Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Aanhangsel van de Handelingen

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

1219

Vragen van de leden **Bontenbal** en **Van der Molen** (beiden CDA) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «Studentgegevens ondanks kritiek massaal in de Amerikaanse cloud gezet»* (ingezonden 20 oktober 2022).

Antwoord van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Minister van Onderwijs, Cultuur en Wetenschap (ontvangen 9 januari 2023).

Vraag 1
Bent u bekend met het bericht «Studentgegevens ondanks kritiek massaal in de Amerikaanse cloud gezet»[1]?

Antwoord 1
Ja.

Vraag 2
Kunt u bevestigen dat op dit moment 75% van alle Nederlandse studentgegevens opgeslagen staat bij (Amerikaanse) big tech-cloudaanbieders? In hoeverre geldt dit ook voor onderzoeksgegevens en digitale lessystemen?

Antwoord 2
Eigen gegevens over het cloudgebruik door universiteiten zijn niet bekend bij het Ministerie van OCW. Instellingen zijn zelf eigenaar van data en «verwerkingsverantwoordelijke» zoals bedoeld in de Algemene Verordening Gegevensbescherming (AVG). Ze zijn dan ook vrij en zelf verantwoordelijk voor het vormgeven en aangaan van samenwerkingen op het gebied van ICT en het gebruik van cloud. Uiteraard moeten die samenwerkingen in lijn zijn met de AVG, waarin ook bepalingen over het delen van data met derde landen zijn opgenomen. De Autoriteit Persoonsgegevens (AP) ziet toe op de zorgvuldige omgang met persoonsgegevens in het onderwijs. Om het onderwerp public cloudgebruik verder op te pakken willen wij, in lijn met het Rijksbreed cloudbeleid 2022, sessies organiseren om het onderwerp verder uit te dragen. Hierbij willen wij graag maatschappelijk relevante organisaties, waaronder kennisinstellingen, uitnodigen. Daarnaast gaan we dit onderwerp

[1] https://fd.nl/samenleving/1454238/studentgegevens-ondanks-kritiek-massaal-in-de-amerikaanse-cloud-gezet-jrj2ca00CiRh.

ah-tk-20222023-1219
ISSN 0921 - 7398
's-Gravenhage 2023

verder oppakken in het kader van de Werkagenda Waardengedreven Digitalisering.
In de Kamerbrief van 14 juli 2022, over het verhogen van digitale veiligheid in onderwijs en onderzoek[2], wordt door de Minister van OCW ook ingegaan op hoe de sector daarbij wordt ondersteund, bijvoorbeeld door het faciliteren van Data Protection Impact Assessments (DPIA's), op producten die in het onderwijs veel gebruikt worden. Daarmee geeft het kabinet uitvoering aan de motie van de leden Kwint en Van Meenen.[3] Door de DPIA's kunnen instellingen beter geïnformeerde keuzes maken over de privacy van leerlingen en studenten. De DPIA's, waarbij de instellingen worden ondersteund door SURF en SIVON, sluiten aan op het advies van de AP.
Verder is op 11 mei 2022 het «Referentiekader privacy en ethiek voor studiedata» voor verantwoord gebruik van studiedata gepubliceerd door Versnellingsplan ICT[4]. Hierin zijn gezamenlijke kaders bepaald die zorgvuldige omgang met studiedata en studentgegevens bevorderen. Het referentiekader is omarmd door de onderwijs koepelorganisaties Universiteiten van Nederland (UNL) en de Vereniging Hogescholen (VH).

Vraag 3
Deelt u de mening dat deze situatie het risico op privacyschending, spionage en een verlies van strategische autonomie met zich meebrengt?

