

Aan de leden van Provinciale Staten van Noord-Holland

Datum ingekomen vragen : 30 januari 2019

Datum GS-besluit: : 5 maart 2019

Vragen nr. 13

Vragen van de heer **F.A.S. Zoon** (Partij voor de Dieren) over Privacygevoelige informatie gedeeld met Amerika

De voorzitter van Provinciale Staten van Noord-Holland deelt u overeenkomstig het bepaalde in artikel 45 van het Reglement van Orde voor de vergaderingen en andere werkzaamheden van Provinciale Staten mede, dat op 30 januari 2019 door het lid van Provinciale Staten, de heer **F.A.S. Zoon** (Partij voor de Dieren), de volgende vragen bij Gedeputeerde Staten zijn ingekomen.

INLEIDING VRAGEN

Het krantenartikel "Data ambtenaar niet naar VS" in het Noord-Hollandsdagblad van 22 januari 2019, maar ook het NRC-artikel "Microsoft lekt dat Nederlandse ambtenaren naar VS" van 13 november 2018¹, roepen bij de Partij voor de Dieren een aantal vragen op.

Binnen de organisatie van de Provincie Noord-Holland wordt er gewerkt met producten van Microsoft. Tevens wordt er in de begroting 2019 vermeld dat er een programma is opgesteld met als titel "Nieuw Technisch Fundament". In dit programma wordt gewerkt naar een diepere integratie met Office 365 en met cloud/online werkplekken.

Er zijn gegronde redenen aan te nemen dat in het verleden, en nu nog, informatie buiten de EU wordt opgeslagen, die strijdig is met de Europa GDPR en Nederlandse AVG-regels. Dit blijkt uit de "Data Protection Impact Assessment op Microsoft Office"² dat namens de rijksoverheid is uitgevoerd. Hierbij zijn ook adviseren gegeven om de gevolgen te mitigeren, totdat er een afdoende oplossing gevonden is.

De Partij voor de Dieren heeft de volgende vragen:

VRAGEN

Vraag 1:

Bent u er bekend mee dat er privacygevoelige gegevens doorgestuurd kunnen worden, vanuit Microsoft-producten, naar Amerikaanse servers en dat dit strijdig kan zijn met de AVG-regels?

Antwoord 1:

Ja.

Vraag 2:

Is het aannemelijk dat dit ook het geval is geweest met gegevens verwerkt door de Provincie Noord-Holland?

¹ <https://www.nrc.nl/nieuws/2018/11/13/microsoft-lekt-data-nederlandse-ambtenaren-naar-vs-a2755066>

² <https://www.rijksoverheid.nl/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office>

Antwoord 2:

Zoals bij elke (overheids)organisatie wordt ook door de provincie Noord-Holland gebruik gemaakt van Microsoft producten. Elke medewerker van de provincie maakt gebruik van Windows10 en Microsoft Office Professional Plus 2016 op de uitgerolde apparatuur (laptops). Het is niet uit te sluiten dat het doorsturen van privacygevoelige gegevens ook bij deze Microsoft producten het geval kan zijn geweest.

Vraag 3:

Zijn de adviezen opgevolgd van het ministerie van Justitie en Veiligheid om de risico's te minimaliseren?

Antwoord 3:

Nee.

Het Strategisch Leveranciersmanagement Microsoft Rijk (SLM Rijk, het inkoopcentrum voor Microsoft producten bij de Rijksoverheid) heeft hiervoor het DPIA³ rapport laten opstellen, waarnaar u in uw vragen verwijst. Dit rapport stelt dat de voorgestelde maatregelen niet in alle gevallen realistisch of haalbaar zijn. In de huidige situatie zijn maatregelen voor de provincie Noord-Holland niet nodig, omdat we nog geen gebruik maken van het pakket Office 365. Inmiddels heeft Microsoft toegezegd mogelijkheden toe te voegen aan de instellingen voor diagnostiek en zal het inzicht geven in de inhoud van de datastromen met Amerika. Microsoft verwacht eind april deze update uit te brengen.

Vraag 4:

Heeft het rapport "DPIA Microsoft Office 2016 en 365 (Engels)" gevolgen voor de ICT-projecten binnen de provincie?

Antwoord 4:

Nee, maar als provincie Noord-Holland volgen we de ontwikkelingen tussen SLM Microsoft en Microsoft nauwgezet en sluiten we ons aan bij de uitkomsten van de discussies tussen het Rijk en Microsoft.

Vraag 5:

Heeft de "Clarifying Lawful Overseas Use of Data Act" (Cloud act)⁴ gevolgen voor de manier en locatie waar de provincie gegevens opslaat en ICT-diensten die worden afgenomen?

Antwoord 5:

Nee, alle servers waar de Provincie Noord-Holland gebruik van maakt, staan in de Europese Unie.

Vraag 6:

Stelt u in het kader van hierboven; regels op voor ingehuurde externen en stelt u regels op voor diensten die werkzaamheden uitvoeren namens de Provincie Noord-Holland die gegevens verwerken die AVG gevoelig zijn?

Antwoord 6:

Ja. De provincie vindt de integriteit van het openbaar bestuur erg belangrijk. Medewerkers en samenwerkingspartners moeten altijd integer handelen. Voor de ambtelijk medewerkers van de provincie gelden gedragscodes en wettelijke- of provinciale regelingen. Hierin staat wat de provincie verstaat onder integer handelen. Ook staat er hoe de provincie integer handelen controleert. Bestuur en medewerkers leggen een belofte of eed af als zij bij de provincie komen werken.

