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

842

Vragen van het lid **Van der Woude** (VVD) aan de Minister van Onderwijs, Cultuur en Wetenschap over *het artikel «Studentgegevens ondanks kritiek massaal in de Amerikaanse cloud gezet.»* (ingezonden 17 oktober 2022).

Antwoord van Minister **Dijkgraaf** (Onderwijs, Cultuur en Wetenschap), mede namens de Minister voor Buitenlandse Handel en Ontwikkelingssamenwerking (ontvangen 25 november 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 642.

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

Antwoord 1
Ja.

Vraag 2
Heeft u, in het kader van kennisveiligheid en als stelselverantwoordelijke, eigen gegevens over de aard en omvang van cloudgebruik door universiteiten? Komen die overeen met de gegevens die deze internationale studie heeft gevonden?

Antwoord 2
Eigen gegevens over het cloudgebruik door universiteiten heb ik niet. 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 clouddiensten. Instellingen moeten zeer zorgvuldig met persoonsgegevens omgaan en zij moeten de juiste technische en organisatorische maatregelen nemen om risico's voor betrokkenen zoveel mogelijk te beperken. De Autoriteit Persoonsgegevens (AP), waarin ook bepalingen over het verstrekken van data aan derde landen zijn opgenomen, ziet toe op de zorgvuldige omgang met persoonsgegevens in het onderwijs. Wanneer een derde partij wordt ingezet

[1] Financieele Dagblad, 16 oktober 2022, Studentgegevens ondanks kritiek massaal in de Amerikaanse cloud gezet, https://fd.nl/samenleving/1454238/studentgegevens-ondanks-kritiek-massaal-in-de-amerikaanse-cloud-gezet#:~:text=Ondanks%20waarschuwingen%20van%20experts%20staat,blijkt%20uit%20een%20internationale%20studie.

ah-tk-20222023-842
ISSN 0921 - 7398
's-Gravenhage 2022

bij de verwerking van persoonsgegevens, zal elke instelling zich ervan moeten vergewissen dat zij enkel een beroep doet op partijen die voldoende waarborgen bieden, om zo te kunnen voldoen aan de vereisten van de AVG. De AP ziet toe op de zorgvuldige omgang met persoonsgegevens in het onderwijs.

Vraag 3
Bent u het eens met de auteur en de stellers van eerdere noodkreten vanuit universiteiten en de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW), dat het risicovol is om universiteiten afhankelijk te laten zijn van techbedrijven voor hun gegevensbeheer?

Antwoord 3
Het kabinet is zich bewust van de risico's die voortkomen uit de afhankelijkheid en marktmacht van grote IT dienstverleners. Juist omdat we de mogelijke risico's erkennen, zetten we als kabinet in op goede risicoanalyses en de bevordering van concurrentie. Ook brengen we ons beleid en dat van het veld in lijn met Europese Verordeningen op dit gebied, waaronder de Cyber Security Act. Zie voor meer details de antwoorden op de volgende vragen.
In mijn kamerbrief van 14 juli 2022, over het verhogen van digitale veiligheid in onderwijs en onderzoek[2], ga ik dieper in op hoe wij de sector bij hun digitale veiligheid ondersteunen, wat niet wegneemt dat zij daar uiteindelijk zelf verantwoordelijk voor zijn. Zo faciliteren wij 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, sluiten aan op het advies van de AP.
Een eerder uitgevoerde DPIA van Microsoft maakte ook duidelijk dat er voor het gebruik van bepaalde Microsoft-producten geen grote risico's overblijven, mits de gebruiker een aantal mitigerende maatregelen neemt. 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. In algemene zin is het beheersen van risico's ook een essentieel onderdeel in de Nederlandse Cybersecuritystrategie (NLCS) 2022–2028 die recent is gepubliceerd.[4]
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.

Vraag 4
Vindt u dat hierin een risico schuilt op misbruik van data van studenten en docenten door Big Tech?

