Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

# 31 293 Primair Onderwijs

# 31 289 Voortgezet Onderwijs

# 26 643 Informatie- en communicatietechnologie (ICT)

**Nr. 593**

## BRIEF VAN DE MINISTER VOOR BASIS- EN VOORTGEZET ONDERWIJS EN MEDIA

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 24 september 2021

De voortschrijdende digitalisering in het funderend onderwijs biedt kansen voor verdere verbetering van de onderwijskwaliteit. Tegelijkertijd vraagt dit dat de randvoorwaarden voor toegankelijkheid, privacy en informatiebeveiliging op orde zijn. In deze brief ga ik in op twee aspecten hiervan. Ten eerste moeten leerlingen over een laptop of tablet kunnen beschikken als het onderwijs daar om vraagt. Ten tweede moeten leerlingen en docenten er op kunnen vertrouwen dat er zorgvuldig wordt omgegaan met hun persoonsgegevens.

### Digitalisering in dienst van onderwijskwaliteit

*Digitalisering tijdens Corona*

Scholen hebben in de coronacrisis een prestatie van formaat geleverd door het onderwijs zo goed mogelijk doorgang te laten vinden gedurende de schoolsluitingen. Digitale hulpmiddelen hebben een bijdrage geleverd door onderwijs op afstand te faciliteren, waarmee leerachterstanden zo goed mogelijk beperkt zijn.[1] Er zijn zelfs enkele scholen waar de leerlingen er op vooruit zijn gegaan gedurende de lockdowns met behulp van digitale middelen.[2] Tegelijkertijd zijn bij andere leerlingen de leeropbrengsten onder druk komen te staan, mede als gevolg van een ongunstiger thuissituatie.[3]

Publieke en private partijen hebben scholen zo goed mogelijk ondersteund in de opgave om onderwijs op afstand vorm te geven. Kennisnet en SIVON hebben hard gewerkt om ervoor te zorgen dat het onderwijs over devices, internettoegang en ondersteuning kon beschikken om

[1] Zie bijlage voor een overzicht van de gebruikte platformen, zoals toegezegd aan het lid Wiersma
[2] Inspectie van het Onderwijs (2021), *Effectief afstandsonderwijs*.
[3] Sociaaleconomische Raad (2020), *Online leren in corona-tijd*.

kst-31293-593
ISSN 0921 - 7371
's-Gravenhage 2021

onderwijs op afstand zo effectief mogelijk vorm te geven. Met onder meer de PO-Raad en VO-raad heeft OCW dit gefaciliteerd. Het kabinet heeft hiervoor in totaal € 24 miljoen uitgetrokken.

Via het Nationaal Programma Onderwijs (NPO) ontvangen scholen financiële middelen om corona-gerelateerde leervertragingen in te halen. Daarvoor kiezen ze uit een menukaart van kansrijke interventies, waar de inzet van digitale technologie deel van uitmaakt. Kennisnet heeft voor scholen die hiermee aan de slag willen een overzicht van relevante tools, artikelen en publicaties opgesteld.[4]

*Kansen voor onderwijskwaliteit*

De ervaring en geleerde lessen van de afgelopen periode kunnen scholen benutten voor een doordachte inzet van digitalisering in hun onderwijs in de komende jaren. Bij digitaal ondersteund onderwijs blijft de leraar de bepalende factor voor goed onderwijs. ICT biedt geen vervanging voor fysiek contact. Digitaal lesmateriaal maakt het wel makkelijker om lesstof adaptief, aantrekkelijk en op maat aan te bieden aan leerlingen. Ook kan ICT de werkdruk van docenten verminderen door taken als lesvoorbereidingen te verlichten en goede feedback aan leerlingen digitaal te ondersteunen.

Hierbij is het belangrijk oog te hebben voor de toegankelijkheid van het onderwijs en de privacy van leerlingen en leraren. Ook moeten we ons realiseren dat de continuïteit van het onderwijs in toenemende mate wordt bepaald door de veiligheid van digitale systemen.

## Beschikbaarheid van devices

Het gebruik van devices in het onderwijs is de afgelopen jaren toegenomen en door de coronacrisis nog verder in een stroomversnelling gekomen. Devices waren tijdens de crisis noodzakelijk voor onderwijs op afstand. Bij fysiek onderwijs op school wordt een laptop of tablet ook steeds vaker gebruikt, omdat leerlingen daarmee toegang hebben tot het digitale lesmateriaal dat in toenemende mate in de les wordt gebruikt. Scholen mogen ouders expliciet vrijwillig vragen om een laptop of tablet aan te schaffen, maar wanneer een device noodzakelijk is voor het onderwijs moet de school daarin voorzien als ouders niet kunnen of willen betalen.

Omdat devices in de Wet gratis schoolboeken (WGS) niet onder de definitie van lesmateriaal zijn opgenomen, bestaat er in het voortgezet onderwijs soms onduidelijkheid over de vraag of de kosten voor een device voor de school of voor de ouders zijn. Deze vraag maakt ook deel uit van de aankomende evaluatie van de WGS, zoals is verzocht in de gewijzigde motie van het lid Westerveld c.s.[5] Het eindrapport van deze evaluatie wordt op 28 september 2021 opgeleverd, twee dagen voor het geplande commissiedebat over digitalisering in het onderwijs. Ik vind het belangrijk uw Kamer hier tijdig over te informeren, zodat u de resultaten van het rapport kunt betrekken bij uw oordeelsvorming. Om deze reden zal ik de evaluatie van de WGS op 29 september aanstaande zonder beleidsreactie aan uw Kamer aanbieden. Daarnaast ben ik, de wens van een meerderheid van uw Kamer inachtnemend, gestart met de voorbereidingen om tot besluitvorming te komen over dit vraagstuk. Daarbij neem ik zowel de juridische vraag over de definitie van lesmateriaal in de WGS,

[4] https://www.kennisnet.nl/artikel/11431/nationaal-programma-onderwijs-digitale-technologie-als-interventie/
[5] Kamerstuk 35 300 VIII, nr. 176

als de consequenties voor de bekostiging van scholen mee. De kosten voor het structureel financieren van devices in het vo zijn naar schatting minimaal € 84 mln per jaar. Een zelfde maatregel voor het po kost minimaal € 110 mln per jaar.

**Privacy van leerlingen en informatiebeveiliging**

Door de toenemende inzet van ICT in het onderwijs neemt ook de hoeveelheid gegevens over leerlingen die worden gegenereerd, verzameld en verwerkt toe. Het is van groot belang dat zorgvuldig met persoonsgegevens van leerlingen wordt omgegaan. Zeker waar het gaat om kinderen is het belangrijk dat privacy optimaal geborgd is. Zij hebben volgens de Algemene verordening gegevensbescherming (AVG) en het Verdrag inzake de rechten van het kind recht op specifieke bescherming. Daarnaast moet het onderwijs voorbereid zijn op hacks en (ransomware-)aanvallen, omdat leerlinggegevens op straat kunnen komen te liggen en de continuïteit van het onderwijs in gevaar kan komen.

Veilig digitaal ondersteund onderwijs kan alleen gerealiseerd worden als alle partijen hun verantwoordelijkheid nemen, zodat een sluitende aanpak ontstaat. Ik neem het advies van de Autoriteit Persoonsgegevens (AP) om hierbij ook de stelselverantwoordelijkheid van OCW in te vullen ter harte. Ook het recente rapport van de Inspectie van het Onderwijs naar digitale weerbaarheid in het hoger onderwijs is daar heel duidelijk over: digitale veiligheid moet stevig op de agenda, in alle onderwijssectoren.[6] Ik zal in overleg met de sector en ondersteunende organisaties een pakket aan maatregelen uitwerken dat erop ziet dat de hele keten van informatiebeveiliging en privacy versterkt wordt. Op elk niveau kunnen en moeten nog extra stappen gezet worden: (1) welke verantwoordelijkheden kunnen individuele onderwijsinstellingen zelf invullen; (2) welke vraagstukken kunnen beter door schoolbesturen gezamenlijk worden opgepakt en (3) waar is aanvullende coördinatie of ondersteuning vanuit de rijksoverheid nodig.

*Ad 1. Wat kunnen onderwijsinstellingen zelf?*

Onderwijsinstellingen zijn verantwoordelijk voor de omgang met persoonsgegevens conform de AVG en worden geacht hier zorgvuldig invulling aan te geven. Vrijwel alle schoolbesturen hebben inmiddels beleid ten aanzien van informatiebeveiliging en privacy (IBP).[7] Tegelijkertijd wordt het voor elke school steeds complexer om de privacy van leerlingen optimaal te borgen en zich voldoende te beschermen tegen digitale dreigingen.

De AP houdt als onafhankelijk toezichthouder toezicht op de naleving van de AVG door schoolbesturen. Mede naar aanleiding van de gewijzigde motie van het lid Wiersma[8]heb ik contact gehad met de AP over het gebruik van digitale leermiddelen in het onderwijs. De AP monitort de toenemende inzet van digitale leermiddelen op basis van signalen die zij binnenkrijgen en geeft daar zo nodig ook advies over. Dit is bijvoorbeeld gebeurd naar aanleiding van de adviesaanvraag over Google Workspace for Education.

---

[6] Inspectie van het Onderwijs (2021). *Binnen zonder kloppen: digitale weerbaarheid in het hoger onderwijs*

[7] CHOICE Insights + Strategy. (2020) *Monitor IBP 2019 1-meting*

[8] Kamerstuk 32 034, nr. 38

*Ad 2. Wat kunnen onderwijsinstellingen gezamenlijk?*

Door samen te werken kunnen schoolbesturen kennis en capaciteit bundelen zodat complexe vraagstukken rondom privacy en informatiebeveiliging gezamenlijk aangepakt kunnen worden. Een goed voorbeeld hiervan is het Privacyconvenant. Dit is een gezamenlijk initiatief van publieke en private partijen die in de leermiddelenketen van het po, vo en mbo actief zijn.[9] Het convenant is een waardevol instrument dat ervoor zorgt dat leveranciers van digitale onderwijsmiddelen in Nederland duidelijke en eenduidige afspraken maken met onderwijsinstellingen over de verwerking van persoonsgegevens. Voor Nederlandse leveranciers van digitaal lesmateriaal kan dat via de modelovereenkomst van het Privacyconvenant.

Wanneer een leverancier persoonsgegevens verwerkt die een hoog risico vormen voor de privacy van leerlingen of leraren, volgt uit de AVG dat er meer nodig is: er dient een gegevensbeschermingseffectbeoordeling (ook wel Data Protection Impact Assessment of DPIA) uitgevoerd te worden. Ook bij leveranciers die het Privacyconvenant hebben ondertekend kan een DPIA nodig zijn. Het is voor individuele scholen lastig om zelf een dergelijke complexe DPIA uit te voeren. Een krachtige vorm van samenwerking op dit vlak is de afgelopen jaren ontstaan in de coöperatie SIVON, die namens schoolbesturen DPIA's op veelgebruikte leerlingadministratiesystemen uitvoert. Op dit moment zijn 385 besturen lid van SIVON. Dat is 24 procent van de besturen in het po en 62 procent van de besturen in het vo. Dat is nog niet genoeg. Ik roep daarom alle schoolbesturen in het po en vo die nog geen lid zijn van SIVON op om dit zo snel mogelijk te worden.

*Ad 3. Waar moet de overheid ondersteunen of coördineren?*

De toenemende complexiteit van vraagstukken rondom privacy en informatiebeveiliging vraagt ook om een reflectie op de rol van de overheid hierbij. Daar waar scholen zelf of in samenwerking met elkaar onvoldoende in staat zijn om de privacy van leerlingen te beschermen en zich te beschermen tegen digitale dreigingen, zal de overheid extra ondersteuning moeten bieden. Er is op dit moment geen sluitend beeld van cyberveiligheid in het funderend onderwijs. Dat is kwetsbaar. De Inspectie van het Onderwijs trekt diezelfde conclusie over het hoger onderwijs in hun rapport over digitale weerbaarheid in het hoger onderwijs. Er is meer regie nodig vanuit de overheid om gaten op stelselniveau te voorkomen.

Kennisnet brengt op mijn verzoek in kaart hoe het digitaal ondersteund onderwijs nog veiliger gemaakt kan worden, zodat alle schoolbesturen in het funderend onderwijs hun verantwoordelijkheid voor privacy, beveiliging en continuïteit op een duurzame manier kunnen invullen.

