE DES MATIÈRES SIMPLIFIÉE

Chapitre 1. Les obligations de sécurité et de notification des violations des traitements de données à caractère personnel – F. Dumortier	11
Chapitre 2. Transposition de la directive NIS en Belgique – V. Vander Geeten, M. Dargent et B. Docquir	97
Chapitre 3. La sécurité dans le marché unique numérique européen : le Règlement 2019/881 (« Cybersecurity Act ») – M. Knockaert	157
Chapitre 4. Cybersécurité, vie privée, imputabilité, journalisation et log files – F. Dumortier	181
Chapitre 5. La criminalité informatique et les politiques de divulgation coordonnée des vulnérabilités – V. Vander Geeten	211
Chapitre 6. Cybersécurité – cybercriminalité : de l'enquête administrative à l'enquête pénale – C. Forget	257

TABLE DES MATIÈRES

CHAPITRE 1

LES OBLIGATIONS DE SÉCURITÉ ET DE NOTIFICATION DES VIOLATIONS DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

	11
A. Introduction	13
B. Les notions de base	16
1. La définition large de donnée à caractère personnel	16
2. Les traitements régis par le RGPD	19
C. L'avènement d'un « nouveau » principe de base d'intégrité et de confidentialité	21
D. Les débiteurs de l'obligation de sécurité	27
E. Nature de l'obligation de sécurité	29
F. Une obligation de sécurité axée autour des risques pour les personnes concernées	32
1. La notion de risque sous le RGPD	32
2. Les sources des risques pour les personnes physiques	33
3. Un risque à géométrie variable	35
G. L'analyse du risque	37
1. Objet	37
2. Méthodologie de l'évaluation des risques	38
3. L'obligation d'effectuer une AIPD en cas de risque élevé	40
4. La notion de risque élevé	41
H. Les traitements non soumis à l'obligation d'AIPD	44
1. Les critères énumérés par le Groupe 29	45
2. Projet de liste de l'APD de traitements non soumis à l'AIPD	46
I. L'analyse d'impact relative à la protection des données	48
1. Objet	48
2. Étendue de l'AIPD	49
3. Rôles des différents acteurs lors de l'exécution de l'AIPD	51
4. Éléments essentiels d'une AIPD	54
J. Le caractère « approprié » des mesures de sécurité	58
1. La politique de la sécurité de l'information	58
2. L'état des connaissances et les coûts de mise en œuvre	59
3. Codes de conduite, certifications, labels et marques	61
K. De quelques mesures de sécurité	69
1. Objet	69
2. Aperçu de quelques mesures de sécurité techniques	70
3. Aperçu de quelques mesures de sécurité organisationnelles	75
L. La notification et la communication des violations de données	80
1. Objet	80
2. Prise de connaissance et délais	81
3. Les critères de gravité d'une violation de données	83
4. Les violations de données ne devant pas être notifiées	85
5. Les violations de données ne devant pas être communiquées	86

6.	Contenu de la notification à l'autorité de contrôle	87
7.	Contenu et modalités de la communication aux personnes concernées	88
8.	Documentation	90
M.	Conclusion	91

CHAPITRE 2

TRANSPOSITION DE LA DIRECTIVE NIS EN BELGIQUE

		97
A.	Introduction	99
1.	Généralités	99
2.	Notions essentielles	100
3.	Règlement Cybersécurité (« Cybersecurity Act »)	102
4.	Champ d'application territorial	103
5.	Harmonisation et relation avec d'autres instruments	105
B.	Dispositions générales	107
C.	Autorités compétentes	108
1.	Contenu de la directive	108
2.	Compétence de l'État fédéral	108
3.	Désignation des autorités	111
D.	Réseaux et systèmes d'information des opérateurs de services essentiels	115
1.	Notion d'OSE	115
2.	Différence entre un OSE et un exploitant d'une infrastructure critique	119
3.	Processus d'identification des OSE	120
4.	Mesures de sécurité des OSE	123
5.	Désignation d'un point de contact	134
E.	Réseaux et systèmes d'information des fournisseurs de service numérique	141
1.	Les notions	141
2.	Mesures de sécurité	143
3.	Notification d'incidents	144
4.	Contrôle et sanctions	145
F.	Traitement des données à caractère personnel	155
1.	Introduction	155
2.	Périmètres et principes des traitements	155
3.	Mesures de sécurité	156
4.	Droits des personnes concernées	157

