Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

Aanhangsel van de Handelingen

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

2456

Vragen van de leden **De Liefde**, **Moors**, **Dijkhoff** en **Litjens** (allen VVD) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *de opslag van vertrouwelijke data door overheidsorganisaties en semi-publieke instellingen* (ingezonden 27 mei 2014).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 8 juli 2014). Zie ook Aanhangsel Handelingen, vergaderjaar 2013–2014, nr. 2228.

Vraag 1
Acht u het wenselijk dat buitenlandse inlichtingen- en veiligheidsdiensten vertrouwelijke data van de Nederlandse overheid kunnen inzien? Zo nee, welke stappen gaat u ondernemen om alle vertrouwelijke data van overheidsorganisaties en semi-publieke instellingen binnen Nederland te houden, of anderszins te waarborgen dat buitenlandse veiligheidsdiensten zich geen toegang kunnen verschaffen tot deze vertrouwelijke data?

Antwoord 1
Nee, dat is niet wenselijk. De Rijksoverheid heeft er daarom op basis van haar Rijkscloudstrategie voor gekozen om een Rijkscloud in te richten als een voorziening die generieke diensten gebaseerd op cloudtechnologie levert binnen de Rijksdienst. Deze voorziening wordt ingericht binnen een eigen beveiligd netwerk. Er is dus gekozen voor een community/private clouddienst in eigen beheer. Binnen de Rijkscloud kunnen diensten zoals dataopslag, servercapaciteit, infrastructuurcapaciteit en diensten zoals e-mail, werkplekomgeving, samenwerkingsfunctionaliteit en aansluiting op applicaties worden afgenomen.
De Rijkscloud wordt ondergebracht in de vier Overheidsdatacenters. Strikte eisen hierbij zijn dat de gegevens in Nederland blijven, de veiligheid voor alle afnemers adequaat is en op een voor de gekozen toepassingen acceptabel niveau kan worden geregeld. Daar waar dat opportuun is en veilig kan gebeuren, wordt bij het realiseren van een Rijkscloud gebruik gemaakt van diensten van marktpartijen. De regie op de inrichting en het beheer zal echter binnen de Rijksoverheid blijven.
De laatste van die datacenters moet aan het einde van dit jaar gereed komen. Het is de bedoeling dat gefaseerd de data(systemen) van de Rijksoverheid die nu nog deels verspreid zijn over kleinere datacenters in deze vier datacentra (en die van Defensie) ondergebracht gaan worden. Ook Rijksoverheidspartijen die hun data nu op externe locaties hebben staan, zullen deze in principe

ah-tk-20132014-2456
ISSN 0921 - 7398
's-Gravenhage 2014

migreren naar de Rijkscloud. Op dit moment vinden verkenningen plaatst om te bezien of ook andere overheidspartijen zoals provincies en gemeenten voor hun data(systemen) gebruik kunnen maken van de voor de Rijksdienst ingerichte basisinfrastructuur van de Rijkscloud.
De Rijkscloud en alle ondersteunende functionaliteiten en componenten worden ingericht volgens de Baseline Informatiebeveiliging Rijksdienst (BIR). Dit is vergelijkbaar met het opslaan en verwerken van informatie met het Departementaal Vertrouwelijk (Dep.V) niveau.
Behalve dat er is gekozen voor de vorming van een Rijkscloud wordt ook op diverse andere terreinen gewerkt aan de verdere implementatie van maatregelen die het Rijk beter weerbaar maken tegen buitenlandse inlichtingen- en veiligheidsdiensten. Inlichtingenactiviteiten van buitenlandse inlichtingen- en veiligheidsdiensten worden door de AIVD onderzocht en tegengegaan. Er wordt extra geïnvesteerd in de monitoring en detectiecapaciteiten van het Rijk. Dit door aansluiting te vinden bij het Nationaal Detectie Netwerk, een samenwerkingsverband op initiatief van Ministerie van Veiligheid en Justitie – om digitale dreigingen in een voortijdig stadium te detecteren en informatie over digitale dreigingen te delen – en door de ontwikkeling van Security Operations Centers (SOC's) Rijksbreed te stimuleren. Daarnaast wordt binnen het Rijk de BIR geïmplementeerd waarmee alle geledingen van het Rijk aan een minimum beveiligingsniveau dienen te voldoen, gebaseerd op internationale ISO beveiligingsnormen.
De medeoverheden en semi-publieke instellingen zijn zelf verantwoordelijk voor de beveiliging van hun vertrouwelijke gegevens. Ik kan dan daar slechts adviserend optreden vanuit mijn coördinerende bevoegdheid voor de informatievoorziening binnen de openbare sector.
Voor gemeenten heeft de Informatiebeveiligingsdienst voor gemeenten (IBD) van VNG/KING een operationeel product beschikbaar binnen de Baseline Informatiebeveiliging voor Gemeenten (BIG): «Cloud Computing Gemeenten», die gemeenten een handreiking biedt op dit vlak.
De Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) ontwikkelt tevens een tweetal handreikingen waarmee medeoverheden worden ondersteund. Allereerst een handreiking Clouddienstverlening, uitgaande van de ervaringen zoals deze op zijn gedaan met de Rijkscloud, ten tweede een handreiking goed opdrachtgeverschap informatiebeveiliging, in het bijzonder in het kader van aanbestedingen. Deze handreikingen worden dit najaar afgerond.

