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

841

Vragen van het lid **Kwint** (SP) aan de Minister van Onderwijs, Cultuur en Wetenschap over *het bericht dat studentgegevens ondanks kritiek massaal in de cloud zijn gezet* (ingezonden 18 oktober 2022).

Antwoord van Minister **Dijkgraaf** (Onderwijs, Cultuur en Wetenschap) (ontvangen 25 november 2022). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 643.

Vraag 1
Wat is uw reactie op het bericht «Studentgegevens ondanks kritiek massaal in de cloud gezet»?[1]

Antwoord 1
Ik herken de bezorgdheid die uw Kamer hierover uit. Het gebruik van clouddiensten is sterk groeiend vanwege de voordelen die het biedt. Er zijn internationaal vele aanbieders, en het is afhankelijk van de leverancier en contractbepalingen of de privacy in het geding zou zijn of niet. Net als bij andere vormen van uitbesteding is het nodig de voordelen en de risico's af te wegen. Dat is een afweging die een kennisinstelling zelf maakt. Dat maakt dat ik over digitale veiligheid, privacy en de daarbij horende risico's al langer in gesprek ben met de sector.

Vraag 2
Waarom hebben het Ministerie van Onderwijs, Cultuur en Wetenschap, universiteiten en hogescholen de waarschuwingen van experts in de wind geslagen en driekwart van hun studentgegevens opgeslagen bij datacenters van Microsoft en Amazon?

Antwoord 2
Ik deel de stelling niet dat universiteiten en hogescholen de waarschuwingen in de wind hebben geslagen. In de gesprekken die ik met de sector voer, merk ik dat digitale veiligheid serieus wordt genomen. We maken gezamenlijk werk van digitale veiligheid. Een belangrijk voorbeeld zijn Data Protection Impact Assessments (DPIA's). Dit zijn risicoanalyses die we samen met SURF,

[1] Het 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?utm_medium=social&utm_source=whatsapp&utm_campaign=earned&utm_content=20221018.

ah-tk-20222023-841
ISSN 0921 - 7398
's-Gravenhage 2022

Kennisnet en SIVON faciliteren[2] op producten die in het onderwijs veel gebruikt worden. Daardoor kunnen instellingen beter geïnformeerde afwegingen maken over de privacy van leerlingen en studenten.
Een eerder uitgevoerde DPIA van Microsoft maakte 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.[3]
In meerdere Kamerbrieven heb ik uiteengezet welke maatregelen (hoger) onderwijsinstellingen precies nemen om de digitale veiligheid en de cyberweerbaarheid van de sector te vergroten, zo ook in mijn laatste Kamerbrief over digitale veiligheid[4]. Bij die maatregelen ligt prioriteit op het vergroten van bewustzijn rondom cyberdreigingen, het borgen van risicomanagement om meer inzicht te krijgen in de risico's en deze op kosteneffectieve wijze te mitigeren én aandacht voor (keten-) samenwerking om kennis-en informatiedeling over risico's, monitoring en detectie te vergroten. Verder is in de Nationale Leidraad Kennisveiligheid een hoofdstuk over cyberveiligheid opgenomen. Tot slot werkt SURF met de aangesloten instellingen, onderwijskoepels, ketenpartners en marktpartijen doorlopend aan het verbeteren en waarborgen van de digitale veiligheid.

Vraag 3
Erkent u dat het cloudgebruik omstreden is, omdat de privacy in het geding is? Welke mogelijke gevaren liggen op de loer door dit cloudgebruik?

Antwoord 3
Zoals ik bij vraag 1 schreef zijn er internationaal vele aanbieders, en het is afhankelijk van de leverancier en contractbepalingen of de privacy in het geding zou zijn of niet. Net als bij andere vormen van uitbesteding is het zinvol de voordelen en de risico's af te wegen en dat doen de instellingen ook.
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. Zo kan die op grond van een objectieve en zo concreet mogelijke risicobeoordeling passende technische en organisatorische maatregelen nemen. Die maatregelen moeten passen bij de grootte van het risico. 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.
Mocht de verwerking van persoonsgegevens door Clouddiensten van buiten de Europese Unie plaatsvinden, dan is het verder belangrijk dat inzichtelijk wordt gemaakt hoe dit rechtmatig plaatsvindt. Een dergelijke verwerking kan rechtmatig zijn, mits voldaan aan de voorwaarden van hoofdstuk V van de AVG. Daarbij is het van belang dat de richtsnoeren die op 18 juni 2021 zijn vastgesteld door het Europees Comité voor Gegevensbescherming (EDPB) worden gevolgd. Deze richtsnoeren beogen bedrijven en organisaties conform de AVG handvatten te bieden bij de beoordeling welke aanvullende maatregelen zij kunnen treffen bij de verwerking van persoonsgegevens door derden.

