THE POWER OF BEING UNDERSTOOD

AUDIT I TAX I CONSULTING

IT INSIGHTS

APRIL 2019

RSM

Dear,

IT Advisory has summarized the highlights of the past month in its newsletter of April 2019. You will find out what new legislation was voted in European Parliament, how to assess a data breach and what data loss prevention means.

If you have any questions about data protection, don't hesitate to contact us by email s.vermeulen@rsmbelgium.be or telephone +32 3 449 57 51.

Kind regards,

STEVEN VERMEULEN
Partner
RSM IT ADVISORY

THE NEW COPYRIGHT DIRECTIVE

After a long battle of different stakeholders the European Parliament voted in favour of the new Copyright Directive. Copyright ensures that authors and other creators receive recognition, payment and protection of their work. The modernization of the EU copyright framework was necessary to make EU copyright rules fit for the digital age.

The Directive aims to provide a high level of protection for rightholders, facilitate the clearance of rights and create a framework in which the exploitation of works and other protected subject matter can take place. By now the adopted text is already formally confirmed by the Council of the European Union but we are still waiting for the publication so the rest of the sentence is correct.

You can find the latest version of the Directive here:

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

A detailed analyze about the consequences of this new legislation on your business will be performed by RSM IT Advisory and communicated later this year via our newsletter.

You can find the latest version of the Directive here.

ENISA METHODOLOGY FOR ASSESSING THE RISK OF DATA BREACHES

The controller must notify the competent supervisory authority of every data breach that is likely to result in a “risk” to the rights and freedoms of natural persons (art. 33 GDPR). If the data breach is likely to result in a “high risk” to the rights and freedoms of a natural person, the data subject should also be notified (art. 34 GDPR).

The Regulation does not define any criteria to assess if a data breach must be considered as a risk or high risk. Therefore, it is useful to use a risk-based methodology like the ENISA method.

ENISA proposed a methodology that focuses on the impact on the individuals whose personal data have been breached. Such breaches can lead to serious impact on the affected individuals’ private lives, including humiliation, discrimination, financial loss, physical or psychological damage or even threat to life.

When assessing the impact of a personal data breach the following elements should be considered:

- Assess the data protection context (DPC): define the type of personal data and adjust with contextual factors.
- Assess the identification risk (EI)
- Assess the circumstances of the breach (CB)

Each of those parameters is rated based on the severity of its impact. Different scenarios are then constructed by ENISA for different kind of personal data breaches.

Severity of a data breach: SE= DPC x EI + CB

You can find the full methodology through this link: https://www.enisa.europa.eu/publications/dbn-severity/at_download/fullReport

DATA LOSS PREVENTION AND PROTECTION

If we talk about data loss prevention (DLP) we automatically think about software applications that are designed to detect potential data breaches/data ex-filtration transmission and to prevent them by monitoring, detecting and blocking sensitive data while in-use, both in-motion and at-rest.

Examples of DLP applications are OpenDLP, MyDLP and those offered by Symantec, McAfee and Kaspersky. However, DLP is not only about the technical aspect of data protection. In practice most of the breaches occur due to missing or overlooked nontechnical IT controls.

DLP is also about adopting measures on an organizational level by implementing a DLP framework that ensures a consistent and measurable approach to information security. An example of such a framework is ISACA's COBIT® 5 framework for the enterprise governance of information and technology (EGIT).

Four questions an entity needs to address to ensure a successful and value-driven DLP program:

- Question 1: What information is of value to an organization?
- Question 2: Who is responsible for the protection of organizational information?
- Question 3: How can organizational information best be protected?
- Question 4: How effective is the DLP program?

For more information: 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

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM