De voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Ministerie van Onderwijs, Cultuur en Wetenschap

Onderzoek en Wetenschapsbeleid
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Contactpersoon

Onze referentie
34878174

Bijlagen

>Retouradres Postbus 16375 2500 BJ Den Haag

Datum 25 november 2022

Betreft Antwoord op schriftelijke vragen van het lid Ephraim (Groep van Haga) aan de minister van Onderwijs, Cultuur en Wetenschap over de inbreuk op de privacy van Nederlandse studenten door Amerikaanse techbedrijven.

Hierbij stuur ik u de antwoorden op de vragen van lid Ephraim (Groep van Haga) aan de minister van Onderwijs, Cultuur en Wetenschap over de inbreuk op de privacy van Nederlandse studenten door Amerikaanse techbedrijven.

De vragen werden ingezonden op 20 oktober 2022 met kenmerk 2022Z19985.

De minister van Onderwijs, Cultuur en Wetenschap,

Robbert Dijkgraaf

Onze referentie
34878174

2022Z19985
(ingezonden 20 oktober 2022)

Onze referentie
34878174

Vragen van het lid Ephraim (Groep Van Haga) aan de minister van Onderwijs, Cultuur en Wetenschap over de inbreuk op de privacy van Nederlandse studenten door Amerikaanse techbedrijven.

1. Kent u de alarmerende nieuwsberichten van de NOS (*'Driekwart Nederlandse studentendata opgeslagen bij Amerikaanse techbedrijven'* [1]), Scienceguide [2] en KNAW [3] waaruit blijkt dat nu 3/4 van de gegevens van Nederlandse studenten in handen is van datacentra van commerciële Amerikaanse Tech bedrijven ten opzichte van 25 % in 2015?

Ja.

2. Erkent u dat de onafhankelijkheid en integriteit van universiteiten sterk in het geding is nu de gegevens grotendeels in handen zijn van Amerikaanse “tech bedrijven” als Amazon, Microsoft en Google en dat dit een ongewenste situatie is die onderzocht en gestopt dient te worden?

De onafhankelijkheid en integriteit van universiteiten is niet (per definitie) in het geding door het gebruik van clouddiensten. Het gebruik van zulke diensten is sterk groeiend vanwege de voordelen die het biedt. Instellingen moeten zich tegelijkertijd bewust zijn van de risico’s en van de afhankelijkheden die door zulke overeenkomsten kunnen ontstaan.

Ik vind dat de keuze voor leveranciers onderdeel is van de autonomie die universiteiten 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.

Verder is het belangrijk om open source alternatieven te verkennen, op nationaal en Europees niveau. Mijn voorganger heeft dit 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[1]. Tegelijkertijd bevordert SURF het onderzoeken van mogelijke alternatieven. SURF biedt een mix van eigen clouddiensten en aanbod van marktpartijen. Binnen de SURFcumulus cloud dienst van SURF bieden 13 leveranciers hun diensten aan. 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. SURF is continu met leden in gesprek over deze kwesties.

[1] *Kamerstukken II* 2021/22, 21501-34, nr. 370

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, ondanks het feit dat zij daar 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 Autoriteit Persoonsgegevens (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 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. 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.

3. Ziet u ook de ernst van de gevaren in van het afstandsonderwijs dat halsoverkop in Coronatijd moest worden ingevoerd en kunt u deze in kaart brengen alsmede eventuele oplossingen?

Gedurende de lockdown was fysiek onderwijs zeer beperkt mogelijk. Om de studievoortgang van studenten te bewaken, zijn onderwijsinstellingen destijds tijdelijk overgestapt naar voornamelijk afstandsonderwijs. Volledig afstandsonderwijs kent nadelen, maar daardoor konden studenten gedurende de lockdown wel blijven studeren. Daarnaast is het bekend dat afstandsonderwijs risico's met zich kan meebrengen rondom privacy en digitale veiligheid. Het is daarbij wel belangrijk om te noemen dat er vele soorten van afstandsonderwijs mogelijk zijn en dat zij ook een eigen risicoprofiel kennen. De risico's moeten worden afgewogen, waarbij de voordelen kunnen opwegen tegen de nadelen.

Hoger onderwijsinstellingen werken aan de privacybescherming naar aanleiding van het advies van de AP. Daarin krijgen onderwijsinstellingen ondersteuning van SURF, bijvoorbeeld met betrekking tot DPIA's. Eind juni 2022 publiceerde SURF het nieuwe 'SURF audit toetsingskader Privacy 2022' waarmee een pilot wordt gestart

[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.

bij de bij SURF aangesloten onderwijsinstellingen. Het toetsingskader zal door het hoger onderwijs worden gebruikt voor gegevensbeschermingsbeleid in overeenstemming met privacyregelgeving. De verwachting van SURF is dat het nieuwe toetsingskader inzicht zal geven in het privacy volwassenheidsniveau van het hoger onderwijs. Eind 2022 worden de resultaten van de pilot door SURF bekendgemaakt.

