AUTORITEIT
PERSOONSGEGEVENS

Advies: Google G Suite for Education; z2021-08230

1 Inleiding

Op 4 maart 2021 heeft u, ingevolge artikel 58, derde lid, onder b van de Algemene Verordening Gegevensbescherming (AVG), bij de Autoriteit Persoonsgegevens (AP) een verzoek om advies ingediend, betreffende Google G Suite for Education (thans: Google Workspace for Education).

2 Procedureverloop

De AP heeft op 4 maart 2021 het verzoek om advies ontvangen.

Op 6 april heeft de AP u enkele vragen gesteld ten aanzien van uw adviesvraag.

Op 14 april heeft u de AP voorzien van antwoorden op de door de AP gestelde vragen.

Gelet op de overeenkomsten met het verzoek om voorafgaande raadpleging van de Minister van Justitie en Veiligheid, heeft de AP ervoor gekozen gebruik te maken van haar bevoegdheid ex art. 58 lid 3 sub b AVG en is uw verzoek in samenhang met het verzoek om voorafgaande raapleging van de Minister van Justitie en Veiligheid behandeld.

3 Feitelijke weergave voorgenomen verwerking

Uit de informatie blijkt dat de Hogeschool van Amsterdam en de Rijksuniversiteit Groningen een gegevensbeschermingseffectbeoordeling (hierna: DPIA) hebben laten uitvoeren op de verwerkingen die hierdoor (zullen gaan) plaatsvinden. SURF en SIVON onderschrijven de uitkomsten van deze DPIA. SURF en SIVON voeren - via en met het ministerie van Justitie en Veiligheid – overleg met Google over de privacy- en contractvoorwaarden voor het gebruik van Google G Suite (Enterprise) for Education voor het gehele onderwijs. SURF en SIVON zijn voornemens om deze (vernieuwde) contracten aan te bieden aan onderwijsinstellingen in Nederland (van primair onderwijs tot en met universiteiten). Het betreft onderwijsinstellingen die nog geen gebruik maken van Google G Suite (Enterprise) for Education alsmede instellingen die daar al wel gebruik van maken en hun contracten wensen te vervangen door de nieuwe contracten via SIVON en SURF. SURF en SIVON zijn niet de verwerkingsverantwoordelijke voor de inzet van Google G Suite for Education, maar de onderwijsinstellingen. Door samen te werken middels SURF en SIVON kunnen onderwijsinstellingen kennis en kunde bundelen en mogelijk komen tot (betere) afspraken met beoogde leveranciers in het licht van de AVG. De AP richt zich met dit advies derhalve niet alleen tot SURF, maar ook tot de Nederlandse onderwijsinstellingen.

Een DPIA kan uitermate geschikt zijn om te onderzoeken of er leveranciers bestaan die soortgelijke diensten leveren die een hoger niveau van bescherming van persoonsgegevens bieden dan reeds bestaande leveranciers. Zeker bij een (voorgenomen) inzet van applicaties door een veelheid van onderwijsinstellingen is het wenselijk om een diepgaande analyse uit te voeren naar de risico's voor de rechten en vrijheden van betrokkenen die het inzetten van deze applicaties mogelijk met zich meebrengen. De zorg voor een rechtmatige verwerking van persoonsgegevens van onderwijspersoneel is essentieel, zeker daar waar een werkgever andere organisaties inschakelt die direct of indirect persoonsgegevens van onderwijspersoneel gaat verwerken. Dat geldt uiteraard ook voor onderwijsdeelnemers (en wettelijk

vertegenwoordigers) wiens persoonsgegevens mogelijk worden verwerkt via deze applicaties; zij hebben daarbij veelal geen keuze om al dan niet in deze applicaties voor te komen.