CHAPITRE 3

LA SÉCURITÉ DANS LE MARCHÉ UNIQUE NUMÉRIQUE EUROPÉEN : LE RÈGLEMENT 2019/881 (« CYBERSECURITY ACT »)

		161
A.	Introduction	163
B.	Objectifs	164
C.	Schéma européen de certification	165
1.	Objectifs	165
2.	La certification	167
3.	Auto-évaluation de la conformité	174
4.	Réclamation	176
5.	Sanctions	176

D.	ENISA	177
1.	Composition	177
2.	Tâches	179
3.	Transparence	181
4.	Accès aux documents et confidentialité	182
E.	Conclusion	182

CHAPITRE 4

CYBERSÉCURITÉ, VIE PRIVÉE, IMPUTABILITÉ, JOURNALISATION ET LOG FILES

		185
A.	Introduction	187
B.	La journalisation non expressément prévue par le RGPD	190
C.	La journalisation prévue par la directive NIS et le Cybersecurity Act	193
D.	La journalisation, une mesure appropriée de sécurisation des données à caractère personnel	197
1.	La journalisation recommandée par la doctrine et la jurisprudence	197
2.	L'importance de la journalisation au regard de l'obligation d'accountability	199
3.	L'importance de la journalisation en cas de sous-traitance	203
E.	Le traitement de log files au regard des principes du RGPD	204
1.	Les log files contiennent des données à caractère personnel	204
2.	Finalité, minimisation et base de licéité des log files	205
3.	Durée de conservation et droits d'accès aux log files	209
4.	Information et sécurité des log files	211
F.	Conclusions	212

CHAPITRE 5

LA CRIMINALITÉ INFORMATIQUE ET LES POLITIQUES DE DIVULGATION COORDONNÉE DES VULNÉRABILITÉS

		215
A.	Introduction	217
B.	Les notions	217
C.	L'application du droit pénal belge	219
D.	L'intrusion dans un système informatique	220
1.	L'intrusion externe	220
2.	L'intrusion interne	227
3.	Les circonstances aggravantes de l'intrusion	229
E.	Les infractions connexes à l'intrusion	233
1.	La tentative d'intrusion	233
2.	La mise à disposition de moyens pour faciliter une intrusion	234
3.	L'ordre ou l'incitation	235
4.	Le recel de données informatiques obtenues suite à une intrusion	236
5.	Le <i>hacking</i> éthique et les infractions connexes à l'intrusion	238
F.	La violation de données informatiques	239
1.	Les éléments constitutifs matériels	239
2.	Élément moral	240
3.	Les circonstances aggravantes	240

4.	La mise à disposition de moyens pour faciliter la violation de données	241
5.	La tentative	242
6.	La politique de divulgation coordonnée des vulnérabilités et la violation de données informatiques	242
G.	Le faux en informatique et la fraude informatique	243
1.	Le faux en informatique et l'usage de faux en informatique	243
2.	La fraude informatique	246
3.	La politique de divulgation coordonnée des vulnérabilités, le faux en informatique et la fraude informatique	247
H.	Les infractions relatives au secret des communications	248
1.	Infractions relatives au secret des communications non accessibles au public et des données d'un système informatique	248
2.	Les actes préparatoires	251
3.	Le recel de communications illicitement obtenues	252
4.	La tentative	253
5.	Le secret des communications électroniques	253
6.	La politique de divulgation coordonnée des vulnérabilités et les communications	259
I.	La politique de divulgation coordonnée des vulnérabilités et d'autres dispositions légales	260
1.	Les données à caractère personnel	261
2.	Qualification juridique du rôle du participant	263
3.	Les conséquences légales	263