Vraag 2
Hoe wordt de veiligheid van vertrouwelijke data die de overheid bewaart en bewerkt gewaarborgd? Waar worden deze data fysiek opgeslagen? Worden vertrouwelijke Nederlandse data ook opgeslagen bij (dochters van) buitenlandse bedrijven en instellingen? Zo ja, welke zijn dat? Maken overheidsorganisaties en semi-publieke instellingen uitsluitend gebruik van datacenters op Nederlands grondgebied en van Nederlandse bedrijven? Zo nee, waarom niet?

Antwoord 2
De Rijksoverheid is op grond van het Besluit Voorschrift informatiebeveiliging rijksdienst (VIR) en de Wet bescherming persoonsgegevens gehouden om passende maatregelen te nemen om persoonsgegevens te beveiligen. Binnen de Rijksoverheid zijn daartoe informatiebeveiligingsplannen opgesteld.
Nederlandse overheidsdata, waaronder vertrouwelijke overheidsdata, worden – net als data die door het Nederlandse bedrijfsleven voor en namens burgers en bedrijfsleven wordt opgeslagen – op diverse plaatsen en bij diverse dienstverleners opgeslagen, zowel in binnen- als buitenland. Daarbij is ook sprake van outsourcing en situaties waarbij leveranciers ook onderdelen van de dienstverlening verder hebben geoutsourcet. In alle gevallen geldt dat outsourcing door het Rijk plaatsvindt met in achtneming van het Besluit Voorschrift Informatiebeveiliging. Gezien de complexiteit, hoeveelheid en vertrouwelijkheid is het thans niet mogelijk om een compleet en dekkend beeld te geven.
Deze situatie was eerder de aanleiding voor het formuleren van een Rijkscloudstrategie en de ontwikkeling van de in vraag 1 genoemde Rijkscloud.

Over het algemeen eisen provincies bij aanbestedingen dat dataverwerking en -opslag binnen de EU moet plaatsvinden. Sommige provincies maken gebruik van commerciële diensten waarbij niet altijd duidelijk is waar de datacenters staan. Daarbij valt niet uit te sluiten dat er ook data buiten de EU wordt opgeslagen.

Vraag 3
Zijn er standaardprocedures voor het kiezen van een dataopslaglocatie en -aanbieder, bijvoorbeeld in Nederland, Europa dan wel ergens anders in de wereld, voor het bewaren van vertrouwelijke data door overheidsorganisaties en semi-publieke instellingen?

Antwoord 3
Het kiezen van een marktpartij wordt beheerst door het aanbestedingsrecht. Met betrekking tot de bijvoorbeeld de Rijksoverheidsdatacenters is als kader gesteld dat een datacenter van de markt zich in Nederland moet bevinden. Voorts geldt bij de keuze de bestaande regels waaronder de al eerder genoemde voorschriften zoals het VIR, BIR en VIRBI.
In de Wet bescherming persoonsgegevens is geregeld dat persoonsgegevens die aan een verwerking worden onderworpen of die bestemd zijn om na hun doorgifte te worden verwerkt, slechts naar een land buiten de Europese Unie worden doorgegeven indien, onverminderd de naleving van de wet, dat land een passend beschermingsniveau waarborgt.
Het College Bescherming Persoonsgegevens kan een vergunning geven voor een doorgifte of een categorie doorgiften van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt. Aan de vergunning worden de nadere voorschriften verbonden die nodig zijn om de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen, alsmede de uitoefening van de daarmee verband houdende rechten te waarborgen.
Voor de openbare lichamen Bonaire, Sint Eustatius en Saba, die niet vallen onder het EU-acquis, is een vergelijkbaar regime geregeld in de Wet bescherming persoonsgegevens BES. De Commissie toezicht bescherming persoonsgegevens BES kan een vergunning verlenen voor doorgifte naar derde landen zonder passend beschermingsniveau.

