AH 3420
2022Z04151

Antwoord van minister Weerwind (Rechtsbescherming) , mede namens de minister van Economische Zaken en Klimaat en de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 30 juni 2022)

Zie ook Aanhangsel Handelingen, vergaderjaar 2021-2022, nr. 2254

Vraag 1
Hoe oordeelt u over dit bericht? Kunt u daarbij ingaan op het feit dat Amerikaanse inlichtingendiensten Microsoft en andere Amerikaanse clouddiensten kunnen dwingen om op basis van wetgeving data van Nederlandse burgers te overhandigen? [1]

Antwoord op vraag 1
Het is goed dat dit soort grootschalige Data Protection Impact Assessments (DPIA´s) op veelgebruikte diensten, zoals in dit geval die van Microsoft, op verzoek van onder meer het Rijk worden uitgevoerd en breed beschikbaar worden gesteld. Op deze manier hebben organisaties in de samenleving baat bij het verrichte werk.

Daarbij is van belang te benadrukken dat de DPIA niet indiceert dat er geen gebruik meer gemaakt kan worden van de onderzochte diensten van Microsoft. Er worden risico's gesignaleerd die raken aan de toegang tot overheidsdiensten, maar ook oplossingen geïdentificeerd om dit risico te mitigeren. Dit kan bijvoorbeeld door het gebruik van eigen encryptiesleutels die door de organisatie zelf – en dus niet door Microsoft - worden beheerd.

Er kunnen op basis van de DPIA over deze clouddienst geen algemene conclusies worden getrokken over alle Amerikaanse clouddiensten en de relatie met inlichtingendiensten. Per dienst kan immers verschillen wat de specifieke risico´s van gegevensoverdracht zijn. Als het gebruik van een dienst een gegevensoverdracht meebrengt is het belangrijk in kaart te brengen wat de specifieke risico´s zijn en deze te mitigeren. Om dat goed te doen kunnen partijen een zogeheten Data Transfer Impact Assessment (DTIA) uitvoeren. De wetgeving in het land waar de gegevens naartoe gaan speelt daarbij een belangrijke rol.

Wat meer algemeen wel van belang is om te benadrukken is dat de toegang tot gegevens van Europese burgers door Amerikaanse overheidsdiensten een belangrijke rol speelt in het Schrems-II arrest van het Hof van Justitie van de

Europese Unie (HvJEU). Daarin heeft het HvJEU het ´adequaatheidsbesluit´[1] voor de VS ongeldig heeft verklaard, onder meer vanwege zorgen omtrent overheidstoegang tot persoonsgegevens in de VS. Recent is er door de Europese Commissie en de VS een principeakkoord gesloten welk de basis zou kunnen vormen voor een nieuw adequaatheidsbesluit.[2] Onderdeel daarvan is onder meer dat de VS stappen zal zetten om de privacy van Europese burgers te beschermen.[3] In de komende maanden zal duidelijk worden welke precieze maatregelen de VS zal nemen.

De Autoriteit Persoonsgegevens heeft aangegeven dat het opnemen 'standard contractual clauses' het ontbreken van adequaatsheidsbesluit voor internationale doorgifte kan ondervangen.[4] Voor relevante Microsoft (cloud)diensten en recent ook Google Workspace is dit door SLM Rijk ook gedaan.

Als laatste wil ik onder de aandacht brengen dat de Europese gegevensbeschermingsautoriteiten momenteel een gezamenlijk onderzoek uitvoeren naar het gebruik van clouddiensten door publieke sector organisaties.[5]

Vraag 2
Deelt u de mening dat het gebruik van Amerikaanse clouddiensten zoals Microsoft een inbreuk op de privacy van de Nederlandse burgers tot gevolg kan hebben zoals ook omschreven in het Schrems arrest van het Europese Hof van Justitie? [2]

