Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

3136

Vragen van het lid **Kathmann** (PvdA) aan de Minister van Justitie en Veiligheid over *het bericht dat de meeste Nederlandse bedrijven niet voldoen aan privacywetgeving* (ingezonden 7 april 2021).

Antwoord van Minister **Dekker** (Rechtsbescherming) (ontvangen 10 juni 2021). Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 2525.

Vraag 1
Bent u bekend met het artikel «Meerderheid Nederlandse bedrijven voldoet na drie jaar nog niet aan privacywet»?[1]

Antwoord 1
Ja.

Vraag 2
Wat vindt u ervan dat kosten en inspanningen om de AVG-wetgeving op te volgen volledig op het bord komen te liggen van Europese bedrijven, terwijl die in hoge mate afhankelijk zijn van niet-Europese techgiganten?

Antwoord 2
De kosten en inspanningen om aan de vereisten uit de Algemene Verordening Gegevensbescherming (AVG) te voldoen liggen niet volledig op het bord van Europese bedrijven. In voorkomend geval kan de AVG ook rechtstreeks van toepassing zijn op bedrijven die niet in de EU zijn gevestigd.[2] De AVG kent een systematiek waarin er een «verwerkingsverantwoordelijke» is die het doel en de middelen van een gegevensverwerking bepaalt. Daarnaast is er de «verwerker», deze wordt door de verwerkingsverantwoordelijke ingeschakeld om gegevens te verwerken. Op deze verwerker rusten ingevolge artikel 28 AVG ook verplichtingen.
De verwerkingsverantwoordelijke mag ingevolge artikel 28 lid 1 alleen beroep doen op verwerkers die voldoende garanties bieden opdat de verwerking aan de AVG voldoet. In lid 3 van ditzelfde artikel wordt voorts bepaald dat tussen beide partijen een overeenkomst wordt opgesteld waarin de verplichtingen van de verwerker worden vastgelegd, in de praktijk bekend als de «verwer-

[1] Financieele Dagblad, 6 april 2021, «Meerderheid Nederlandse bedrijven voldoet na drie jaar nog niet aan privacywet», https://fd.nl/economie-politiek/1379255/meerderheid-nederlandse-bedrijven-voldoet-na-drie-jaar-nog-niet-aan-privacywet

[2] Artikel 3 lid 2 Algemene Verordening Gegevensbescherming (AVG).

ah-tk-20202021-3136
ISSN 0921 - 7398
's-Gravenhage 2021

kersovereenkomst». Hierin wordt onder meer vastgelegd welke instructies de verwerker krijgt om de gegevens te verwerken, welke beveiligingsmaatregelen moeten worden genomen en hoe de rechten van betrokkenen worden geëffectueerd. Als een verwerker in strijd met de AVG zelf de doeleinden en middelen van een verwerking bepaalt, dan moet die partij zelf als verwerkingsverantwoordelijke worden beschouwd.[3] Al met al kent de AVG dus een systeem waarin de verantwoordelijkheden en verplichtingen verdeeld zijn over betrokken partijen.

Vraag 3
Bent u het eens met de observatie dat Nederlandse bedrijven een te slechte onderhandelingspositie hebben tegenover Amerikaanse techgiganten op het gebied van de implementatie van AVG-maatregelen? Zo nee, waarom niet?

Antwoord 3
Zoals in antwoord op vraag 2 geschetst leggen partijen in de verwerkersovereenkomst vast op welke wijze gegevens verwerkt worden en welke vereisten daarbij in acht worden genomen. De verwerkersovereenkomst moet derhalve worden afgestemd op de verwerking die de verwerker namens de verwerkingsverantwoordelijke verricht.
De overeenkomst kan dus per verwerking die ten behoeve van de verwerkingsverantwoordelijke wordt verricht verschillen. Hoewel dit maakt dat een algemene gevolgtrekking over de onderhandelingspositie lastig ligt, is dit wel de kern van de problematiek waar veel Nederlandse afnemers van clouddiensten mee worden geconfronteerd. Het standaardcontract van de leverancier biedt de afnemer niet altijd de noodzakelijke garanties die het ingevolge artikel 28 lid 1 nodig heeft. Sommige diensten worden geleverd door een aantal grote spelers die niet altijd bereid zijn het individuele contract aan de noden van de afnemer aan te passen. Bijkomend nadeel voor de afnemer is voorts dat het soms veel middelen vergt om te vergewissen hoe de dienst van de verwerker precies in elkaar steekt en welke contractsbepalingen derhalve nodig zijn. Als vervolgens wordt geconcludeerd dat de leverancier geen geschikte verwerker is omdat deze onvoldoende garanties biedt en daar niets aan wil veranderen, is het gelet op het beperkte aantal aanbieders, maar zeer de vraag of er een geschikt alternatief beschikbaar is. Zoals in het FD-artikel tevens aangegeven is het voor de overheid wel gelukt om AVG-maatwerk af te dwingen in relatie met een leverancier van clouddiensten. Het artikel kaart terecht aan dat bedrijven niet in elk geval in eenzelfde goede onderhandelingspositie verkeren en dit dus niet altijd af kunnen dwingen.