De rijksoverheid[10] ondersteunt samen met SURF en SIVON het onderwijs bij de uitvoering van DPIA's op grote internationale technologiebedrijven. Inmiddels zijn er DPIA's op Microsoft en Google uitgevoerd en is er overeenstemming over het mitigeren van de daarin geconstateerde risico's. Tevens loopt er een DPIA op Zoom. Ten aanzien van internationale technologiebedrijven worden er in aanvulling op het Privacyconvenant

---

[9] Initiatiefnemers van het Privacyconvenant zijn: de PO-Raad, de VO-raad, de MBO Raad, de Groep Educatieve Uitgeverijen (GEU), de Vereniging Digitale Onderwijs Dienstverleners (VDOD) en de leden van de sectie Educatief van de Koninklijke Boekverkopersbond (KBb-e)

[10] Via het onderdeel Strategisch Leveranciersmanagement Rijk van het Ministerie van Justitie en Veiligheid.

dus maatregelen genomen om de privacy van leerlingen en leraren optimaal te beschermen. Op deze manier geef ik invulling aan de motie van de leden Kwint en Van Meenen[11] over het Privacyconvenant. Ik licht deze invulling nader toe in de bijlage bij deze brief. Tevens informeer ik u daarin over de stand van zaken van de DPIA op Google Workspace for Education.

In lijn met het advies van de AP ga ik samen met mijn collega Van Engelshoven en de sectororganisaties in het onderwijs bezien wat in de toekomst nodig is om ook met dit soort bedrijven goede afspraken te maken over de privacy van leerlingen en studenten. Omdat de AVG gestoeld is op Europese regelgeving zal ik ook in Europa aandacht vragen voor dit vraagstuk.

*Tot slot*

Ik ben ervan overtuigd dat digitalisering het onderwijs aantrekkelijker, leuker en effectiever kan maken. In dit kader werk ik met de Staatssecretaris van EZK, de sectorraden, bonden, beroepsorganisaties en uitvoerende expertorganisaties aan voorstellen voor de tweede ronde van het Groeifonds om doordachte digitalisering van het onderwijs te stimuleren en de kennisinfrastructuur te verbeteren. Lodewijk Asscher is gevraagd en bereid gevonden de ontwikkeling van deze voorstellen in goede banen te leiden.

In de bijlage van deze brief vindt u een nadere toelichting over de uitvoering van de deze brief genoemde moties en toezeggingen en een update over de stand van zaken van de invoering van het pseudoniem in het po, vo en mbo.

De Minister voor Basis- en Voortgezet Onderwijs en Media,
A. Slob

[11] Kamerstuk 32 034, nr. 33

## Bijlage: toezeggingen en moties op het gebied van digitalisering

Toezegging aan het lid Wiersma over gebruikte digitale platformen voor afstandsonderwijs

Zoals toegezegd in het VSO Digitale leermiddelen van 16 juli 2020 informeren we uw Kamer over de digitale platformen die in het primair en voortgezet onderwijs gebruikt zijn voor afstandsonderwijs en of deze veilig zijn. Uit de *Monitor hybride onderwijs* van Kennisnet blijkt dat in het primair onderwijs vooral gebruik is gemaakt van oefensoftware en digitaal materiaal van de gebruikte lesmethode om onderwijs op afstand vorm te geven. Daarnaast maakte 91% van de ondervraagde leraren regelmatig of (heel) vaak gebruik van videoconferencing om contact te houden met leerlingen, bijvoorbeeld via toepassingen van Google, Microsoft of Zoom. In het voortgezet onderwijs is vooral gebruik gemaakt van de elektronische leeromgevingen waar de scholen al mee werkten, aangevuld met toepassingen als Microsoft Teams en Google Classroom. Een derde van de ondervraagde schoolleiders geeft aan dat ze daarvoor een nieuwe licentie aangeschaft hebben. Het overige deel beschikte daar al over.

Uit een peiling van Kennisnet onder ruim 500 scholen over digitale samenwerkplatformen blijkt dat toepassingen van Microsoft op de meeste scholen gebruikt worden (79% in het po en 83% in het vo), gevolgd door Apple (46% in het po en 37% in het vo) en Google (45% in het po en 32% in het vo).[12]

Onderwijsinstellingen zijn verantwoordelijk voor de omgang met persoonsgegevens conform de Algemene verordening gegevensbescherming (AVG) en worden geacht hier zorgvuldig invulling aan te geven, ook bij onderwijs op afstand. Om scholen hier weloverwogen keuzes in te kunnen laten maken heeft Kennisnet via lesopafstand.nl een privacy-quickscan voor veelgebruikte applicaties gepubliceerd. Scholen kunnen op basis daarvan een eigen afweging maken. Daarnaast zijn er met leveranciers die het Privacyconvenant hebben ondertekend afspraken over de verwerking van persoonsgegevens en is er zowel op Microsoft als op Google een DPIA uitgevoerd waarna er afspraken zijn gemaakt over het verwerken van persoonsgegevens conform AVG. Op Zoom wordt op dit moment een DPIA uitgevoerd. Ten slotte nemen we het advies van de AP om te komen tot een versterking van informatiebeveiliging en privacy in het onderwijs ter harte en zullen we hier met de sector over in gesprek gaan.