Vraag 4
Waarom kiezen hogescholen en universiteiten ervoor om studentgegevens op te slaan bij datacenters van buitenlandse techreuzen? Bent u bereid om hier een stokje voor te steken?

---

[2] Kamerstuk 32 034, nr. 39.
[3] Nederlandse cybersecuritystrategie (NLCS) 2022–2028. Ambities en acties voor een digitaal veilige samenleving.
[4] Kamerbrief Verhogen Digitale veiligheid onderwijs en onderzoek. 14 juli 2022.

Antwoord 4
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. Daarbij moet geldende wet- en regelgeving worden nageleefd. Dat wordt onder andere geëffectueerd met de eerdergenoemde DPIA's en geborgd met de implementatie van de Nationale Leidraad Kennisveiligheid. Zoals ik eerder noemde moeten instellingen gedetailleerde risicoanalyses uitvoeren. Op basis van die analyses kan SURF onderhandelen met leveranciers, om te borgen dat met name niet-Europese leveranciers zich aan Europese (en Nederlandse) wetgeving houden.
De Nederlandse onderwijswereld gebruikt, net als de rest van de maatschappij, op grote schaal de digitale diensten van een beperkte groep van grote Amerikaanse techbedrijven. In ons veld helpt SURF met het bevorderen of onderzoeken van mogelijke Europese alternatieven onder meer om vendor lock-in te voorkomen. Zo is SURF actief in de European Open Science Cloud van de EU en lid van GAIA-X. Daarnaast draait bijvoorbeeld SURFdrive, voor het opslaan en delen van data, op daar onderliggende Europese open software zoals ownCloud. Ook 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.

Vraag 5
Klopt het dat Amerikaanse opsporingsdiensten toegang kunnen hebben tot de studentgegevens van Nederlandse studenten? Welke andere (buitenlandse) instanties hebben inzage in deze gegevens?

Antwoord 5
Onder de AVG (GDPR) is doorgifte van persoonsgegevens naar een land buiten de Europese Economische Ruimte (EER) alleen toegestaan als dat land persoonsgegevens even goed beschermt als landen binnen de EER.[5]
Nationale wetgeving in de VS kent bevoegdheden voor inlichtingendiensten om toegang te verkrijgen tot persoonsgegevens van EU-burgers. Datadoorgifte tussen de EU en de Verenigde Staten (VS) was mogelijk via de EU-VS Privacy Shield afspraken. Op 16 juli 2020 heeft het Hof van Justitie van EU deze afspraken echter ongeldig verklaard. Het beschermingsniveau was onvoldoende. Dit betekent dat voor doorgifte van persoonsgegevens aan de VS, het EU-VS privacy shield niet meer gebruikt mag worden en de gegevensverantwoordelijke aanvullende waarborgen moet treffen.
Op 25 maart 2022 maakten president Von der Leyen en president Biden bekend dat ze een principeakkoord hebben bereikt over nieuwe afspraken voor datadoorgifte. Op 7 oktober 2022 ondertekende president Biden een Executive Order voor implementatie van deze afspraken. De Executive Order introduceert nieuwe bindende waarborgen om alle door het Hof van Justitie van de EU aan de orde gestelde punten aan te pakken, de toegang tot EU-gegevens door Amerikaanse inlichtingendiensten te beperken en een Data Protection Review Court in te stellen.[6]
SURF werkt ook actief aan dit onderwerp. Binnen de Taskforce Beyond Privacy Shield werkt SURF samen met de onderwijs- en onderzoekssector om te bepalen hoe de sector het beste met deze situatie kan omgaan. Er wordt gezamenlijk gewerkt aan aanbevelingen en best practices voor een veilige internationale uitwisseling van persoonsgegevens en alternatieven voor het EU-VS Privacy Shield. SURF en de leden kunnen deze aanbevelingen en best practices gebruiken binnen de eigen organisatie.[7]

---

[5] https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/doorgifte-binnen-en-buiten-de-eu
[6] https://ec.europa.eu/commission/presscorner/detail/nl/qanda_22_6045
[7] https://www.surf.nl/surf-taskforce-beyond-privacy-shield

De Cloud Act en wet- en regelgeving uit andere landen maakt het in theorie mogelijk dat opsporingsdiensten toegang krijgen tot deze gegevens. Een risicobeoordeling kan als uitkomst hebben dat dat risico niet onacceptabel groot is. Echter, het is niet uitgesloten dat nadere regelgeving dit anders maakt. Aan het einde van dit jaar wordt namelijk onder meer nadere guidance verwacht van de EDPB (privacytoezichthouders van de EU lidstaten) aangaande internationale doorgifte van persoonsgegevens. Onder meer het Strategisch Leveranciersmanagement Microsoft (SLM) Rijk volgt deze ontwikkelingen op de voet.

