

## RSM InterAudit

Lozenberg 22 b2  
B 1932 Zaventem

T +32 (0)2 725 50 04  
F +32 (0)2 725 53 41

[www.rsmbelgium.be](http://www.rsmbelgium.be)

## MDEON VZW

### VERSLAG VAN DE VEILIGHEIDSCONSULENT INZAKE BEVEILIGING VAN DE INFORMATICA OMGEVING BIJ DE VERWERKING VAN PERSOONSgegevens IN OVEREENSTEMMING MET GENERAL DATA PROTECTION REGULATION EN BELGISCHE PRIVACY WETGEVING

---

Binnen het kader van de privacy wetgeving werd RSM InterAudit gevraagd om de functie van veiligheidsconsulent waar te nemen. Hiertoe werd Dhr. Steven Vermeulen door de privacy commissie erkend als veiligheidsconsulent voor Mdeon VZW.

Onderhavig verslag heeft tot doel de betrokkenen te informeren over de beveiligingsmaatregelen die genomen werden op de informatica omgeving van Mdeon VZW, waarbinnen persoonsgegevens worden beheerd.

Ons onderzoek bestond enerzijds uit nazicht van documenten, anderzijds werden interviews met de verantwoordelijken Mdeon alsook uitbestedingspartijen uitgevoerd.

In het kader van de Europese GDPR wetgeving die van kracht is sinds april 2016 en gepubliceerd werd onder EU Regulation 2016/679, zijn wij overgegaan tot het informeren over en het nazicht op het nakomen van deze wetgeving door de vzw MDEON.

**“REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”**

#### AUDIT | TAX | CONSULTING

RSM InterAudit is a member of the RSM network and trades as RSM. RSM is the trading name used by the members of the RSM Network. Each member of the RSM network is an independent accounting and consulting firm which practices in its own right. The RSM network is not itself a separate legal entity in any jurisdiction.

RSM InterAudit Cvba <sup>CV</sup> - bedrijfsrevisoren - Maatschappelijke zetel - wijk Donselsesteenweg 1151 - B 1180 Brussel  
[interaudit@rsmbelgium.be](mailto:interaudit@rsmbelgium.be) - VAT BE 0436 391 122 - RPR Brussel - <sup>CV</sup> Belgische vennootschap met handelsvorm

Member of RSM Toelen Cats Dupont Koevoets - Offices in Antwerp - Brussels - Charleroi - Mons and Zaventem

## **Bewustwording**

Wij bevestigen dat er op regelmatige tijdstippen informatiesessies gegeven werden aan alle personeelsleden van vzw Mdeon. Deze informatieve sessies werden gepresenteerd door Dhr. Steven Vermeulen en Dhr. Nicolas Delcroix van het consultancykantoor RSM Belgium; met als doel de medewerkers van vzw Mdeon bewust te maken over de wijzigende wetgeving inzake privacy op Europees niveau; in casu de GDPR wetgeving.

Deze bewustwordingscampagne werd tevens doorgetrokken naar de uitbestedingspartijen die persoonsgegevens in en naam en voor rekening van vzw Mdeon behandelen.

Er werd op toegezien dat alle personeelsleden, zowel intern als extern, die bij de verwerking van persoonsgegevens betrokken zijn ingelicht werden over de vertrouwelijkheids- en beveiligingsverplichtingen die zowel voortvloeien uit de verschillende wettelijke vereisten als uit het beveiligingsbeleid.

## **Evaluatie van de risico's (Privacy Impact Analysis)**

Wij zijn overgegaan tot een evaluatie van de risico's inzake de behandeling en het beheer van persoonsgegevens. Op basis van deze evaluatie werd een veiligheidskader ontworpen waaraan de informatica omgeving van Mdeon vzw dient te voldoen. De wettelijke basis voor de behandeling van persoonsgegevens werd geverifieerd, alsook de proportionaliteit van de persoonsgegevens die door vzw Mdeon worden aangehouden.

## **Informatie Register**

Wij hebben nazicht uitgeoefend op het bestaan, de volledigheid en de juistheid van het Informatie Register, waarin de data die persoonsgebonden zijn, gedefinieerd staan. De informatiestromen, wettelijke basis alsook toestemming van betrokkene wiens persoonsgegevens worden verwerkt (consent) werden op verstaanbare en duidelijk wijze in kaart gebracht.

## **Data Protection Officer**

De rol van Data Protection Officer wordt sinds erkenning van RSM InterAudit en ondergeschikt Dhr. Steven Vermeulen als veiligheidsconsulent door de Privacycommissie waargenomen. Binnen deze rol als veiligheidsconsulent wordt er gewaakt over de compliance met Belgische alsook Europese en Internationale wetgeving inzake bescherming van de persoonsgegevens.

## **Gedragscode**

Wij hebben nazicht uitgeoefend op het bestaan van gedragscodes, zowel op niveau van het platform vzw Mdeon alsook voor intern personeel inzake de behandeling van persoonsgegevens. Vzw Mdeon beschikt hiertoe over een Code voor deontologie, goedgekeurd door de Raad van Bestuur en kenbaar gemaakt aan de belanghebbenden.