Uit de uitgevoerde DPIA blijkt dat de inzet van deze applicaties zal leiden tot verwerkingen van persoonsgegevens. De DPIA noemt daarbij verwerkingen van drie soorten gegevens. Het gaat daarbij om Customer Data, Diagnostic Data en Functional Data. Er wordt in de DPIA stilgestaan bij de applicaties die worden ingezet en voor welke doelen daarbij persoonsgegevens worden verwerkt. In de DPIA is aangegeven dat een aantal beginselen en artikelen uit de AVG niet of onvoldoende worden ingevuld en dit tot risicovolle aspecten leidt. Door de geconstateerde onvoldoende invulling van beginselen en artikelen voldoet de voorgenomen verwerking op die punten volgens de indieners niet aan de AVG. Het gaat daarbij, samengevat, om de volgende gesignaleerde risico's in de DPIA:

- Gebrek aan doelbinding over de Inhoudelijke gegevens (Customer Personal Data) en Diagnostische gegevens (Diagnostic Data);
- Gebrek aan transparantie over de Inhoudelijke gegevens (Customer Personal Data) en Diagnostische gegevens (Diagnostic Data);
- Geen grondslag voor Google en de verwerkingsverantwoordelijke en onenigheid over rolverdelingen;
- Ontbrekende privacycontroles voor beheerders en gebruikers;
- Gebrek aan controle over het delen van gegevens met (sub-)verwerkers en derde partijen;
- Onvermogen om de rechten van de betrokkenen uit te (laten) oefenen.

Na gesprekken tussen de minister van Justitie en Veiligheid c.q. SURF en SIVON en Google zijn deze risico's naar het oordeel van SURF en SIVON in onvoldoende mate gemitigeerd. SURF en SIVON hebben daarom over deze risico's een verzoek om advies ingediend bij de AP.

4 Beoordeling verzoek om advies

Rol AP en scope

De AP merkt vooraf op dat vrijwel alle risico's rondom de verwerking van persoonsgegevens tevens ook onderdeel zijn van de onderhandelingen tussen SURF en SIVON en Google. Zo is in de DPIA bijvoorbeeld aangegeven dat er verschil van mening bestaat tussen partijen over de vraag wie ten aanzien van bepaalde verwerkingen verwerkingsverantwoordelijke(n) is/zijn. Het is niet de rol van de AP om bij dit verzoek namens bepaalde partijen in discussie te treden over deze vragen en risico's of als geschilbeslechter op te treden in deze onderhandelingen. Partijen zijn zelf gehouden de AVG na te leven.

De AP constateert daarbij dat het onderhavige verzoek enkel is ingediend door SURF en SIVON en niet mede ook namens, of door, Google. Dit levert met name een problematische situatie op indien er verwerkingen zijn waarbij mogelijk sprake is van een gezamenlijke verwerkingsverantwoordelijkheid. De AP heeft zich daarom enkel een algemeen beeld gevormd van de verwerking op basis van de documentatie die is aangeleverd door SURF en SIVON en doet nadrukkelijk geen inhoudelijke uitspraken over de juistheid van de standpunten van partijen.

Basisprincipes AVG, minimumniveau van bescherming

De AP merkt uit de documentatie op dat er in het proces rondom het opstellen van de DPIA gesprekken zijn gevoerd over de beginselen en artikelen uit de AVG. De AP wijst erop dat deze fundamentele beginselen juist in de AVG zijn opgenomen om een uniform hoog niveau van gegevensbescherming binnen de EU te bewerkstellingen. Deze fundamentele beginselen zijn opgesteld om onderhandelingen

over het niveau van de gegevensbescherming overbodig te maken. De AP merkt op dat dit bijvoorbeeld, en dus niet uitsluitend, geldt voor:

- het afwijken van de definitie van persoonsgegevens waardoor discrepanties kunnen ontstaan ten aanzien van de definitie zoals deze is opgenomen in art. 4 lid 1 AVG;
- de toepassing van de beginselen van rechtmatigheid en transparantie zoals opgenomen in art. 5 lid 1 onder a AVG;
- de toepassing van het beginsel van doelbinding zoals opgenomen in art. 5 lid 1 onder b AVG;
- de toepassing van het beginsel van gegevensminimalisatie zoals opgenomen in art. 5 lid 1 onder c AVG;
- de mogelijkheid die betrokkenen dienen te hebben om hun rechten uit te oefenen zoals deze zijn opgenomen in hoofdstuk III van de AVG.