Motie van de leden Kwint en Van Meenen over het ondertekenen van het privacyconvenant door internationale technologiebedrijven[13]

*Het Privacyconvenant*

Het Convenant Digitale Onderwijsmiddelen en Privacy (hierna: Privacyconvenant) is een initiatief van de PO-Raad, de VO-raad, de MBO Raad, de Groep Educatieve Uitgeverijen (GEU), de Vereniging Digitale Onderwijs Dienstverleners (VDOD) en de leden van de sectie Educatief van de Koninklijke Boekverkopersbond (KBb-e). Het doel van het Privacyconvenant is zorgen dat leveranciers van digitale onderwijsmiddelen in Nederland duidelijke en eenduidige afspraken maken met onderwijsinstellingen over de verwerking van persoonsgegevens. Inmiddels is het Privacyconvenant door meer dan 400 partijen ondertekend. Het Privacy-

[12] https://www.kennisnet.nl/artikel/10423/onderzoek-naar-gebruik-van-devices-en-samenwerkplatformen-dit-zijn-de-cijfers/

[13] Kamerstuk 32 034, nr. 33

convenant is hiermee dé graadmeter geworden voor goede privacy-afspraken over digitale onderwijsmiddelen. Op basis van actuele inzichten en ervaringen wordt het convenant periodiek door de convenantpartijen geüpdatet. Momenteel wordt er in het kader van het publiek-private overlegplatform Edu-K gewerkt aan versie 4.0.

Het Privacyconvenant is geen wet- of regelgeving voor het onderwijs maar een concretisering van bepaalde verplichtingen die uit de AVG voorvloeien. Hoewel in het Privacyconvenant bepaald is dat de daarin opgenomen bepalingen niet in rechte afdwingbaar zijn, betekent dit niet dat ondertekening daarvan zonder waarde is. Met het convenant beloven partijen de modelverwerkersovereenkomst te gebruiken. Voor scholen geeft deze modelverwerkersovereenkomst duidelijkheid en zekerheid omdat zij met iedere leverancier die zich bij het Privacyconvenant heeft aangesloten eenzelfde type verwerkersovereenkomst kunnen afsluiten. De verwerkersovereenkomsten die scholen en leveranciers met elkaar afsluiten op basis van de modelverwerkersovereenkomst zijn wel in rechte afdwingbaar. Partijen kunnen elkaar aanspreken op ieders verantwoordelijkheid volgens de AVG.

Dit betekent dat ondertekening van het Privacyconvenant geen doel op zich is, maar fungeert als een waardevol (signalerings- en disciplinerings-)instrument om middels gemeenschappelijk vastgestelde afspraken de onderwijsinstellingen en leveranciers te ondersteunen bij de naleving van de wettelijke regels. Wanneer een leverancier het Privacyconvenant ondertekent is dat voor scholen een signaal dat deze leverancier een betrouwbare partner wil zijn voor de school. Op de website www.privacy-convenant.nl kunnen scholen voor dit doel een actuele lijst van aangesloten bedrijven vinden.

*Data Protection Impact Assessment (DPIA)*

Wanneer een leverancier persoonsgegevens verwerkt die een hoog risico vormen voor de privacy van leerlingen, studenten of docenten volgt uit de AVG dat er een gegevensbeschermingseffectbeoordeling (ook wel Data Protection Impact Assessment of DPIA) uitgevoerd moet worden. Naar aanleiding van de DPIA kunnen maatregelen getroffen worden om deze privacyrisico's te verkleinen. Onderwijsinstellingen zijn, in het kader van de AVG, verantwoordelijk voor het uitvoeren van een DPIA. Het Privacy-convenant maakt transparant welke bedrijven zich hebben gecommitteerd aan gezamenlijke afspraken over een goede omgang met leerlinggegevens.