Vraag 4
Kunt u een overzicht sturen in welke landen, en indien mogelijk bij welke organisaties, de vertrouwelijke data van alle ministeries, provincies, gemeenten en de semi-publieke instellingen wordt opgeslagen?

Antwoord 4
Het is niet mogelijk om een dergelijk overzicht voor alle ministeries, provincies, gemeenten en de semi-publieke instellingen te geven en valt wat betreft provincies, gemeenten en de semi-publieke instellingen buiten mijn verantwoordelijkheid. Wel kan ik u wijzen op het antwoord op vraag 1 voor wat betreft de plannen van de Rijksoverheid voor het inrichten van een Rijkscloud. Voor de Rijksdienst kan ik gezien de complexiteit, hoeveelheid en vertrouwelijkheid op dit moment geen compleet en dekkend beeld geven. In dezen verwijs ik ook naar het verslag van de European Cloud Partnership Steering Board november 2013:«The general goal of establishing a fully functioning Internal Market for cloud computing needs to be stressed. In practice, the cloud market remains fragmented at this time: the location of data is often seen as critical, especially in the public sector, not only because of security reasons, but due to restrictive regulations in this regard, and due to the problems administrations face when procuring a cloud service. We must avoid any «Fortress Europe» perception that isolates European clouds from international markets (or bars access to them to international service providers). Security, integrity, accessibility and control over clouds must be ensured, but the members agree that geographical location is not a necessary component of these high level requirements; strong encryption based on open and established algorithms could achieve better results than geographic restrictions. There is a need in the cloud market to move from trusting companies to trusting standards and systems.» In de European Cloud Partnership Steering Board werken overheidsinstanties en het bedrijfsleven samen met het doel bij te dragen aan de opbouw van een digitale interne

markt voor cloud computing in de EU, overeenkomstig de Europese cloud computing-strategie. Voor Nederland neemt de CIO Rijk hieraan deel.

Vraag 5
Kunt u uitsluiten dat vertrouwelijke data van overheidsorganisaties en/of semi-publieke instellingen in datacenters buiten Nederland of in eigendom van niet-Nederlandse bedrijven zijn opgeslagen? Zo ja, hoe dan? Zo nee, bent u bereid u in te zetten dat op zo kort mogelijke termijn alle vertrouwelijke data in beheer bij overheidsorganisaties en semi-publieke instellingen enkel nog in datacenters binnen Nederland en van Nederlandse bedrijven en instellingen worden bewaard en beheerd? Zo nee, waarom niet? Zo ja, per wanneer kunt u dit bewerkstelligen?