Antwoord 3
Het kabinet ziet de genoemde risico's, en heeft daartoe reeds verschillende stappen gezet. Deze worden hierna kort uiteen gezet.
Voor wat betreft privacy worden er Data Protection Impact Assessments (DPIA's) uitgevoerd en worden contractonderhandelingen met grote leveranciers in het onderwijs centraal gevoerd.[5] Daarmee kunnen instellingen beter geïnformeerde keuzes maken over de privacy van leerlingen en studenten en kunnen alle instellingen gebruikmaken van dezelfde contractvoorwaarden. Hiermee wordt aangesloten op het advies van de AP.
Verder is op 11 mei 2022 het «Referentiekader privacy en ethiek voor studiedata» voor verantwoord gebruik van studiedata gepubliceerd. Hierin zijn gezamenlijke kaders bepaald die zorgvuldige omgang met studiedata en studentgegevens bevorderen. Het referentiekader is omarmd door de VH en UNL. SURF, koepels en marktpartijen trekken gezamenlijk op in de uitvoering en er wordt continu bekeken of er waarborgen kunnen worden verbeterd.
Voor wat betreft spionage weten we dat kennisinstellingen doelwit zijn van spionageactiviteiten. Een aantal staten voert een offensief programma tegen Nederlandse belangen en probeert onder andere aan unieke Nederlandse kennis (bijvoorbeeld onderzoeksgegevens) en technologieën te komen. Daarbij is in een aantal, veelal autoritaire staten, een nauwe verwevenheid tussen het bedrijfsleven en de overheid.[6, 7] Deze risicos adresseert het kabinet met de aanpak Kennisveiligheid en de aanpak Tegengaan Statelijke Dreigingen.[8]c[9]
In de Nederlandse gedragscode wetenschappelijke integriteit is opgenomen dat kennisinstellingen een zorgplicht hebben voor een werkomgeving waarin goed onderzoek gewaarborgd wordt. Databeheer wordt daarin expliciet genoemd. In de Nationale Leidraad Kennisveiligheid is ook een hoofdstuk over digitale beschermingsmaatregelen en cyberveiligheid opgenomen. Zo worden instellingen die met sensitieve onderzoeksdata of resultaten werken gewezen op het nemen van maatregelen op het gebied van rubricering, autorisatie en de implementatie van specifieke organisatorische en technologische maatregelen om mogelijke aanvallen te detecteren en te monitoren om zodoende de risico's beter te borgen.
Voor strategische autonomie heeft het kabinet op 8 november jl. de kabinetsbrede visie op de open strategische autonomie van de EU naar de Kamer

[2] Kamerbrief «Verhogen digitale onderwijs en onderzoek»| 14-7-2022.
[3] Kamerstuk 32 034, nr. 34.
[4] Versnellingsplan ICT. Referentiekader privacy en ethiek voor studiedata.
[5] Kamerstuk 32 034, nr. 34.
[6] Kamerstuk 30 821, nr. 125
[7] Kamerstuk 29 924, nr. 212 en 30 977
[8] Kamerstuk 31 288, nr. 894.
[9] Kamerstuk 30 821, nr. 125

gestuurd.[10] Het kabinet werkt verder onder coördinatie van EZK aan een nadere invulling van de digitale autonomie van de digitale economie en infrastructuur. Deze invulling is naar verwachting in de loop van 2023 gereed.

Vraag 4
Welke afspraken maken Nederlandse (hoger)onderwijsinstellingen met techbedrijven bij het aangaan van contracten over bijvoorbeeld (economische) veiligheid en privacy? In hoeverre is hier überhaupt ruimte voor in de onderhandeling?