Antwoord op vraag 2
Dat er specifieke zorgen bestaan over de gegevensbeschermingsrisico's bij het gebruik van Amerikaanse clouddiensten begrijp ik, specifiek ook in het licht van de overwegingen van het HvJEU in het Schrems-II arrest. Precies

---

[1] Zie artikel 45 AVG Een adequaatheidsbesluit is een besluit van de Europese Commissie dat een derde land een ´passend niveau van gegevensbescherming´ biedt, wat betekent er rechtmatig persoonsgegevens naar dit land kunnen worden doorgegeven.
[2] "Joint Statement on Trans-Atlantic Data Privacy Framework" te raadplegen via: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087
[3] | The White House "FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework", te raadplegen via: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ https://autoriteitpersoonsgegevens.nl/nl/nieuws/aanbevelingen-edpb-voor-doorgifte-persoonsgegevens-na-schrems-ii-uitspraak
[5] European Data Protection Board, ¨Launch of coordinated enforcement on use of cloud by public sector¨ d.d. 15 februari 2022, te raadplegen via: https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_en

met die zorgen in het achterhoofd worden DPIA´s en DTIA´s als die in het door u aangehaalde bericht worden besproken uitgevoerd.

Het gaat mij echter te ver, zoals ook in antwoord op vraag 1 aan de orde komt, om te stellen dat het gebruik van ´Amerikaanse Clouddiensten´ per definitie een privacy schending oplevert. We hebben in EU-verband strikte regels om onze privacy te beschermen, specifiek ook via de Algemene Verordening Gegevensbescherming. Daar moeten alle partijen die zich aan houden, ook Amerikaanse clouddiensten die onder het AVG-regime persoonsgegevens verwerken. Per geval moet worden bezien of en hoe deze diensten rechtmatig gebruikt kunnen worden.

Vraag 3
Deelt u daarom de mening, ook van Privacy Company, dat het gebruik van Amerikaanse clouddiensten bij overheidssystemen en andere gevoelige sectoren als universiteiten niet gewenst is wanneer dit over de uitwisseling of opslag van gevoelige ofwel bijzondere persoonsgegevens gaat? Zo ja, kunt u aangeven welke concrete maatregelen u neemt om dit gebruik te verminderen en daarbij specifiek ingaan op de inzet van versleuteling? Zo nee, kunt u verder uitweiden waarom het bovengenoemde niet weg te nemen risico wel toelaatbaar zou zijn?
Antwoord op vraag 3
Ik kan dergelijke algemene conclusies over alle Amerikaanse clouddiensten niet onderschrijven. Daarbij komt dat die conclusie ook niet voortvloeit uit de voorliggende DPIA. Deze indiceert namelijk dat er maatregelen moeten worden genomen om te voorkomen dat er bijzondere persoonsgegevens worden verwerkt in de onderzochte diensten van Microsoft. Hiertoe kunnen verschillende maatregelen worden genomen. Strategisch Leveranciersmanagement Rijk (SLM Rijk) heeft hierover nader advies uitgebracht.[6] Als deze maatregelen in acht worden genomen kunnen deze diensten in principe in overeenstemming met de AVG worden gebruikt.

Daarnaast zal SLM Rijk er bij Microsoft op aandringen dat end to end-encryptie (E2EE) voor groepsgesprekken in Microsoft Teams wordt gerealiseerd, zodat Microsoft Teams ook geschikt kan worden gemaakt voor verwerking van bijzondere persoonsgegevens in het geval daarvoor een juridische grondslag aanwezig is bij de organisatie die Microsoft Teams inzet.

Vraag 4
Kunt u uitweiden over de verschillende overwegingen wat betreft de voor- en nadelen van het gebruik van niet-Europese clouddiensten bij

[6] Zie memo d.d. 28 februari 2022 te raadplegen via: https://slmmicrosoftrijk.nl/wp-content/uploads/2022/02/Memo-Verwerking-bijz-pers-gegevens-en-publicatie-DTIA.pdf

overheidssystemen en andere gevoelige sectoren voor de uitwisseling of opslag van gevoelige of bijzondere persoonsgegevens?
Antwoord op vraag 4
Zoals aangekondigd in de I-strategie Rijk 2021-2025 wordt er momenteel een rijksbreed strategisch cloudbeleid ontwikkeld en worden handreikingen/richtlijnen ontwikkeld voor het gebruik van clouddiensten.[7] In deze strategie wordt ook ingegaan op de uitwisseling van gegevens met derde landen.