Antwoord 4
Het gebruik van clouddiensten is sterk groeiend vanwege de voordelen die het biedt. Er zijn internationaal vele aanbieders en ook SURF biedt een mix van eigen clouddiensten en aanbod van marktpartijen. Het is afhankelijk van de leverancier en de contractbepalingen of de privacy van gebruikers in het geding zou zijn of niet. Net als bij andere vormen van uitbesteding is het nodig de voordelen, nadelen en de risico's af te wegen.
Als onderwijsinstellingen voor een bepaald platform kiezen, zijn zij verantwoordelijk voor een zorgvuldige omgang met de persoonsgegevens van leerlingen, studenten en docenten en de naleving van privacywetgeving, waarvan de AVG de belangrijkste is. Instellingen moeten onder meer zorgdragen voor het opstellen van informatiebeveiligings- en privacybeleid,

---

[2] Kamerbrief Verhogen Digitale veiligheid onderwijs en onderzoek. 14 juli 2022.
[3] Kamerstuk 32 034, nr. 34.
[4] Nederlandse cybersecuritystrategie (NLCS) 2022–2028. Ambities en acties voor een digitaal veilige samenleving.

de aanstelling van een functionaris voor de gegevensbescherming, de inrichting van toegangs- en beheerrechten in ICT-systemen, de logging hiervan, de uitvoering van risicoanalyses (waarbij prioriteit wordt gegeven aan het analyseren van de diensten die op grote schaal worden gebruikt) en het afsluiten van verwerkersovereenkomsten met leveranciers.[5] SURF ondersteunt de instellingen bij het maken van deze afwegingen en ook in de NLCS wordt de uitvoering van risicoanalyses gestimuleerd. De AP kan op verzoek een advies geven en houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens.

Vraag 5
Ziet u daarnaast een risico op te grote economische afhankelijkheid van universiteiten van Big Tech?

Antwoord 5
Het kabinet is zich bewust van de risico's die voortkomen uit de marktmacht van grote IT dienstverleners. De Autoriteit Consument en Markt (ACM) heeft recent een marktstudie uitgevoerd naar de markt voor clouddiensten.[6]De ACM benoemt daarin het ingesloten raken van gebruikers (lock-in effecten) als een van de belangrijkste risico's in deze markt. Daarnaast benoemt de ACM dat de grootste actieve spelers op de markt verschillende diensten aanbieden in de keten, waarmee het moeilijk concurreren is voor kleinere aanbieders van clouddiensten. En doordat het voor gebruikers moeilijk is om over te stappen naar een andere aanbieder en er steeds minder aanbieders zijn, worden ze steeds afhankelijker van de aanbieder. Dit geldt voor burgers en voor universiteiten. Hierdoor heeft de aanbieder van clouddiensten op de langere termijn minder prikkels om betere of goedkopere diensten aan te bieden. Mede vanwege dit risico zet Nederland zich al langer in voor meer concurrentie in digitale markten, waaronder de markt voor clouddiensten. Daar ga ik dieper op in bij vraag negen.

Vraag 6
Bent u zich bewust van het spionagerisico dat schuilt in het opslaan van onderzoeksgegevens in systemen die onder wetgeving van een ander land vallen? Welke afspraken zijn gemaakt in het kader van cyberveiligheid met universiteiten over het opslaan van onderzoeksgegevens op deze manier?

Antwoord 6
Ja, het kabinet is zich van dit risico bewust. Het kan voorkomen dat kennisinstellingen doelwit zijn van spionageactiviteiten. Een aantal staten voert een offensief programma om bijvoorbeeld aan unieke Nederlandse kennis (zoals onderzoeksgegevens) en technologieën te komen. Daarbij is in een aantal, veelal autoritaire staten, een nauwe verwevenheid tussen het bedrijfsleven en de overheid.[7, 8] Deze risicos adresseert het kabinet met de aanpak Kennisveiligheid en de aanpak Tegengaan Statelijke Dreigingen.[9, 10]
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. Bovendien is in de Nationale Leidraad Kennisveiligheid 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 (veiligheids-) maatregelen.