Vraag 6
Bent u van mening dat studentgegevens niet door commerciële partijen bewaard moeten worden? Zo nee, waarom niet?

Antwoord 6
Universiteiten en hogescholen zijn vrij om de softwareleveranciers te kiezen die het beste bij hun activiteiten passen, of deze partijen nu een winstoogmerk hebben of niet. Uiteraard zijn de eerder genoemde waarborgen en risicoanalyses belangrijk bij het kiezen van leveranciers.

Vraag 7
Van welke andere commerciële bedrijven zijn universiteiten en hogescholen nog meer afhankelijk? Vindt u dat deze commerciële afhankelijkheid onwenselijk is en de vrije keuze van universiteiten en wetenschappelijke integriteit ondermijnt?

Antwoord 7
Een lijst van alle commerciële bedrijven waarmee instellingen zaken doen kan ik niet te geven. De keuze voor leveranciers is onderdeel van de autonomie die universiteiten en hogescholen hebben. Bij elke afspraak tot commerciële dienstverlening bestaat een zekere afhankelijkheid. Deze is niet inherent beperkend voor de vrije keuze van universiteiten, en ondermijnt niet inherent de wetenschappelijke integriteit. Dergelijke risico's moeten onderdeel zijn van de afweging van de instelling, voordat en terwijl de dienst wordt afgenomen. Dit geldt voor commerciële en voor niet-commerciële dienstverlening.
Verder is het belangrijk om open source alternatieven te verkennen, op nationaal en Europees niveau. Dit heeft mijn voorganger ook eerder in Brussel aangekaart bij de Europese Commissie en hen verzocht om de ontwikkeling van openbare opensource alternatieven voor grote particuliere digitale platforms te ondersteunen.

Vraag 8
Bent u bereid om in samenspraak met deskundigen en onderwijsinstellingen de mogelijkheid van een alternatief in eigen beheer te onderzoeken, zodat hogescholen en universiteiten niet meer afhankelijk zijn van techreuzen?

Antwoord 8
Zoals ik bij vraag 4 benoemde voert SURF projecten uit waarin wordt gekeken naar open source alternatieven, o.a. voor open source leeromgeving, open source samenwerkingsomgeving (waar de bekende officeapplicaties incl. videobellen een subonderdeel van kunnen zijn), open source enquête tools en meer keuzes in grafische software, ook in open source varianten. De verkenningen moeten antwoord geven op vragen over o.a. de gebruiksvriendelijkheid, de toepasbaarheid binnen een bestaande organisatie, support en ondersteuning, beheer, security, privacy, betrouwbaarheid en kansen van die software in relatie tot andere onderwijssystemen.
Mijn voorganger heeft de Europese Commissie verzocht om de ontwikkeling van openbare opensource alternatieven voor grote particuliere digitale platforms te ondersteunen.[8] Vooralsnog heeft dit in EU-verband niet tot

[8] Kamerstuk 21 501-34, nr. 370

concrete vervolgacties op onderwijsgebied geleid.[9] Nederland zal hiervoor aandacht blijven vragen. Ook zal Nederland een gezonde(re) marktwerking, publieke waarden en onderwijskwaliteit blijven agenderen in het Europese debat.

Vraag 9
Kunt u een overzicht geven van de bedragen die worden overgemaakt naar deze techreuzen door hogescholen en universiteiten voor de data-opslag?

Antwoord 9
Het is niet mogelijk om een dergelijk overzicht te geven, omdat het veld decentraal georganiseerd is en de instellingen autonoom keuzes maken. Dergelijke afspraken worden niet bij OCW gemeld.

Vraag 10
Bent u bereid om met hogescholen en universiteiten in gesprek te gaan om een einde te maken aan het opslaan van studentgegevens bij techreuzen?

Antwoord 10
In dit vraagstuk vind ik het niet zozeer van belang of de gegevens bij een «techreus» zijn opgeslagen of bij een andere commerciële of niet-commerciële aanbieder. Het opslaan van gegevens in de cloud kent, naast risico's, ook voordelen voor de instellingen. Ik ben bereid om, naast de inspanningen die ik eerder noemde, in de periodieke gesprekken die ik met de instellingen voer, het gesprek aan te gaan over het opslaan van studentgegevens bij derden. Een einde maken aan het extern opslaan van gegevens is daarbij echter geen uitgangspunt door de autonomie die instellingen hebben en de risicoanalyses en maatregelen die door de instellingen worden toegepast.

[9] 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.