Het tekenen van het Privacyconvenant is geen alternatief voor het uitvoeren van een DPIA. Ook op partijen die het Privacyconvenant ondertekend hebben moeten onderwijsinstellingen een DPIA uitvoeren wanneer er potentieel hoge privacyrisico's bestaan. Op dit moment worden er DPIA's uitgevoerd bij de vijf grootste leerlingadministratiesystemen in het primair en voortgezet onderwijs.[14] Bij elke DPIA zijn meerdere schoolbesturen betrokken en SIVON en Kennisnet ondersteunen hen daarbij. Omdat de producten voor alle scholen in Nederland hetzelfde zijn en ook het gebruik in hoge mate overeenkomt, worden de resultaten van de DPIA onder alle schoolbesturen gedeeld.

Het is een goede zaak dat de coöperaties SIVON en SURF scholen en onderwijsinstellingen ondersteunen die DPIA's uitvoeren op partijen die op grote schaal persoonsgegevens in het onderwijs verwerken. Een

[14] Magister, Somtoday, ParnasSys, Esis en SchoolOAS. Deze leveranciers hebben het Privacyconvenant ondertekend.

individuele school of instelling mist de expertise om dit voor al hun leveranciers te doen. Omdat een DPIA complex is en de systemen die scholen gebruiken weinig van elkaar verschillen is het efficiënter om gezamenlijk DPIA's uit te voeren.

*Internationale technologiebedrijven en het Privacyconvenant*

Het Privacyconvenant staat ook voor internationale technologiebedrijven open om zich bij aan te sluiten omdat delen van hun dienstverlening vallen onder de definitie «digitale onderwijsmiddelen». Als zij ervoor kiezen om dit niet te doen, dan is het wenselijk dat zij hun beweegredenen transparant en begrijpelijk uitleggen aan de scholen en instellingen. Scholen kunnen deze informatie dan betrekken bij hun bredere afweging om producten van deze bedrijven te gebruiken.

OCW is geen partij in het Privacyconvenant, dat is een initiatief van de sectorraden en private partijen. Ik kan partijen niet verplichten om het Privacyconvenant te ondertekenen. Daarnaast is ondertekening van het Privacyconvenant geen doel op zich. De privacy van leerlingen is geborgd wanneer er goede verwerkersovereenkomsten met leveranciers worden gesloten. Daarom bevordert het kabinet dat er DPIA's worden uitgevoerd op deze internationale technologiebedrijven die (onder meer) in het Nederlandse onderwijs actief zijn, en dat scholen en onderwijsinstellingen ook met deze bedrijven de juiste overeenkomsten t.a.v. de verwerking van persoonsgegevens kunnen afsluiten. De rijksoverheid werkt hierbij, via het onderdeel Strategisch Leveranciersmanagement Rijk van het Ministerie van Justitie en Veiligheid, nauw samen met de organisaties in het onderwijs, zoals SURF en SIVON. Dit heeft geleid tot DPIA's op Microsoft en Google en overeenstemming over het mitigeren van de geconstateerde risico's.

Ten aanzien van internationale technologiebedrijven die in het Nederlandse onderwijs actief zijn worden er in aanvulling op het Privacyconvenant dus maatregelen genomen om de privacy van leerlingen en leraren optimaal te beschermen. Tevens zullen we het gesprek hierover met de sector, ook naar aanleiding van het advies van de AP aan ons, blijven voeren.

De motie van het lid Wiersma over in gesprek gaan met de Autoriteit Persoonsgegevens over digitale leermiddelen en of deze voldoen aan de privacywetgeving[15]

Ten principale houdt de Autoriteit Persoonsgegevens (AP) als onafhankelijk toezichthouder toezicht op iedereen die persoonsgegevens verwerkt, ook in het onderwijs. De AP richt zelf haar eigen toezicht in en maakt daarbij eigen keuzes. Om deze onafhankelijkheid te waarborgen is het niet aan ons om te bepalen waar de AP onderzoek naar doet. Naar aanleiding van de motie Wiersma zijn we in gesprek gegaan met de AP over het gebruik van digitale leermiddelen in het onderwijs. Daarin gaf de AP aan de toenemende inzet van digitale leermiddelen in het onderwijs te monitoren op basis van de signalen die zij binnenkrijgen, conform de werkwijze van de AP als onafhankelijk toezichthouder. In die rol heeft de AP een advies uitgebracht aan SURF en SIVON naar aanleiding van de adviesaanvraag over Google Workspace for Education. Daarnaast adviseert de AP dat OCW vanuit haar stelselverantwoordelijkheid de aanpak van gegevensbescherming binnen het onderwijs coördineert door het instellen, dan wel ondersteunen van organisaties en samenwerkingsverbanden die daarin voorzien. Met de Minister van OCW neem ik dit