---

[5] Kamerstuk 32 034, nr. 39.
[6] ACM, «marktstudie clouddiensten», https://www.acm.nl/nl/publicaties/marktstudie-clouddiensten.
[7] Kamerstuk 30 821, nr. 125
[8] Kamerstuk 29 924, nr. 212
[9] Kamerstuk 31 288, nr. 894.
[10] Kamerstuk 30 821, nr. 125

Vraag 7
Zijn er specifiek afspraken die voorkomen dat kennis uit gevoelige kennisdomeinen, zoals in het geval van dual-use-producten, op die manier worden opgeslagen? Zo nee, bent u bezig met het opstellen van afspraken?

Antwoord 7
Ja, zulke afspraken zijn gemaakt door mijn collega M.BHOS van BZ. Navraag bij haar leert dat de overdracht van dual-use-software en -technologie naar buiten het douanegebied van de Europese Unie aan exportcontrole wordt onderworpen. Dit staat in de herziene EU dual-use-verordening 2021/821. Hieronder wordt onder andere (en niet uitsluitend) overdracht via de cloud verstaan. De wijze waarop deze controle kan en zou moeten plaatsvinden, is momenteel onderdeel van besprekingen in EU-verband over de implementatie van de dual-use-verordening.
Nederland heeft reeds beleid omtrent export via de cloud geïmplementeerd. Voor de export vanuit Nederland van dual-use-kennis en -technologie gelden dezelfde regels als voor de export van goederen en apparatuur. Aan de opslag van dual-use-technologie worden daarom ook specifieke eisen gesteld. Deze informatie moet volgens de industriestandaarden worden opgeslagen. Deze industriestandaarden zijn bedoeld om de onrechtmatige toegang tot deze data te voorkomen. Het Ministerie van Buitenlandse Zaken heeft hierover een factsheet[11] opgesteld voor het bedrijfsleven en is hierover blijvend in gesprek met de industrie.

Vraag 8
Op welke manier is een beheersing van bovengenoemde risico's verwerkt in de nieuwe aanpak kennisveiligheid voor het hoger onderwijs?

Antwoord 8
De aanpak kennisveiligheid bestaat uit een palet aan beleidsmaatregelen die elkaar aanvullen. Een van de maatregelen is de Nationale Leidraad Kennisveiligheid, waarin de bovengenoemde risico's en de mitigatie daarvan wordt behandeld. De Leidraad gaat onder andere in op het toetsen en inschatten van risico's, risicomanagement en cyberveiligheid. Eind dit jaar gaat een externe audit van start om bij de universiteiten en hogescholen om te toetsen hoe ver zij zijn met de implementatie van de Leidraad. Zie ook mijn antwoord bij vraag 9.

Vraag 9
Welke stappen onderneemt u om economische onafhankelijkheid en kennisveiligheid te borgen?

Antwoord 9
Ik zal in het onderstaande antwoord eerst ingaan op kennisveiligheid en daarna economische afhankelijkheid.
De maatregelen op het gebied van kennisveiligheid zijn te verdelen in drie onderdelen. Ten eerste zet het kabinet in op het versterken van bewustzijn bij en zelfregulering door de kennisinstellingen. De rijksoverheid heeft samen met kennisinstellingen de Nationale Leidraad Kennisveiligheid opgesteld. Over de implementatie van de maatregelen in deze leidraad zijn afspraken gemaakt in het bestuursakkoord hoger onderwijs en wetenschap. Onderdeel van die afspraken is dat kennisinstellingen op systematische wijze risicoanalyses uitvoeren op kennisveiligheid, waarna zij rapporteren aan hun Raden van Toezicht. Ik spreek vervolgens met de Raden van Toezicht gezamenlijk over de bevindingen. Op de implementatie van de Leidraad, waar de risicoanalyse onderdeel van uitmaakt, wordt een externe audit uitgevoerd. Ook het Rijksbrede Loket Kennisveiligheid en de bestuurlijke kennisveiligheidsdialoog dragen bij aan bewustwording en zelfregulering op dit thema.
Ten tweede zet het kabinet in op het instellen van een toetsingsmechanisme voor de meest sensitieve kennisgebieden. Zoals in de laatste voortgangsrapportage over kennisveiligheid al werd aangekondigd, zal het toetsingskader op zijn vroegst in 2023 in werking treden, gezien invoering van de maatregel