Uit de DPIA blijkt dat SURF en SIVON de meest fundamentele hoge restrisico's zien rondom deze principes. Zo wordt aangegeven dat onduidelijk is welke (telemetrische) gegevens worden verwerkt en de doeleinden waarvoor gegevens worden verwerkt niet specifiek genoeg zijn en er mogelijk doeleinden ontbreken. Dientengevolge is volgens SURF en SIVON ook geen grondslag vast te stellen voor deze verwerkingen.

Deze risico's die zijn geschetst in de DPIA zien grotendeels op fundamentele beginselen die een vereiste zijn voor elke verwerking van persoonsgegevens die valt onder de AVG. Deze beginselen bepalen met andere woorden of een verwerking van persoonsgegevens mogelijk is. Wanneer een verwerkingsverantwoordelijke (onder andere) niet in staat is om vast te stellen welke verwerkingen van persoonsgegevens er plaatsvinden, voor welk doel, noch welke grondslag van toepassing is, kan deze verwerking niet rechtmatig plaatsvinden.

Verwerkingsverantwoordelijkheid en rolverdeling

Daarnaast constateert de AP dat sommige hoge (rest)risico's samenhangen met de exacte invulling van de rollen van verwerkingsverantwoordelijke en verwerker onder de AVG, welke onderwerp van discussie is tussen partijen. Dit hangt mede samen met het feit dat niet duidelijk is welke gegevensverwerkingen er plaatsvinden. Naar de mening van de AP biedt de DPIA op dit punt ook onvoldoende duidelijkheid. Volgens de rechtspraak van het Hof dient bij het bepalen van de vraag of er sprake is van gezamenlijke verwerkingsverantwoordelijkheid te worden nagegaan of partijen gezamenlijk het doel en de middelen bepalen ten aanzien van de betreffende verwerking. Een antwoord op deze vraag wordt naar de mening van de AP onvoldoende beantwoord in de DPIA; het enkele feit dat een onderwijsinstelling een verwerking mogelijk maakt door het inschakelen van een derde partij onderbouwt onvoldoende de conclusie dat die onderwijsinstelling als (gezamenlijke) verwerkingsverantwoordelijke moet worden beschouwd voor die verwerkingen. Uit deze conclusie blijkt immers niet duidelijk of de onderwijsinstelling ten aanzien van bepaalde verwerkingen de doeleinden mede bepaalt. [1]

De AP komt hiermee tot de conclusie dat de onduidelijkheid over de rolverdeling dermate groot is dat:

[1] Zie ook de EDPB-Guidelines 07/2020 on the concepts of controller and processor in the GDPR: "As such, an important criterion to identify converging decisions in this context is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. The situation of joint controllers acting on the basis of converging decisions should however be distinguished from the case of a processor, since the latter – while participating in the performance of a processing – does not process the data for its own purposes but carries out the processing on behalf of the controller."

- niet kan worden bepaald wie er op dit moment voor welke verwerkingen de rol van respectievelijk verwerkingsverantwoordelijke en verwerker inneemt, of dat er sprake is van gezamenlijke verwerkingsverantwoordelijkheid;
- onvoldoende kan worden vastgesteld of de beoordeling juist is van die situaties waarin sprake zou zijn van gezamenlijke verwerkingsverantwoordelijkheid, gelet op de rechtspraak van het Hof van Justitie van de Europese Unie[2] en de (concept)richtsnoeren van de EDPB[3];
- niet kan worden vastgesteld of er een situatie bestaat waarbij een verwerker door het zelfstandig bepalen van doelen en middelen verwerkingsverantwoordelijke is en dus ook zelfstandig aan de AVG zal dienen te voldoen;
- niet kan worden vastgesteld of er sprake zou zijn van een situatie waarbij een partij verwerker is en handelt binnen de kaders van art. 28 AVG.

