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

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 professeures Cécile de Terwangne et Élise Degrave.

TABLE DES MATIÈRES SIMPLIFIÉE

TABLE DES MATIÈRES

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.