[15] Kamerstuk 32 034, nr. 38

advies ter harte en zal in overleg met de sector en ondersteunende organisaties een pakket aan maatregelen uitwerken die erop zien dat de hele keten van informatiebeveiliging en privacy versterkt wordt, zodat de veiligheid van digitaal onderwijs in de praktijk geborgd wordt.

DPIA op Google Workspace for Education

Voor de zomer hebben mijn collega Van Engelshoven en ik uw Kamer een aantal keer geïnformeerd over de DPIA die op Google Workspace for Education is uitgevoerd.[16] Eerder dit jaar hebben er intensieve gesprekken plaatsgevonden met Google door SURF, SIVON en het Ministerie van Justitie en Veiligheid namens de rijksoverheid. Deze gesprekken hebben geleid tot een uitgebreide set contractuele, organisatorische en technische maatregelen. Deze maatregelen mitigeren alle in de DPIA geïdentificeerde hoge privacy-risico's in voldoende mate. Hierover hebben we uw Kamer op 8 juli 2021 geïnformeerd.[17]

Ik ben blij dat ik uw Kamer kan melden dat Google conform de gemaakte afspraken de nieuwe voorwaarden naar al hun klanten in het onderwijs heeft gestuurd. Daarnaast zijn de scholen door SURF, SIVON en Kennisnet geïnformeerd over wat zij zelf nog moeten doen om de producten van Google veilig te gebruiken.

Gezien het belang dat onderwijsinstellingen de diensten van Google veilig en met bescherming van de privacy moeten kunnen gebruiken, blijven SURF en SIVON namens het onderwijs Google monitoren en met Google in gesprek over de verwerking van persoonsgegevens. Zo wordt er een DPIA op Chrome browser en Chrome OS uitgevoerd. Deze resultaten worden door SURF en SIVON met Google op een vergelijkbare manier besproken als bij Workspace for Education.

De voortgang van de implementatie van het pseudoniem in het po, vo en mbo

Bij het gebruik van digitale leermiddelen worden gegevens over de leerling gedeeld tussen de school en de leverancier van die leermiddelen, zoals inloggegevens en leer- en toetsresultaten. Om de gegevensuitwisseling rond digitale leermiddelen veiliger te maken, is in 2018 de wet pseudonimiseren ingevoerd. Scholen kunnen hierdoor voor elke leerling een uniek pseudoniem krijgen. Met dit pseudoniem kunnen scholen en leveranciers minder gegevens van leerlingen uitwisselen. Zoals bij de wetsbehandeling is toegezegd aan uw Kamer, informeren wij u over de stand van zaken.

In het po is voor ruim 96 procent van de leerlingen een pseudoniem aangevraagd, in 2019 was dat nog 70 procent. In het vo is voor zo'n 95 procent van de leerlingen een pseudoniem aangevraagd. Scholen en leveranciers werken gezamenlijk aan het voorzien van de laatste groep leerlingen van een pseudoniem zodat de gegevensuitwisseling in de keten voor alle leerlingen op basis van het pseudoniem kan plaatsvinden. Ook in het mbo wordt gebruik gemaakt van de voorziening. We zien dat de invoering van het pseudoniem in het po en vo bijna is afgerond en dat ook in het mbo stappen gezet worden door instellingen leveranciers. Wanneer het pseudoniem succesvol is ingevoerd kan het aantal persoonsgegevens dat wordt uitgewisseld door instellingen worden beperkt. Daarmee geven onderwijsinstellingen invulling aan het uitgangspunt van dataminimalisatie zoals de Algemene verordeningen gegevensbe-

[16] Voorheen Google G Suite for Education, Kamerstuk 32 034, nr. 39
[17] Kamerstuk 32 034, nr. 41

scherming voorschrijft. Ik waardeer dat scholen en leveranciers op deze manier gezamenlijk werken aan een veiliger en betrouwbaarder toegang tot digitaal lesmateriaal.