Ministerie van Justitie en Veiligheid

CIO Rijk, CIO Beraad, CIO Raad, CTO Raad, CTO Overleg, deelnemers SLM Microsoft Rijk, Surf, VNG en geïnteresseerden

**Directie Informatievoorziening en Inkoop**

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

**Contactpersoon**
Rob Herkemij
*Coördinerend adviseur*

T 070 370 79 11

**Datum**
8 april 2021

**Projectnaam**
SLM Rijk audit-rapport

**Ons kenmerk**
3283437

# memo

Audit op Microsoft

In de kamerbrief van 1 juli 2019 is toegezegd dat SLM Rijk de nakoming van Microsoft ten aanzien van verwerking van persoonsgegevens zal controleren door middel van het contractueel afgedwongen auditrecht. Aan deze toezegging is invulling gegeven. In aanvulling hierop: de controle van SLM Rijk is ook bruikbaar voor SURF en VNG, aangezien SLM Rijk ook deze organisaties vertegenwoordigt bij privacy-audits op Microsoft.

Op 17 maart jl. heeft de externe auditor Ernst & Young (hierna: EY) in opdracht van SLM Rijk zijn bevindingen opgeleverd in het rapport 'Assurance report on profiling restrictions with regard to Microsofts Office 365 ProPlus'[1], gedurende de periode van 1 juli tot en met 30 september van het afgelopen jaar. Het onderzoek richtte zich op de vraag in hoeverre Microsoft zich houdt aan de contractueel overeengekomen restricties met betrekking tot profilering. De resultaten zijn met Microsoft afgestemd volgens het principe van hoor en wederhoor.

Als basis voor de bevindingen heeft een specifiek control framework gediend. Dit control framework bevat kort gezegd de operationele maatregelen die nodig zijn om het risico op onrechtmatige profilering te beheersen. Voor de volledigheid is tevens een lijst met operationele maatregelen opgenomen die aan de kant van het Rijksonderdeel nodig zijn. Deze lijst is echter geen onderdeel geweest van het onderzoek. Het is voor Rijksonderdelen wel verstandig om van deze maatregelen kennis te nemen en deze, waar relevant, te implementeren.

De conclusie van het onderzoek is dat de operationele maatregelen bij Microsoft afdoende zijn beschreven, afdoende zijn vormgegeven en afdoende werken in de onderzochte periode. Dit betekent dat Microsofts interne processen op orde zijn ten aanzien van het contractuele verbod op profilering.

Het is van belang om te vermelden dat deze constatering niet garandeert dat er geen onrechtmatige profilering zal plaatsvinden. Om die reden acht SLM Rijk het noodzakelijk om vanuit meerdere invalshoeken zijn controle op de nakoming door Microsoft uit te oefenen, met betrekking tot alle aspecten van de verwerkingen van persoonsgegevens. Naast het onderzoeken van operationele maatregelen zal

[1] De brief voorafgaande aan pagina 1 is gekenmerkt als 'vertrouwelijk'. Echter, SLM Rijk heeft EY kennis gegeven van zijn voornemen het volledige auditrapport te publiceren. Dit in het kader van de door SLM Rijk gewenste transparantie.

SLM Rijk met regelmaat technische verificatieonderzoeken uitvoeren, waarbij concreet gekeken wordt naar datastromen. De uitkomsten van deze onderzoeken worden vervolgens getoetst aan de contractuele afspraken. Momenteel vindt er een technisch verificatieonderzoek plaats op een aantal applicaties. Deze controle wordt in de loop van dit jaar afgerond. Uiteraard zal SLM Rijk hierover publiceren. SLM Rijk voert daarnaast juridische controles uit. Zo is SLM Rijk momenteel met Microsoft in gesprek over de sub-verwerkercontracten, waarbij SLM Rijk onderzoekt of de instructies die aan Microsoft gegeven zijn op een juiste manier door Microsoft aan zijn sub-verwerkers wordt doorgegeven. Door middel van deze verschillende controlemaatregelen verwacht SLM Rijk voldoende grip op de verwerkingsactiviteiten van Microsoft te houden.

Tot slot: de volledige rapportage van EY is gepubliceerd op de SLM Rijk-website en is hier te vinden.

Met hartelijke groet,
Team Strategisch Leveranciersmanagement.

**Directie Informatievoorziening en Inkoop**

**Datum**
8 april 2021

**Ons kenmerk**
3283437