## **Gegevensbescherming als standaard en als ontwerp (Privacy by default and design)**

Wij zijn overgegaan tot het nazicht van de bescherming van persoonsgegevens als standaard en als ontwerp binnen de verwerking van deze gegevens via geïnformatiseerde tools. De vzw Mdeon en haar informaticapartners hebben de nodige acties genomen om de geïnformatiseerde gegevensbescherming zoveel als mogelijk te integreren binnen het wettelijk kader waarin zij actief zijn.

## **Informatiebeveiliging**

Wij hebben nazicht uitgevoerd op de informatiebeveiligingsbeleidslijn dewelke Mdeon in samenspraak met haar informaticapartners heeft opgesteld. De informatiebeveiligingsbeleidslijn is opgebouwd uit een algemene beschrijving van de informatica-omgeving, een inventaris van de informatica hardware die in gebruik is, de monitoring tools die gebruikt worden, een overzicht van de informatiestromen doorheen verschillende applicaties alsook de beveiligingsinstrumenten die op het netwerk, de website, het dataverkeer en de applicaties van toepassing zijn. Tevens staat in het informatiebeveiligingsbeleid de behandeling van incidenten beschreven. Het informatiebeveiligingsbeleid is aangepast aan de omvang en de noden van de Vzw Mdeon.

Wij hebben nazicht uitgevoerd op de toepasselijkheid van de beveiligingsmaatregelen die genomen werden om een niet-gemachtigde of onnodige fysieke toegang te verhinderen tot de dragers die verwerkte persoonsgegevens bevatten.

De noodzakelijke maatregelen werden genomen om elke fysiek schade die de verwerkte persoonsgegevens in gevaar zouden kunnen brengen, te verhinderen.

De verschillende netwerken gekoppeld aan de apparatuur die de persoonsgegevens verwerkt, zijn op afdoende wijze beschermd.

Een onderzoek naar de dragers van persoonsgegevens werd uitgevoerd. Deze dragers werden in kaart gebracht teneinde de volledigheid van het onderzoek te waarborgen.

## **Communicatie**

Wij bevestigen dat vzw Mdeon en haar informaticapartners de nodige acties hebben genomen teneinde middelen ter beschikking te hebben om te voldoen aan de voorwaarden gesteld inzake:

- Toegang (Access)
- Overdraagbaarheid van gegevens (Portability)
- Juistheid – Rechtzetting van persoonsgegevens (Rectification)
- Gegevenswissing (Right to be forgotten)

## **Behandeling incidenten gerelateerd aan persoonsgegevens**

Wij bevestigen het bestaan van een incident response procedure die dermate werd opgesteld teneinde te voldoen aan de vereisten gesteld inzake de behandeling van incidenten gerelateerd aan persoonsgegevens; in casu Data Breach Incidents. De analyse van deze procedure is op heden nog theoretisch, daar zich tot op datum van controle geen dergelijke incidenten hebben voorgedaan.

## **Doorgifte van gegevens**

De doorgifte van gegevens is in casu niet van toepassing vermits er geen sprake is van persoonsgegevens die worden doorgegeven door het platform aan derde landen of internationale organisaties.

### **Lijst met gemachtigde personen**

Wij bevestigen dat er op moment van onze controlewerkzaamheden een actuele lijst bestond van de verschillende personen die in het kader van de verwerking toegang hebben tot de persoonsgegevens alsook hun respectievelijke toegangsniveau (creatie, raadpleging, wijziging, vernietiging).

Er zijn mechanismen voor toegangsmachtiging van kracht, die verzekeren dat de verwerkte persoonsgegevens en de verwerking die betrekking hebben op deze gegevens uitsluitend toegankelijk zijn voor personen en toepassingen die daartoe uitdrukkelijk gemachtigd werden.

Er is een informatiesysteem dat permanente logging, opsporing en analyse mogelijk maakt van de toegang die personen van vzw Mdeon en haar informaticapartners gehad hebben tot de verwerkte persoonsgegevens.

Hierbij werd voldoende aandacht besteed aan volgende beveiligingsaspecten:

- Toezicht, aanpassing en onderhoud
- Urgentiebeheer van informatiebeveiligingsincidenten
- Documentatie

### **Conclusie**

Gebaseerd op het door ons uitgevoerd nazicht kunnen wij bevestigen dat aan de voorwaarden gesteld door de Privacy Commissie alsook de Europese Commissie, inzake beveiliging van de informatica omgeving binnen het kader van de bescherming van persoonsgegevens, op datum van ons verslag werd voldaan.

Zaventem, 8 juni 2017

RSM INTERAUDIT CVBA  
VERTEGENWOORDIGD DOOR



JEAN-FRANÇOIS NOBELS  
VENNOOT



STEVEN VERMEULEN  
CERTIFIED INFORMATION SYSTEM AUDITOR