Daarnaast voeren zoals hiervoor aangegeven de Europese gegevensbeschermingsautoriteiten momenteel een gezamenlijk onderzoek uit naar het gebruik van clouddiensten door publieke sector organisaties. Het is nog onzeker hoe zij de risico's van het gebruik van clouddiensten door overheden gaan beoordelen. Eind 2022 komt de European Data Protection Board (EDPB) met een gezamenlijk rapport hierover.[8] De uitkomsten van dit onderzoek kunnen meer inzicht geven in hoeverre het gebruik van clouddiensten door overheidssystemen extra risico's met zich mee brengt voor de bescherming van persoonsgegevens.

Vraag 5
Zijn de juridische mogelijkheden voor oplossingen voor het Schrems arrest voldoende verkend?

Antwoord op vraag 5
Mijn indruk is dat dit het geval is. Zo heeft de Europese Commissie in juni 2021 hernieuwde *´standard contractual clauses´* voor internationale doorgifte gepubliceerd[9], op basis waarvan gegevens op grond van ´passende waarborgen´ kunnen worden doorgegeven.[10] Verder zijn ook de aanbevelingen van EDPB van groot belang geweest om de gevolgen van het arrest goed te duiden en zorg te dragen voor de rechtmatige overdracht van gegevens; niet alleen naar de VS maar naar alle derde landen waarvoor geen ´adequaatheidsbesluit´ van de Europese Commissie bestaat.[11]

---

[7] Te raadplegen via: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/i-strategie-rijk-2021-2025/
[8] Te raadplegen via: https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_en
[9] Europese Commissie "Standard Contractual Clauses for international transfers", te raadplegen via: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en
[10] Artikel 46 AVG betreft doorgifte op grond van passende waarborgen. Artikel 46 tweede lid onder c betreft de doorgifte op grond van de ´standaardbepalingen inzake gegevensbescherming´ .
[11] Te raadplegen via: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

Als in antwoord op vraag 1 al gemeld is er recent een principeakkoord gesloten tussen de Europese Commissie en de VS over een nieuw raamwerk voor trans-Atlantische datastromen. Dat betekent niet dat er reeds een nieuw adequaatheidsbesluit is: daarvoor moet de in artikel 45 AVG geformuleerde procedure worden gevolgd. Nederland heeft hierin als lidstaat een rol via de comitologie procedure.[12]

Vraag 6
In hoeverre helpt de verdere ontwikkeling van het GAIA-X project om de technologische autonomie van Europa te bevorderen? Welke risico's zijn er dat Amerikaanse cloudbedrijven diensten leveren binnen het GAIA-X project en zo alsnog de Europese technologische autonomie beperken? Welke invloed heeft u hierop?

Antwoord op vraag 6
GAIA-X is een snelgroeiend privaat initiatief (een vereniging) onder Belgisch recht met inmiddels meer dan 300 leden. Het doel van GAIA-X is het verbinden van Europese cloudinfrastructuren en het vergemakkelijken van het delen van data. Daarbij is het naleven van Europese regelgeving en waarden een kernpijler. Het initiatief draagt bij aan veilige uitwisseling en verwerking van gegevens en verkleint waar wenselijk de afhankelijkheid van niet-Europese spelers.