Antwoord 5
Nee, ik kan dit niet uitsluiten voor alle overheidsorganisaties. Binnen de Rijksdienst is gekozen voor inbesteding en onderbrenging in de eigen datacenters, maar voor andere overheidsorganisaties kan ook sprake zijn van uitbestedingen. Daarbij gelden de Europese aanbestedingsregels. In 2011 is naar aanleiding van de motie Elissen en Schouw (Vergaderjaar 2011–2012, Kamerstuk 32 761, nr. 13), daarover het volgende aan uw Kamer gerapporteerd: «Op overheidsopdrachten zijn de algemene beginselen van mededinging van de Europese Unie van kracht, waaronder het beginsel van non-discriminatie. De Europese aanbestedingsregels zijn mede op deze beginselen gebaseerd. Het uitvoeren van de motie Elissen en Schouw kan gelet op het voorgaande niet tot het gewenste resultaat leiden. Zoals al is gesteld in het antwoord van de Minister van Veiligheid en Justitie aan de Kamer op vragen van het lid Elissen (Aanhangsel van de Handelingen, nr. 3681) is hier sprake van een conflict in wetgeving dat in eerste instantie tussen overheden moet worden opgelost. De consequenties van dit conflict in wetgeving kunnen niet via de aanbestedingsprocedure worden opgelost. Dit conflict in wetgeving beperkt zich bovendien niet tot Nederland. Ook in andere landen van de Europese Unie speelt dit op vergelijkbare wijze. In de motie Van der Steur wordt de regering opgeroepen om in Europees verband aan te dringen op een gezamenlijke regeling voor de bescherming van gegevens. Dit probleem is bekend bij de Europese Commissie. In dit verband is te melden dat de Europese Commissaris voor Justitie, grondrechten en burgerschap begin november heeft aangekondigd dat zij eind januari 2012 met voorstellen zal komen voor de herziening van de Richtlijn gegevensbescherming uit 1995. Mogelijk bevatten die voorstellen aanzetten voor een oplossing van dit jurisdictieconflict. Ik zal na publicatie en behandeling van deze voorstellen terugkomen op het onderwerp van de moties.» (Vergaderjaar 2011–2012 Kamerstuk 32 761, nr. 14).
In de onderhandelingen over herziening van de genoemde Richtlijn gegevensbescherming, namelijk de voorgestelde Algemene Verordening Gegevensbescherming, is door Nederland de problematiek van conflicterende jurisdicties naar voren gebracht. Hierbij streeft Nederland naar een zoveel mogelijk sluitende regeling voor dit probleem (BNC fiche, Vergaderjaar 2011–2012, Kamerstuk 22 112, nr. 1372, p. 7). Over de voortgang van de onderhandelingen wordt door het kabinet ieder kwartaal een brief gestuurd, waarvan de laatste op 22 april dit jaar (Vergaderjaar 2013–2014, Kamerstuk 33 169, T). De laatste stand van zaken van de onderhandelingen op dit punt is weergegeven in de geannoteerde agenda voor de JBZ Raad van 5-6 mei, aangeboden per brief van de Minister en Staatssecretaris van Justitie van 28 mei jl. (punt 6, pagina 12: «bescherming van persoonsgegevens in nationale databases»).

Vraag 6
Hoe wordt de veiligheid van vertrouwelijke data in het bezit van de overheid op het gebied van de gebruikte software gewaarborgd? Kunt u aangeven hoeveel overheidsorganisaties en semi-publieke instellingen bijvoorbeeld gebruik maken van Microsoft 365? Bent u er van op de hoogte dat vertrouwelijke data die in Microsoft 365 gegenereerd, bewerkt dan wel beheerd worden, in de Microsoft Cloud worden opgeslagen en dat bijvoorbeeld de NSA deze data desgevraagd kan inzien?

Antwoord 6
In een beperkt aantal gevallen wordt er gebruik gemaakt van de mogelijkheden die Microsoft 365 biedt. Indien en voor zover sprake is van opslag van vertrouwelijke data, dan wel datacommunicatie via Microsoft gelden daarvoor de regels met betrekking tot beveiliging (zoals bij de Rijksdienst de BIR) van die data, waaronder encryptie. Daarbij zullen organisaties die gebruik maken van cloudoplossingen voor opslag en verwerking van – bijzondere – persoonsgegevens moeten voldoen aan het gestelde in de Wet bescherming persoonsgegevens. Het College Bescherming Persoonsgegevens heeft hierover een zienswijze opgesteld [1] Uitgangspunt daarbij is dat de organisatie zelf verantwoordelijk blijft voor de bescherming van persoonsgegevens en eventueel zelf nadere afspraken moet maken. Het College heeft daarnaast ook een document opgesteld voor de beveiliging van persoonsgegevens, de Richtsnoeren beveiliging van persoonsgegevens[2]. Dit document bevat richtlijnen en handvatten voor de beveiliging van persoonsgegevens.
Voor de Rijksoverheid geldt verder dat op het opslaan van gerubriceerde informatie het Besluit Voorschrift Informatiebeveiliging – Bijzondere Informatie 2013 (VIRBI 2013) van toepassing is. Daarin worden aanvullende eisen gesteld.