Vraag 4
Deelt u de mening van het CIO Platform dat de wetgever oproept om alleen toegang te verlenen aan de Europese markt als softwarebedrijven de AVG-eisen naleven? Zo nee, waarom niet?

Antwoord 4
Partijen die in de EU zijn gevestigd en gegevens verwerken moeten voldoen aan de vereisten uit de AVG. In voorkomend geval kunnen ook partijen die niet in de EU zijn gevestigd onder het toepassingsgebied van de AVG vallen.[4] Als zij als verwerkingsverantwoordelijke of verwerker de AVG schenden kunnen de toezichthouders hierop handhaven. Softwarebedrijven die niet conform de AVG handelen kunnen dus al worden aangepakt.
In voorkomende gevallen kan het echter zo zijn dat de leverancier de dienst AVG-compliant aanbiedt, maar dat een organisatie die de dienst wil afnemen deze niet AVG-compliant kan toepassen. Dit kan optreden in situaties waarin leveranciers gegevens tevens willen verwerken voor andere doelen. Dit is soms ook onderdeel van hun verdienmodel. Zolang de leverancier transparant is over deze doelen en de leverancier zélf een rechtmatige verwerkingsgrondslag heeft kan de dienst AVG-compliant zijn. Van de individuele consument kan bijvoorbeeld toestemming worden gevraagd, die deze betrokkene vrijelijk al dan niet kan geven. Deze dienst echter inzetten als

[3] Artikel 28 lid 10 AVG.
[4] Artikel 3 lid 2 AVG.

grotere organisatie (bijv. een bedrijf) kan dan problematisch zijn als die «eigen» doelen van de leverancier niet aansluiten op de doelen waarvoor de gegevens verzameld zijn. Per geval zal dus moeten worden bezien of een dienst op rechtmatige wijze in gebruik genomen kan worden. Het is dan ook niet in alle gevallen mogelijk om bij toegang tot de Europese markt te bepalen of software aan de AVG-eisen voldoet.

Vraag 5
Deelt u de mening van Ronald Verbeek, directeur van het Platform, namelijk dat niet de gebruiker van software, maar de ontwikkelaar verantwoordelijk moet zijn voor het implementeren van AVG-eisen? Zo ja, wat vindt u ervan dat de gebruikers van niet-veilige software een boete kunnen krijgen van 20 miljoen euro of 4% van hun jaarlijkse omzet? Zo nee, waarom niet?

Antwoord 5
Zoals in antwoord op vraag 2 aangegeven biedt de AVG een eigen systematiek voor de verdeling van verantwoordelijkheden bij het verwerken van persoonsgegevens. Deze verdeling kan naar gelang het handelen van betrokken partijen veranderen: als de verwerker zich gaat gedragen als de partij die eigenstandig bepaalt dat het gegevens gaat verwerken, dan moet deze partij als verwerkingsverantwoordelijke worden aangesproken.
Basis van dit systeem is wel dat de partij die de gegevens van burgers verwerkt en bepaalt wat daarmee gebeurt in beginsel verantwoordelijk – en daarmee aanspreekbaar – blijft voor de verwerking. De verwerkingsverantwoordelijke kiest er immers voor om met een bepaalde verwerker in zee te gaan en maakt afspraken met deze verwerker. Die systematiek vind ik juist, omdat burgers anders controle over hun gegevens verliezen. Het is uiteindelijk aan de Autoriteit Persoonsgegevens om te bepalen ten aanzien van welke partij(en) zij handhavend optreedt.