Nederland is goed vertegenwoordigd binnen het initiatief. Een groeiend aantal Nederlandse partijen is lid. Dit betreft onder meer TNO, UvA, NEN, Leaseweb , Philips, AMS-IX, Brainport Industries en Surf. Twee van de Nederlandse leden hebben plaats in GAIA-X 'Board of Directors' en kunnen daarmee meesturen op de ontwikkeling van GAIA-X. Daarnaast kunnen Europese overheden met een Gaia-X hub, via de zogenoemde 'Governmental Advisory Board' van GAIA-X ook gevraagd en ongevraagd advies uitbrengen. Nederland wordt hierin door het ministerie van EZK vertegenwoordigd.

Bedrijven uit niet-Europese landen kunnen ook bijdragen aan het GAIA-X initiatief. Samenwerking tussen Europese en niet-Europese bedrijven kan immers ook tot een hoger niveau van dienstverlening door Europese spelers op de markt leiden. Niet-Europese partijen hebben echter geen stemrecht in het initiatief.

Naast Gaia-X is er ook het ´PublicSpaces´ initiatief. Hierin worden gebruikers en burgers centraal geplaatst en worden publieke waarden: ´open´, ´transparant´ en ´verantwoordelijk´, meegenomen bij de ontwikkeling van technologische producten en diensten. We volgen dit initiatief met interesse.

[12] Zie onder meer het derde lid van artikel 45; en de daarin opgenomen verwijzing naar artikel 93 tweede lid AVG.

Vraag 7
Kunt u een update geven over de huidige mogelijkheden wat betreft Europese versleuteling van clouddiensten die ervoor zouden kunnen zorgen dat Amerikaanse inlichtingendiensten niet via niet-Europese clouddiensten zoals Microsoft bij de uitwisseling of opslag van gevoelige ofwel bijzondere persoonsgegevens van Europese burgers zouden kunnen komen? Hoe draagt het GAIA-X project hier verder aan bij?

Antwoord op vraag 7
De European Data Protection Board heeft in aanbevelingen over de *´measures that supplument transfer tools to ensure compliance with the EU level of protection of personal data´* onder meer aan de hand van zogenaamde *´use cases´* inzicht gegeven in welke technische-, organisatorische- en contractuele maatregelen kunnen worden genomen om doorgifte met ´passende waarborgen´ plaats te laten vinden. Het versleutelen (besproken onder *´use case 3´)* van de gegevens is één van de geïdentificeerde maatregelen.[13] Per doorgifte dient te worden bezien óf, en zo ja welke, passende maatregelen (technisch, organisatorisch of contractueel) kunnen worden genomen. In het in antwoord op vraag 4 genoemde rijksbreed strategisch cloudbeleid, dat binnenkort naar uw Kamer zal worden gestuurd, zal hieraan expliciet aandacht gegeven worden.

Het GAIA-X initiatief draagt bij aan het verbinden van Europese cloudinfrastructuren en het vergemakkelijken van datadelen. De wijze van versleuteling van data kan een rol spelen bij de keuze voor een aanbieder van clouddiensten en of risico verminderen. Door het GAIA-X initiatief zullen naar verwachting nieuwe soorten clouddiensten ontstaan, waardoor er voor bedrijven en eindgebruikers meer keuzemogelijkheden zijn om diensten af te nemen. Door GAIA-X is in december 2021 aangekondigd dat labels ontwikkeld worden om o.a. genoemde toegangsrisico's te mitigeren via andere maatregelen.[14]

Vraag 8
Kunt u deze vragen afzonderlijk beantwoorden?

Antwoord op vraag 8
Ja.

---

[13] European Data Protection Board, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", te raadplegen via: edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (europa.eu), vanaf pagina 29

[14] https://www.gaia-x.eu/news/gaia-x-association-announces-labelling-framework-release

[1] AGConnect, 22 februari 2022, 'Teams, Onedrive en Sharepoint onveilig voor Rijk en onderwijs', https://www.agconnect.nl/artikel/teams-onedrive-en-sharepoint-onveilig-voor-rijk-en-onderwijs

[2] https://www.recht.nl/nieuws/privacyrecht/187414/schrems-ii-arrest-verstrekkende-uitspraak-voor-techbedrijven/