CHAPITRE 6

CYBERSÉCURITÉ – CYBERCRIMINALITÉ : DE L'ENQUÊTE

	ADMINISTRATIVE À L'ENQUÊTE PÉNALE	267
A.	Introduction	269
B.	Les acteurs	270
1.	Le service d'inspection de l'APD	270
2.	Les services d'inspection sectoriel (NIS)	272
3.	Les services de police dans le cadre de l'enquête pénale	273
C.	Les compétences	276
1.	Le service d'inspection de l'APD	277
2.	Le service d'inspection sectoriel (NIS)	278
3.	Les officiers de police judiciaire	279
D.	La clôture de l'enquête et le pouvoir de sanctions	295
1.	Les pouvoirs de sanctions de l'APD	295
2.	Les pouvoirs de sanctions NIS	297
3.	Les pouvoirs de sanctions des juridictions pénales	297
E.	Les règles relatives à la protection des données	298
1.	Principes généraux	298
2.	Les flux de données entre les autorités NIS, l'APD et les autorités policières	301
F.	Conclusion	308

INTRODUCTION

Le présent ouvrage est le résultat d'une étroite collaboration entre le Centre de Recherches Information, Droit et Société (CRIDS) de l'Université de Namur et le Centre pour la Cybersécurité Belgique (CCB). Ce livre est structuré en deux parties principales, constituées elles-mêmes de trois chapitres chacune.

Les trois premiers chapitres sont dédiés à l'analyse détaillée des principales obligations de cybersécurité et de notification d'incidents. Récemment, ces obligations ont été légalement renforcées suite à l'adoption du Règlement général sur la protection des données (RGPD), de la directive sur la sécurité des réseaux et des systèmes d'information (directive NIS) et du Cybersecurity Act. Tant le RGPD que la directive NIS ont notamment pour objectif d'imposer à leurs débiteurs des mesures de sécurité en fonction du risque encouru, mais leur objectif est différent : là où le RGPD vise à protéger le traitement des données à caractère personnel, la directive NIS se concentre sur la résilience des réseaux et des systèmes d'information qui jouent un rôle vital dans la société. Par conséquent, alors que les exigences du RGPD dépendent principalement du risque d'atteinte aux droits et libertés des personnes physiques, sous la directive NIS, ces obligations dépendent du risque d'impact pour la continuité de certains services cruciaux. En parallèle, le Cybersecurity Act – qui renforce le mandat de l'Agence Européenne de Cybersécurité (ENISA) – établit, entre autres, un cadre législatif pour la certification européenne en matière de cybersécurité des produits, processus et services TIC afin d'encourager leurs fabricants ou fournisseurs à protéger au maximum leur sécurité dès la conception.

Après cette première partie descriptive, les trois derniers chapitres de cet ouvrage étudient quelques thématiques plus spécifiques en matière de droit de la cybersécurité. Une première contribution s'intéresse aux implications de l'activité de journalisation, cette méthode qui a pour vocation d'imputer adéquatement les responsabilités en cas d'incident afin d'en identifier l'origine ainsi que pour permettre aux personnes lésées d'exercer leurs droits en toute transparence. Un second auteur examine les dispositions légales à prendre en compte lors de la mise œuvre d'une politique de divulgation coordonnée des vulnérabilités. En effet, la collaboration avec des « hackers éthiques » n'est possible et efficace que si les obligations légales entre les responsables de systèmes informatiques et ces personnes bien intentionnées sont bien définies. Enfin, la dernière contribution s'attache à explorer les rôles et les missions dévolus aux services d'inspection de l'Autorité de protection des données et des autorités NIS. Il va de soi que le renforcement des obligations de cybersécurité implique d'offrir à ces autorités des compétences suffisantes pour leur permettre d'enquêter et de s'assurer du respect des lois soumises à leur contrôle.