Vraag 6
Deelt u de mening dat de Nederlandse overheid meer moet doen om techgiganten te bewegen tot het implementeren van AVG-richtlijnen om op deze manier Nederlandse bedrijven te helpen in het beschermen van persoonsgegevens? Zo ja, wat gaat u doen? Zo nee, waarom niet?

Antwoord 6
Zoals in antwoord op vraag 4 aangegeven moet het vraagstuk omtrent het voldoen aan de eisen uit de AVG genuanceerd worden bezien. Het is te kort door de bocht om te stellen dat aanbieders van clouddiensten niet aan de AVG zouden voldoen, of hun klanten niet in staat willen stellen om aan de AVG te voldoen. Wél heb ik in antwoord op vraag 3 aangegeven dat ik ook zie dat het voor met name kleinere bedrijven lastig en kostbaar kan zijn om te vergewissen hoe de dienst van een potentiële verwerker precies functioneert, om vervolgens aangepaste voorwaarden af te dwingen om de dienst tóch af te kunnen nemen.
De Nederlandse overheid heeft middelen tot haar beschikking om solide onderzoek te verrichten naar de werking van bepaalde software pakketten, bijvoorbeeld door het uitvoeren van een Data Protection Impact Assessment (DPIA), om op basis daarvan in kaart te brengen hoe de verwerkersovereenkomst vorm moet krijgen. Voorbeeld hiervan betreft de DPIA door Strategisch Leveranciersmangement Rijk (SLM Rijk) is uitgevoerd naar Google G Suite Enterprise waarover uw Kamer door de Minister van Justitie en Veiligheid is geïnformeerd.[5] Deze DPIA is voorgelegd aan de Autoriteit Persoonsgegevens omdat er door SLM Rijk restrisicos zijn geconstateerd. De AP brengt hier binnenkort schriftelijk advies over uit. Momenteel worden de mogelijkheden verkend om deze aanpak te verbreden tot de andere strategische leveranciers van de rijksoverheid. Door het systematisch beoordelen van dergelijke softwarepakketten door de overheid en de AP wordt er duidelijkheid verschaft over de mate waarin het gebruik mogelijk is binnen de grenzen van de AVG. Ik verwacht dat leveranciers eventuele geconstateerde risicos serieus nemen en met de Nederlandse overheid zullen werken aan het gezamenlijk aanpakken daarvan. Het is van belang te benadrukken dat er in dit geval dus geen

[5] Kamerstuk 26 643/32 761, nr. 747

sprake is van het gezamenlijk werken aan of ontwikkelen van softwarepakketten. Het is dan ook terecht dat de overheid geen «eigenaar» van de software is. Wél kunnen overheden en private partijen in de toekomst mogelijk profiteren van het werk dat voor deze DPIAs wordt verricht en van eventuele aanpassingen die als gevolg daarvan aan contracten worden gedaan. Daarom deelt de overheid waar mogelijk haar kennis, inzichten en ervaringen, bijvoorbeeld door het publiceren van voornoemde DPIAs.
Voorts zet het kabinet ook in op Europese samenwerking om gezamenlijk de kwaliteit en kwantiteit van aangeboden clouddiensten te stimuleren. Eind 2020 heeft het kabinet een verklaring ondertekend voor een Europees initiatief voor een «cloudfederatie», waarmee lidstaten zich hebben gecommitteerd om gezamenlijk te werken aan en te investeren in Europees verbonden data- en cloud infrastructuren.[6] Daarnaast is er het initiatief GAIA-X, waarbij door het ontwikkelen van standaarden bestaand «cloud aanbod» verbonden en verrijkt wordt, gebaseerd op Europese regelgeving. Voorts werkt TNO aan het oprichten van een Nederlandse GAIA-X hub, waar gezamenlijk use cases ontwikkeld kunnen worden.
Ook de Online Trust Coalitie (OTC) werkt in Europees publiek-privaat verband aan deze problematiek, waarbij zowel het perspectief van de aanbieder als dat van de afnemer wordt geadresseerd. De OTC zet in op het ontwikkelen van eenduidige, efficiënte methode waarmee leveranciers van clouddiensten kunnen aantonen dat hun diensten betrouwbaar en veilig zijn, en die afnemers de gewenste duidelijkheid geeft bij de invulling van de relevante wet- en regelgeving, zoals de AVG.

[6] Declaration «Building the next generation cloud for businesses and the public sector in the EU», te raadplegen via: https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe