# THE POWER OF BEING UNDERSTOOD

AUDIT I TAX I CONSULTING

IT INSIGHTS

APRIL 2019

RSM

Geachte,

IT Advisory heeft de hoogtepunten van de afgelopen maand samengevat in haar nieuwsbrief van april 2019. U zal ontdekken welke nieuwe wetgeving door het Europese Parlement is goedgekeurd, hoe u een datalek kan beoordelen en wat data loss prevention betekent.

Als u vragen heeft over gegevensbescherming aarzel niet om ons te contacteren op s.vermeulen@rsmbelgium.be of +32 3 449 57 51.

Vriendelijke groeten,

Steven Vermeulen
Partner
RSM IT Advisory

## DE NIEUWE EU AUTEURSRECHTRICHTLIJN

Na een lange strijd tussen verschillende belanghebbenden stemde het Europees Parlement de nieuwe auteursrechtrichtlijn goed. Het auteursrecht zorgt ervoor dat auteurs en andere makers erkenning, adequate bescherming en een vergoeding krijgen voor hun werk. De globale doelstelling van de nieuwe richtlijn is het moderniseren van het auteursrecht voor de digitale markt in Europa.

De richtlijn beoogt de rechthebbenden een hoog niveau van bescherming te bieden, het verlenen van rechten te vergemakkelijken en het creëren van een wettelijk kader waarin de exploitatie van werken en ander beschermd materiaal kan plaatsvinden. Na publicatie hebben de lidstaten 24 maanden om de nieuwe regels om te zetten in hun nationale wetgeving.

U kunt de laatste versie van de richtlijn hier terugvinden:

U kunt de laatste versie van de richtlijn hier terugvinden:
http://www.europarl.europa.eu/doceo/document/A-8-2018-0245-AM-271-271_EN.pdf

Een gedetailleerde analyse van de gevolgen van deze nieuwe wetgeving wordt door RSM IT Advisory uitgevoerd en zal later dit jaar worden gecommuniceerd via onze nieuwsbrief.

## ENISA-METHODE VOOR HET BEOORDELEN VAN HET RISICO VAN DATALEKKEN


De controller moet de bevoegde toezichthoudende autoriteit op de hoogte brengen wanneer de inbreuk waarschijnlijk een "risico" inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 33 AVG). Als de inbreuk waarschijnlijk zal leiden tot een "hoog risico" voor de rechten en vrijheden van natuurlijke personen, moet ook de betrokkene op de hoogte worden gebracht (artikel 34 GDPR).

De GDPR definieert geen criteria om te beoordelen wanneer een datalek moet worden beschouwd als een risico of een hoog risico. Daarom is het nuttig om een op risico gebaseerde methodologie te gebruiken, zoals de ENISA-methode.

ENISA heeft een methodiek voorgesteld die zich focust op de impact op personen wiens persoonsgegevens zijn gelekt. Dit type van datalekken kan leiden tot ernstige impact op het privéleven, waaronder vernedering, discriminatie, financieel verlies, fysiek of psychologische schade en levensbedreigende situaties.

Voor het beoordelen van de impact op de persoonsgegevens moeten de volgende elementen in overweging worden genomen:

- Beoordeel het identificatierisico (EI)
- Beoordeel de omstandigheden van het datalek (CB)

Elk van deze parameters krijgt een score die gebaseerd is op de ernst van de inbreuk op de persoonsgegevens.
Vervolgens worden verschillende scenario's door ENISA voorgesteld afhankelijk van het soort datalek.

Ernst van de inbreuk op de persoonsgegevens: SE = DPC x EI + CB

U kunt de volledige methodiek terugvinden via deze link:

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

## DATA LOSS PREVENTION & PROTECTION

Als het gaat over data loss prevention (DLP) denken we automatisch aan softwaretoepassingen die zijn ontworpen om potentiele datalekken/data exfiltratie overdrachten te detecteren en te voorkomen door gevoelige gegevens te controleren, herkennen en blokkeren, zowel in beweging als in rust.
Voorbeelden van DLP-toepassingen zijn OpenDLP, MyDLP en deze die worden aangeboden door Symantec, McAfee en Kaspersky. DLP gaat echter n alleen over het technische aspect van gegevensbescherming. In de praktijk treden de mees datalekken op door het ontbreken of over het hoofd zien van niet-technische IT controles.
DLP gaat dus ook over het nemen van maatregelen op organisatorisch niveau door het implementeren van een DLP framework dat zorgt voor een consistente en meetbare benadering van informatieveiligheid.

Een voorbeeld van dergelijk framework is COBIT® 5 van ISACA voor “the enterprise governance of information and technology (EGIT)”.
Om een succesvol DLP programma te verzekeren dient elke organisatie rekening te houden met de volgende vier vragen:

- Vraag 1: Welke informatie is waardevol voor de organisatie?
- Vraag 2: Wie is verantwoordelijk voor de bescherming van deze informatie?
- Vraag 3: Hoe kan deze informatie het best worden beschermd?
- Vraag 4: Hoe effectief is het huidige DLP programma?

Voor meer informatie: 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