Antwoord 4
Onderwijsinstellingen zijn, conform de AVG, verantwoordelijk voor de omgang met persoonsgegevens en worden geacht hier zorgvuldig invulling aan te geven. Wanneer een instelling gebruik maakt van een product of dienst waarbij persoonsgegevens worden verwerkt moeten zij met de betreffende leverancier een verwerkersovereenkomst afsluiten waarin wordt vastgelegd welke persoonsgegevens voor welke doeleinden mogen worden verwerkt en onder welke voorwaarden dat gebeurt. Om de veiligheid van gegevensverwerkingen te waarborgen en te voorkomen dat een verwerking inbreuk maakt op de AVG, moet de verwerkingsverantwoordelijke de aan de verwerking inherente risico's beoordelen en op grond van een objectieve en zo concreet mogelijke risicobeoordeling passende technische en organisatorische maatregelen nemen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd. Als een verwerking toch een hoog risico blijft inhouden dan is voorafgaand aan de verwerking een DPIA verplicht, zodat op basis daarvan maatregelen kunnen worden genomen om die risico's te voorkomen of te reduceren. Zo maakte een eerder uitgevoerd assessment van Microsoft duidelijk dat er voor het gebruik van bepaalde Microsoftproducten geen grote risico's overblijven, mits de gebruiker een aantal maatregelen neemt om de risico's te mitigeren. Bij het assessment van Google zijn privacyrisico's geconstateerd, met name over hun omgang met metadata. Vervolgens zijn met Google afspraken gemaakt over het mitigeren van deze geconstateerde risico's. Met leveranciers van producten die veel gebruikt worden in het onderwijs, worden deze contracten centraal uitonderhandeld door SURF en worden dan ook afspraken gemaakt over veiligheid en privacy.[11] Deze contracten gelden dan voor de hele sector zodat niet iedere instelling zelf deze onderhandelingen hoeft te doen en alle instellingen ook onder dezelfde voorwaarden producten kunnen gebruiken. Tevens is het omgaan met kennis uit gevoelige kennisdomeinen expliciet opgenomen in de Nationale Leidraad Kennisveiligheid.

Vraag 5
In hoeverre kunt u centrale kaders bieden aan onderwijsinstellingen die zien op het waarborgen van privacy, online veiligheid en strategische onafhankelijkheid in de samenwerking met cloudbedrijven? Ziet u hier voor uzelf een rol weggelegd?

Antwoord 5
In de antwoorden op vraag 2, 3 en 4 heb ik uiteengezet hoe het kabinet, en de Minister van OCW in het bijzonder, hiermee omgaan. In de kamerbrief over het verhogen digitale veiligheid onderwijs en onderzoek van 14 juli 2022 gaat de Minister dieper in op de stappen die gezamenlijk worden gezet.[12]

Vraag 6
Welke serieuze alternatieven zijn er voor onderwijsinstellingen, maar ook voor de rijksoverheid, voor het gebruik van cloudoplossingen van Amerikaanse techbedrijven?

---

[10] «Kamerbrief over open strategische autonomie» | 8-11-2022
[11] Zie ook https://www.surf.nl/compliancyvoor meer informatie over hoe leden via SURF gezamenlijk afspraken maken met ICT- en contentleveranciers over de levering en afname van producten en diensten.
[12] Kamerbrief Verhogen Digitale veiligheid onderwijs en onderzoek. 14 juli 2022.

Antwoord 6
Het kabinet zet zich er op in om door middel van verschillende initiatieven concurrentie op de markt voor clouddiensten te stimuleren. Door meer concurrentie kunnen alternatieve aanbieders van clouddiensten, waaronder Europese aanbieders, inspelen op de vraag vanuit onderwijsinstellingen en de rijksoverheid. Initiatieven die hieraan bijdragen zijn onder andere de DMA en de Dataverordening, de IPCEI Cloud Infrastructure and Services en het GAIA-X project.
Voorts wordt momenteel in het kader van de Cyberbeveiligingsverordening (Cyber Security Act) een Europees certificatieschema ontwikkeld voor de clouddiensten. De cyberbeveiligingsverordening is een Europese verordening, die een Europees kader introduceert op het gebied van cyberbeveiligingscertificering. De cyberbeveiligingsverordening maakt het mogelijk om op Europees niveau cyberbeveiligingscertificeringsregelingen (in de praktijk ook wel aangeduid als «certificatieschema's») vast te stellen voor categorieën van ICT-producten, -diensten en -processen. In opdracht van de Europese Commissie wordt thans een cyberbeveiligingscertificeringsregeling voor de clouddiensten (de zgn. Europese Cloud certificering schema) met cyberbeveiligingsvoorschriften ontwikkeld. Naar verwachting zal dit schema medio 2023 worden opgeleverd. Na de implementatie hiervan zullen de cloudaanbieders binnen twee jaar moeten voldoen aan de vereiste security maatregelen.