Voor externen gelden deze codes en regelingen in formele zin niet. De provincie verwacht echter ook van externen dat ze zich in hun handelen ook laten leiden door deze codes en

³ DPIA staat voor Data Protection Impact Assessment. Dit is een instrument om de privacyrisico's van een gegevensverwerking in kaart te brengen en om maatregelen te kunnen nemen om de risico's te verkleinen.

⁴ <https://www.rijksoverheid.nl/documenten/kamerstukken/2018/10/05/tk-cloud-act>

regelingen. Daarom wordt altijd met externen een integriteitsverklaring opgesteld. Met ondertekening van deze verklaring:

1. Geeft Betrokkene aan dat hij de integriteitsregels in deze verklaring heeft gelezen en begrepen.
2. Beloofd Betrokkene te handelen volgens deze regels.
3. Geeft Betrokkene aan dat hij weet dat de provincie maatregelen kan nemen, indien hij niet handelt volgens deze regels.

Als de provincie vermoedens heeft dat Betrokkene niet integer handelt, kan een onderzoek worden ingesteld naar zijn handelen. Wanneer er sprake is van aantoonbaar niet-integer handelen kan de provincie maatregelen treffen. Hier vallen onder meer onmiddellijke beëindiging van de werkzaamheden, een contractbeëindiging of het vorderen van een schadevergoeding onder.

Wat betreft het tweede deel van de vraag zijn op het terrein van inkoop de volgende aanpassingen doorgevoerd:

- Een aanpassing in de algemene Inkoopvoorwaarden met een artikel dat vermeldt dat partijen informatie en (persoons)gegevens niet aan derden openbaar maken, tenzij hiermee vooraf schriftelijk is ingestemd of tenzij hier een wettelijke verplichting of rechterlijk bevel aan ten grondslag ligt.
- De inkoopjablonen zijn aangepast voor meervoudig onderhandse aanbestedingen. De aanpassing van de inkoopjablonen is gedaan in de vorm van een vraag aan de (interne) aanvrager om alert te zijn op persoonsgegevens die zullen worden verwerkt bij de uitvoering van de in de markt te zetten opdracht. Mocht dit aan de orde zijn, dan wordt de aanvrager verwezen naar de Functionaris Gegevensbescherming die vervolgens ervoor zorgdraagt dat het inkoopproces voldoet aan de AVG-normen. Het gaat hierbij onder andere om het afsluiten van een verwerkerovereenkomst, om de uitvraag naar informatiebeveiligingsmaatregelen van de leverancier en om de registratie in het register van verwerkingen.
- Bij EU aanbestedingen zijn altijd adviseurs betrokken van de sector Inkoop en de sector Informatievoorziening en ICT die tijdens het inkoopproces controleren of wordt voldaan aan de AVG.

Met het nemen van deze maatregelen voldoet de provincie aan de vereisten van de AVG.

Vraag 7:

Kunt u garanties geven dat de gegevens van burgers die de provincie verwerkt op dusdanige wijze is opgeslagen dat deze volgens de AVG verwerkt worden?

Antwoord 7:

Ter bescherming van persoonsgegevens heeft de provincie in het kader van de AVG de volgende maatregelen getroffen:

Een Functionaris Gegevensbescherming (FG) en een Informatiebeveiligingsfunctionaris (CISO) zijn aangesteld. Beide functionarissen hebben uit hoofde van hun functie de consequenties die AVG heeft voor de provincie in kaart gebracht. Een aantal aanpassingen in de interne werkwijze en procedures van de provincie zijn inmiddels doorgevoerd. De belangrijkste daarvan zijn:

- Het inrichten van een privacy organisatie door middel van het vaststellen van beleid inclusief verantwoordelijkheden en bevoegdheden.
- Een algemeen privacyreglement persoonsgegevens van personeelsleden Noord-Holland 2018 (vastgesteld door GS 8 mei 2018)

- Een ingericht register van verwerkingen, waarin wordt gedocumenteerd welke persoonsgegevens met welk doel worden verwerkt, waar deze gegevens vandaan komen en met wie ze worden gedeeld.
- Een model verwerkersovereenkomst wat noodzakelijk is, indien de opdrachtnemer (de verwerker) persoonsgegevens verwerkt ten behoeve van de provincie (de verwerkersverantwoordelijke). Een verwerkersovereenkomst dient te worden bijgesloten bij een hoofdovereenkomst en te worden geregistreerd in het register van verwerkingen.
- Een protocol voor het afhandelen van datalekken. Dit houdt in dat de provincie een datalek onverwijld moet melden aan de Autoriteit Persoonsgegevens en in bepaalde gevallen ook aan betrokkenen.
- Een procedure voor het afhandelen van rechten van betrokkenen, zodat personen van wie de provincie (bijzondere) persoonsgegevens verwerkt, deze rechten kunnen uitoefenen.
- Daarnaast zijn diverse communicatieve acties binnen de provincie ondernomen om te zorgen dat medewerkers op de hoogte zijn van de AVG en weten waar ze terecht kunnen met vragen. Onder andere zijn flyers verspreid, mededelingen op het intranet geplaatst en is een interview geplaatst in het interne personeelsblad.