Ook ten aanzien van de rolverdeling tussen partijen geldt dat het in principe aan partijen zelf is om deze vast te stellen.[4]

Aandacht voor de risico's bij kinderen

De DPIA bij de adviesaanvraag van SIVON/SURF is voornamelijk gericht op de verwerking van persoonsgegevens van onderwijsmedewerkers en onderwijsdeelnemers van instellingen in het hoger onderwijs. Uit de adviesaanvraag blijkt echter dat Google G Suite for Education met name wordt ingezet door het funderend onderwijs en dat SIVON/SURF met hun adviesaanvraag niet alleen vragen heeft ten aanzien van de inzet van Google G Suite for Education door het hoger onderwijs, maar ook het primair-, voortgezet- en middelbaar beroepsonderwijs, waarbij ook kinderen betrokken zijn.

Kinderen hebben recht op een passende invulling van hun grondwettelijke recht op bescherming van persoonsgegevens en dienen te worden beschermd tegen schendingen van dat grondrecht. Een juiste borging van dat grondrecht vergt extra aandacht bij kinderen. Zij hebben volgens de AVG, het Handvest en het Verdrag inzake de rechten van het kind recht op specifieke bescherming. De AP stelt daarom voorop dat bij het inschatten van de risico's aangaande de verwerking van persoonsgegevens in voldoende mate de specifieke risico's voor kinderen moeten worden geïdentificeerd en onderzocht. Dit vergt een nauwkeurige analyse van de specifieke risico's voor kinderen en de uitwerking die deze risico's hebben op kinderen van verschillende leeftijden. Daarbij is het onvoldoende om kinderen te positioneren als betrokkenen met alleen een lagere leeftijd, aangezien kinderen zich minder bewust zijn van de betrokken risico's en gevolgen van de verwerking van hun persoonsgegevens. Daarbij kunnen risico's een andere impact en uitwerking hebben op kinderen dan op volwassenen. Het stelselmatig vastleggen van gegevens over het gedrag en de ontwikkeling van kinderen kan leiden tot risico's zoals discriminatie en uitsluiting. Bovenstaande leidt tot de conclusie dat er bij de verwerking van persoonsgegevens van kinderen extra zorgvuldig zal moeten worden onderzocht welke risico's er spelen en welke waarborgen passend zijn. De AP acht dit in de DPIA nog onvoldoende uitgewerkt.

[2] Onder meer *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551.
[3] Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
[4] Het is niet aan de AP om, zoals wordt gesuggereerd op p. 163 van de DPIA, in een procedure van de voorafgaande raadpleging op verzoek een uitspraak te doen over de juistheid van de stellingen van partijen ten aanzien van de verwerkingsverantwoordelijkheid. Ook is het niet de taak van de AP om als geschilbeslechter op te treden, noch ziet de AP deze adviesprocedure als juiste aanleiding om, zonder nader onderzoek, de AP een uitspraak te laten doen over de rolverdeling tussen partijen.

5 Advies

De AP adviseert u, en daarmee de Nederlandse onderwijsinstellingen, op basis van het bovenstaande de inzet van Google G Suite for Education niet aan te vangen dan wel voort te zetten, nu er onduidelijkheden bestaan op een aantal fundamentele vragen die dienen te worden beantwoord. De AP acht het bespreken van de andere, door SURF en SIVON geschetste risico's hier overbodig daar zonder het wegnemen van bovengenoemde cruciale risico's en onduidelijkheden de verwerking niet aan de AVG kán voldoen. De AP acht het eveneens overbodig om in te gaan op de vragen 1 tot en met 4 in uw verzoek.