Vraag 7
Wat is de status van de voorbereiding van de investeringsvoorstellen in het kader van de IPCEI Cloud[13]?

Antwoord 7
De Nederlandse investeringsvoorstellen voor IPCEI Cloud zijn op 4 april jl. bij de Europese Commissie ingediend. Het verplichte goedkeuringsproces voor de voorstellen neemt door de omvang en complexiteit van deze IPCEI meer tijd in beslag dan eerder aangenomen door alle betrokken partijen. De huidige verwachting is dat dit proces begin 2023 zal worden afgerond, waarna de Tweede Kamer geïnformeerd kan worden over de investeringsvoorstellen die voor subsidie in aanmerking komen.

Vraag 8
Bent u bereid om te onderzoeken of de rijksoverheid samen met onderwijsinstellingen initiatieven kan opstarten of ondersteunen die zien op het ontwikkelingen van eigen cloudoplossingen? Op welke manier zou u kunnen aanhaken bij Europese initiatieven?

Antwoord 8
SURF biedt een mix van eigen clouddiensten en aanbod van marktpartijen. Binnen de SURFcumulus cloud dienst van SURF bieden 13 leveranciers hun diensten aan. Dit betreft Nederlandse, Europese en Amerikaanse aanbieders, grote en kleinere leveranciers. Verder heeft SURF eigen clouddiensten, op eigen rekensystemen van SURF, waaronder de Nationale Supercomputer Snellius. Met SURFdrive, Research Drive en SURFfilesender, kunnen bestanden worden opgeslagen en verstuurd. Ook voert SURF projecten uit waarin verkenningen plaatsvinden binnen diverse toepassingsgebieden waarin wordt gekeken naar open source alternatieven, zoals voor een samenwerkingsomgeving – zoals officeapplicaties –, een leeromgeving, enquête tools en grafische software. De verkenningen moeten antwoord geven op vragen over de gebruiksvriendelijkheid, de toepasbaarheid binnen een bestaande organisatie, support en ondersteuning, beheer, security, privacy, mogelijkheden om te koppelen met andere onderwijssystemen en een duurzame en gezonde governance als het gaat om de betrouwbaarheid van de software en de community daaromheen.
De Minister van OCW heeft in 2021 heeft de Europese Commissie verzocht om de ontwikkeling van openbare opensource alternatieven voor grote particuliere digitale platforms te ondersteunen.[14] Vooralsnog heeft dit in

[13] IPCEI: Important Project of Common European Interest.
[14] Kamerstuk 21 501-34, nr. 370

EU-verband niet tot concrete vervolgacties op onderwijsgebied geleid.[15] Nederland zal hiervoor aandacht blijven vragen. Ook zal Nederland een gezonde(re) marktwerking, publieke waarden en onderwijskwaliteit blijven agenderen in het Europese debat.

[15] Wel lopen er bredere projecten, zoals een van oorsprong Frans-Duits initiatief, GAIA-X dat een data- en cloudinfrastructuur wil gaan ontwikkelen waarbij Europese waarden als data-soevereiniteit geborgd worden en IPCEI-CIS, Important Project of Common European Interest Cloud Infrastructuur en Services. Doel is een Europese cloudinfrastructuur met -diensten op te zetten die moeten bijdragen aan cyberveiligheid, interoperabiliteit en duurzame toepassingen.