Vraag 7
Speelt bij de overwegingen van overheidsorganisaties en semi-publieke instellingen om bepaalde software te gebruiken überhaupt de dataopslaglocatie die deze software gebruikt mee? Zo ja, uit welke documenten blijkt dat? Is hier een strategisch afwegingskader voor of hangt het af van omstandigheden die per situatie kunnen verschillen, zoals bijvoorbeeld kosten?

Antwoord 7
Zie ook het antwoord op vraag 6. De medeoverheden en semi-publieke instellingen zijn zelf verantwoordelijk voor de beveiliging van hun vertrouwelijke gegevens. Ik treedt daarbij adviserend op vanuit mijn coördinerende bevoegdheid voor de informatievoorziening binnen de openbare sector. De AIVD levert de Rijksoverheid onafhankelijk advies over het beschermen van staatsgeheimen met behulp van ICT-beveiligingsoplossingen.
Mede vanwege het vraagstuk rond dataopslag bij gebruik van software, wordt bij het Rijk gebruik gemaakt van eigen applicationstores. Daarmee worden applicaties binnen het Rijk aangeboden waarvan ook de dataopslag en communicatie via de eigen beveiligde infrastructuur loopt.

Vraag 8
Bent u bereid meer aandacht te gaan besteden aan bewustwording bij lokale overheden en semi-publieke instellingen wat betreft de risico's die de fysieke opslaglocatie van vertrouwelijke data buiten Nederland met zich meebrengt? Bent u bereid de Algemene inlichtingen- en veiligheidsdienst (AIVD) om advies te vragen op welke wijze alle Nederlandse overheidsorganisaties hun vertrouwelijke data het beste kunnen opslaan en beheren? Zo ja, op welke termijn kunnen de ministeries, provincies, gemeenten en de semi-publieke instellingen dit AIVD-advies verwachten? Zo nee, waarom niet?

Antwoord 8
De overheid heeft een bijzondere verantwoordelijkheid voor de beveiliging van gegevens die de burger aan haar toevertrouwt en voor de integriteit van data. Voor het behouden van het vertrouwen van burgers en bedrijven in de overheid is het dan ook van groot belang dat de overheid een adequaat informatieveiligheidsbeleid hanteert. Er ligt daarom een belangrijke taak bij de bestuurders van iedere overheidsorganisatie om risicobewust te sturen en informatieveiligheid structureel te verankeren in de organisatie, daarbij ondersteund door een stelsel van verplichtende zelfregulering binnen iedere overheidslaag en -sector. Ik heb dan ook de Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) ingesteld om bestuurders bij de overheid te doordringen van het belang van informatieveiligheid, waarbij overheden zelf verantwoordelijk zijn en blijven voor de wijze waarop informatieveiligheid een

[1] http://www.cbpweb.nl/Pages/med_20120910-zienswijze-cbp-cloudcomputing.aspx
[2] http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf

structurele plek krijgt in de organisatie en de wijze waarop het informatieveiligheidsbeleid gestalte krijgt (vergaderjaar 2012 – 2013, Kamerstuk 26 643, nr. 269).
Behalve bewustwording en borging van informatieveiligheid bij afzonderlijke organisaties is het van belang dat het samenspel van organisaties in het openbaar bestuur op het terrein van informatieveiligheid leidt tot een efficiënte en effectieve manier van de aanpak bij incidenten en crisis. Samen met het Nationaal Cyber Security Centrum (NCSC) en schakelorganisaties van de medeoverheden wordt gewerkt aan een netwerk waarin kennisdeling, melding van incidenten en lessons learned worden gedeeld en incidenten en crises worden opgepakt.
Voor het tweede deel van uw vraag: de AIVD heeft tot taak te bevorderen dat de verantwoordelijke en competente autoriteiten en instanties zorg dragen voor een adequate beveiliging. De beveiligingsbevorderende activiteiten van de AIVD richten zich op de taakvelden bijzondere informatie, vitale sectoren, personen, objecten en diensten behorend tot het rijksdomein, en andere aandachtsgebieden die in relatie tot de nationale veiligheid zijn benoemd. De AIVD ondersteunt de betreffende instanties door te adviseren over beveiligingsmaatregelen en de instelling van vertrouwensfuncties, te informeren over dreigingen, te faciliteren bij de productie, distributie en registratie van cryptografisch sleutelmateriaal, en door onderzoeken naar kandidaten voor vertrouwensfuncties uit te voeren.