4. Wat is er aan concrete maatregelen genomen sinds hoogleraren en internetexperts al jaren geleden waarschuwden voor het gevaar van dat data van studenten konden worden misbruikt voor commerciële en politieke doeleinden?

Door instellingen worden DPIA's uitgevoerd om risico's scherp te krijgen en te kunnen mitigeren. Daarnaast worden contractonderhandelingen met grote leveranciers in het onderwijs centraal gevoerd.[5] Zo kunnen instellingen beter geïnformeerde keuzes maken over de privacy van leerlingen en studenten en kunnen alle instellingen gebruikmaken van dezelfde contractvoorwaarden. We sluiten daarmee aan op het advies van de AP. In de Kamerbrief over het verhogen van digitale veiligheid in onderwijs en onderzoek van 14 juli jl. ga ik ook in op de genomen maatregelen[6]. Het risico dat statelijke actoren toegang krijgen tot gegevens van instellingen wordt door het kabinet tegengegaan met de aanpak Kennisveiligheid en de aanpak Tegengaan Statelijke Dreigingen.[7][8]

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.

5. Denkt u ook niet dat zolang de veiligheid van studentengegevens niet gegarandeerd kan worden, digitaal onderwijs beperkt dient plaats te vinden, mede in acht genomen dat digitaal onderwijs niet automatisch leidt tot beter onderwijs?

Door de instellingen en de koepels wordt hard gewerkt aan het verhogen van de digitale weerbaarheid naar een niveau dat aantoonbaar veiligheid biedt en de continuïteit en kwaliteit van onderwijs en onderzoek waarborgt. Daarbij is 100 procent veiligheid moeilijk te garanderen. Om dit zo goed als mogelijk te bewerkstelligen worden gemeenschappelijke uitgangspunten voor de hele onderwijs en -onderzoeksector gehanteerd. Ook worden sectorspecifieke afspraken gemaakt, omdat de risico's en de mate van volwassenheid tussen sectoren kunnen verschillen. In de Kamerbrief Verhogen digitale veiligheid onderwijs en onderzoek

[5] Kamerstuk 32 034, nr. 34.
[6] Kamerbrief Verhogen Digitale veiligheid onderwijs en onderzoek. 14 juli 2022.
[7] Kamerstukken II 2020/2021, 31288, nr. 894.
[8] Kamerstukken II 2020/21, 30821, nr. 125

van 14 juli jl. heb ik uiteengezet welke maatregelen de instellingen hebben genomen en verder gaan nemen om de cyberweerbaarheid van hun instelling te verhogen.[9] Het gaat hierbij om maatregelen ten aanzien van vergroten van bewustzijn, borgen van risicomanagement en kennis-en informatiedeling.

Het is de verantwoordelijkheid van scholen en instellingen om goed onderwijs te bieden en de risico's die digitaal onderwijs met zich meebrengen in ogenschouw te nemen. Digitalisering kan helpen de onderwijskwaliteit te verbeteren, mits scholen en instellingen vanuit hun eigen onderwijskundige visie passende en doordachte keuzes maken. Wanneer instellingen ervoor kiezen om digitale hulpmiddelen in te zetten in hun onderwijs, dan zijn zij verantwoordelijk voor een zorgvuldige en weloverwogen omgang met persoonsgegevens, conform de AVG. Het is dan ook van groot belang dat gegevens van studenten en leerlingen veilig en verantwoord verwerkt worden door scholen en instellingen.

6. Bestaan er plannen om universiteiten eigen programma's en datacentra te laten ontwikkelen, zoals de Universiteit van Osnabrück het programma BigBlueButton heeft ontwikkeld?

Nee, deze plannen zijn er niet. Wel helpt SURF om mogelijke Europese alternatieven te bevorderen of onderzoeken. SURF biedt een mix van eigen clouddiensten en aanbod van marktpartijen. Binnen de SURFcumulus cloud dienst van SURF bieden 13 leveranciers hun diensten aan. 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. SURF gaat continu met leden in gesprek over alternatieven om zo onder andere vendor lock-in tegen te gaan.

Overigens wordt BigBlueButton ook door Nederlandse onderwijsinstellingen ingezet. SURF biedt met Filesender een dienst voor het veilig en versleuteld online versturen van bestanden, via Nederlandse servers. Filesender is open source en SURF draagt actief bij aan de ontwikkeling hiervan. Andere voorbeelden van programma's die in eigen beheer zijn ontwikkeld en vervolgens aan instellingen worden aangeboden zijn SURFconext, eduVPN, eduroam en SURFdrive.

7. Kunt u deze vragen op tijd beantwoorden voor het begrotingsdebat in week 47?

Helaas is dit niet gelukt.

[9] Kamerbrief over verhogen digitale veiligheid onderwijs en onderzoek |14 juli 2022