THE POWER OF BEING UNDERSTOOD

AUDIT I TAX I CONSULTING

IT INSIGHTS

AVRIL 2019

RSM

Chers tous,

IT Advisory a résumé les faits importants du mois dernier dans son newletter d'avril 2019. Vous découvrirez quelle nouvelle législation a été approuvée par le Parlement européen, comment évaluer une violation de données et ce que signifie la prévention des pertes de données.

Si vous avez des questions sur la protection des données, n'hésitez pas à nous contacter à s.vermeulen@rsmbelgium.be ou au +32 3 449 57 57 51.

Bien à vous,

STEVEN VERMEULEN
Associé
RSM IT ADVISORY

LA NOUVELLE DIRECTIVE EUROPÉENNE SUR LE DROIT D'AUTEUR

Après une longue bataille entre les différentes parties prenantes, le Parlement européen a voté en faveur de la nouvelle directive sur le droit d'auteur. Le droit d'auteur garantit que les auteurs et autres créateurs reçoivent une reconnaissance, une protection adéquate et une rémunération pour leur travail. L'objectif global de la nouvelle directive est de moderniser le droit d'auteur pour le marché numérique en Europe.

La directive vise à assurer aux titulaires de droits un niveau élevé de protection, à faciliter l'octroi de droits et à créer un cadre juridique dans lequel l'exploitation des œuvres et autres objets protégés peut avoir lieu. Le texte adopté doit encore être formellement confirmé par le Conseil de l'Union européenne dans les semaines à venir. Après la publication, les États membres disposent de 24 mois pour transposer les nouvelles règles dans leur législation nationale.

Vous trouverez la dernière version de la directive ici :

http://www.europarl.europa.eu/doceo/document/A-8-2018-0245-AM-271-271_EN.pdf

Une analyse détaillée des conséquences de cette nouvelle législation sera effectuée par RSM IT Advisory et sera communiquée dans le courant de l'année via notre newsletter.

MÉTHODE DE L'ENISA POUR ÉVALUER LE RISQUE DE FUITES DE DONNÉES

Le contrôleur doit informer l'autorité de contrôle compétente lorsque l'atteinte est susceptible de présenter un "risque" pour les droits et libertés des personnes physiques (article 33 de la loi générale sur la protection des données). Si l'atteinte est susceptible d'entraîner un "risque élevé" pour les droits et libertés des personnes physiques, la personne concernée doit également en être informée (article 34 du GDPR).

Le GDPR ne définit pas de critères permettant d'évaluer si une atteinte à la protection des données doit être considérée comme un risque ou un risque élevé. Il est donc utile d'utiliser une méthodologie fondée sur les risques, telle que la méthode de l'ENISA.

L'ENISA a proposé une méthodologie axée sur l'impact sur les personnes dont les données personnelles ont été divulguées. Ce type de fuite de données peut avoir de graves répercussions sur la vie privée, notamment l'humiliation, la discrimination, les pertes financières, les dommages physiques ou psychologiques et les situations mettant la vie en danger.

Afin d'évaluer l'impact sur les données à caractère personnel, les éléments suivants devraient être pris en considération :

- Évaluer le contexte de la protection des données (DPC) : définir le type de données personnelles et prendre en compte les facteurs contextuels.
- Évaluer le risque d'identification (EI)
- Évaluer les circonstances de l'atteinte à la protection des données (CB)

Chacun de ces paramètres reçoit un score en fonction de la gravité de l'atteinte à la protection des données personnelles.
L'ENISA propose ensuite différents scénarios en fonction du type d'atteinte à la protection des données.

Gravité de l'atteinte à la protection des données personnelles : SE = DPC x EI + CB

Vous pouvez trouver la méthodologie complète via ce lien :

https://www.enisa.europa.eu/publications/dbn-severity/at_download/fullReport

PRÉVENTION ET PROTECTION CONTRE LA PERTE DE DONNÉES

En matière de prévention des pertes de données (DLP), nous pensons automatiquement à des applications logicielles conçues pour détecter et prévenir d'éventuelles fuites de données/exfiltrations de données en surveillant, reconnaissant et bloquant les données sensibles, en mouvement et au repos.

Des exemples d'applications DLP sont OpenDLP, MyDLP et celles offertes par Symantec, McAfee et Kaspersky. Cependant, le DLP ne concerne pas seulement l'aspect technique de la protection des données. Dans la pratique, la plupart des fuites de données se produisent parce que les contrôles informatiques non techniques sont absents ou négligés.

Il s'agit donc aussi de prendre des mesures au niveau organisationnel en mettant en place un cadre de travail qui assure une approche cohérente et mesurable de la sécurité de l'information.

Un exemple d'un tel cadre est le COBIT® 5 de l'ISACA pour " la gouvernance d'entreprise de l'information et des technologies (EGIT) ".

Pour assurer le succès d'un programme de DLP, chaque organisation devrait se poser les quatre questions suivantes :

- Question 1 : Quelles informations sont utiles à l'organisation ?
- Question 2 : Qui est responsable de la protection de ces renseignements ?
- Question 3 : Quelle est la meilleure façon de protéger ces renseignements ?
- Question 4 : Quelle est l'efficacité du programme DLP actuel ?

Pour plus d'informations :
http://www.isaca.org/cobit

RSM IT Advisory
Posthofbrug 10 b 4
B 2600 Antwerp
T +32 (0)3 449 57 51

itadvisory@rsmbelgium.be

www.rsmbelgium.be

ZAVENTEM
Lozenberg 22 b 2 - B 1932 Zaventem
T +32 (0)2 725 50 04 - F +32 (0)2 725 53 41

ANTWERP
Posthofbrug 10 b 4 - B 2600 Antwerp
T +32 (0)3 449 57 51 - F +32 (0)3 440 68 27

BRUSSELS
chaussée de Waterloo 1151 - B 1180 Brussels
T +32 (0)2 379 34 70 - F +32 (0)2 379 34 79

CHARLEROI
rue Antoine de Saint-Exupéry 14 - B 6041 Gosselies
T +32 (0)71 37 03 13 - F +32 (0)71 37 01 39

MONS
boulevard Sainctelette 97 b - B 7000 Mons
T +32 (0)65 31 12 63 - F +32 (0)65 36 37 07

AALST
Korte Keppestraat 7 bus 52 - B 9320 Erembodegem
T +32 (0)53 75 12 20

interaudit@rsmbelgium.be
interfiduciaire@rsmbelgium.be
intertax@rsmbelgium.be
interpay@rsmbelgium.be
itadvisory@rsmbelgium.be

WWW.RSMBELGIUM.BE