[11] https://www.rijksoverheid.nl/documenten/brochures/2018/10/23/factsheet-export-via-de-cloud

complex en ingrijpend is. Het kabinet onderstreept daarbij het belang van zorgvuldigheid en van draagvlak onder de Nederlandse kennisinstellingen. Ten derde zet het kabinet in, met gelijkgezinde landen, op afstemming en samenwerking in de EU en internationaal op het gebied van kennisveiligheid. Eind dit jaar ontvangt de Kamer een brief waarin de voortgang van de kennisveiligheidsmaatregelen wordt geschetst.
Op het gebied van economische afhankelijkheid heeft het kabinet zich de afgelopen jaren sterk gemaakt voor het aanpakken van de macht van Big Tech, via inzet voor de Digital Markets Act (DMA). De DMA gaat gelden voor poortwachters, dit zijn platforms waar gebruikers niet of nauwelijks meer omheen kunnen. Deze Europese regelgeving heeft als doel om gebruikers te beschermen en te zorgen voor meer concurrentie op digitale markten. De DMA zal onder andere voor clouddiensten gaan gelden en bevat diverse verplichtingen waar poortwachters die clouddiensten aanbieden zich aan moeten houden. Poortwachters mogen bijvoorbeeld de mogelijkheid voor gebruikers van clouddiensten om over te stappen naar een andere aanbieder niet belemmeren. In een marktstudie naar de markt voor clouddiensten noemt de ACM de DMA als een van de instrumenten die kan bijdragen aan het verminderen van afhankelijkheid en het stimuleren van concurrentie in de cloudmarkt.[12] De DMA is in september aangenomen door het Europees Parlement en de Raad. Vanaf 2024 zullen de verplichtingen uit de DMA gaan gelden voor aangewezen poortwachters.
Ook de aankomende Dataverordening zal naar verwachting bijdragen aan concurrentie in de cloudmarkt, door het wegnemen van financiële, contractuele en technische barrières om tussen clouddiensten over te stappen. Nederland zet hier ook op in bij de onderhandelingen over de Dataverordening. Het verlagen van deze barrières zal op den duur de economische en strategische positie van Nederland en Europa versterken. Er wordt ook geïnvesteerd in de ontwikkeling van alternatieve cloudoplossingen via bijvoorbeeld de IPCEI Cloud Infrastructure and Services.
Daarnaast heeft mijn voorganger de Europese Commissie verzocht om de ontwikkeling van openbare opensource alternatieven voor grote particuliere digitale platforms te ondersteunen.[13] Vooralsnog heeft dit in EU-verband niet tot concrete vervolgacties op onderwijsgebied geleid.[14] Nederland zal hiervoor aandacht blijven vragen. Ook zal Nederland een gezonde(re) marktwerking, publieke waarden en onderwijskwaliteit blijven agenderen in het Europese debat.

Vraag 10
Kunt u deze vragen beantwoorden voor de begrotingsbehandeling van Onderwijs, Cultuur en Wetenschap en tevens meenemen in de update over de nieuwe aanpak kennisveiligheid die is toegezegd voor het einde van dit jaar?

Antwoord 10
Ja.

Vraag 11
Kunt u de vragen afzonderlijk beantwoorden?

Antwoord 11
Ja.

[12] ACM, «marktstudie clouddiensten», https://www.acm.nl/nl/publicaties/marktstudie-clouddiensten.
[13] Kamerstuk 21 501-34, nr. 370
[14] Wel lopen er bredere projecten, zoals een van oorsprong Frans-Duits initiatief, GAIA-X dat een data- en cloud infrastructuur 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 cloud infrastructuur met -diensten op te zetten die moeten bijdragen aan cyberveiligheid, interoperabiliteit en duurzame toepassingen.