Identificatie van verwerkingen, doeleinden, rolverdelingen, grondslagen en risico's bij kinderen

De AP adviseert daarom om in ieder geval de volgende zaken te identificeren bij de verdere dan wel voorgenomen inzet van Google G Suite for Education:

1. Bepalen welke verwerkingen van persoonsgegevens er plaatsvinden en de doeleinden waarvoor deze verwerkingen plaatsvinden.
   Hierbij is het van belang om ook opvolgende verwerkingen te identificeren die kunnen aanvangen door het inzetten van Google G Suite for Education voor zover deze verwerkingen nu niet (evident) bekend zijn. Daarbij dient te worden bepaald of de doeleinden vallen binnen het doelbindingsbeginsel. Daar waar twijfel bestaat over de verwerkingen door een leverancier merkt de AP op dat, mede in het licht van art. 26 AVG en art. 28 AVG, additionele zekerheid over de rechtmatige uitvoering van de verwerking van deze leverancier kan worden gevergd.
2. Welke partij(en) doel en (essentiële) middelen bepaalt/bepalen van de verwerking(en) en welke rolverdeling partijen dientengevolge innemen.
   In het licht van de geldende jurisprudentie en de feitelijke situatie moet worden vastgesteld wie er zeggenschap heeft over de doelen van de verwerking en wie er zeggenschap heeft over de (essentiële) middelen die worden ingezet voor de verwerking. De analyse kan leiden tot een situatie waarbij er sprake is van een verwerkingsverantwoordelijke en verwerker, gezamenlijke verwerkingsverantwoordelijkheid of ook een situatie waarbij er later in de keten van verwerkingen verschillende verwerkingsverantwoordelijken aan te wijzen zijn. Deze analyse kan per (keten van) verwerking(en) tot een andere conclusie leiden.
3. Bepalen van de grondslag(en) voor de voorgenomen verwerking(en);
4. Bepalen van de specifieke risico's aangaande de verwerking van persoonsgegevens van kinderen, voor zover van toepassing voor de betreffende onderwijsinstelling(en).

Aanpassen DPIA

Zodra SURF en SIVON bovenstaande zaken hebben geïdentificeerd zal de DPIA moeten worden aangepast.

Gebruik van Google G Suite for Education door onderwijsinstellingen

SURF en SIVON zijn niet zelf verwerkingsverantwoordelijke voor de inzet van Google G Suite for Education, dit zijn de onderwijsinstellingen. De AP heeft op dit moment niet vastgesteld of, en zo ja in welke mate, individuele onderwijsinstellingen de risico's voor de rechten en vrijheden van betrokkenen voorafgaande aan de inzet van Google G Suite for Education hebben geëvalueerd. Mede door de uitkomst van dit advies acht de AP de kans niet groot dat alle onderwijsinstellingen dit in voldoende mate hebben gedaan en voldoende waarborgen hebben getroffen. Derhalve dienen onderwijsinstellingen die reeds gebruik maken of voornemens zijn om gebruik te maken van Google G Suite/Workspace for Education de uitkomsten van de onderhandelingen van SIVON/SURF en de aanpassingen van de DPIA te volgen en rekening te houden met de volgende situaties.

Indien de onderhandelingen die SURF en SIVON voeren leiden tot een situatie waarbij in voldoende mate invulling wordt gegeven aan de bescherming van persoonsgegevens conform de AVG, kan de inzet van Google G Suite for Education door onderwijsinstellingen op basis van deze afspraken worden heroverwogen. Onderwijsinstellingen die onvoldoende maatregelen hebben getroffen dienen bij de inzet van Google G Suite for Education gebruik te maken van deze door SURF en SIVON gemaakte afspraken, eventuele aanvullende maatregelen treffen en vast te stellen of er bij de onderwijsinstelling mogelijk sprake is van additionele risico's ten opzichte van de DPIA. Onderwijsinstellingen dienen zelf vast te stellen of er in hun specifieke situatie sprake is van additionele risico's die in de weg staan aan het gebruik van Google G Suite for Education, zie ook hierna.

Indien blijkt dat SURF en SIVON niet tot voldoende afspraken kunnen komen waarmee de risico's inzake Google G Suite for Education worden gemitigeerd, dan dient Google G Suite for Education volledig te zijn uitgefaseerd voor de start van het schooljaar 2021/2022 door die onderwijsinstellingen die onvoldoende maatregelen hebben getroffen.

De AP plaatst de kanttekening dat het uiteindelijk aan de onderwijsinstellingen is om te borgen dat de gegevensverwerking middels Google G Suite for Education voldoet aan de AVG. Onderwijsinstellingen kunnen, zelfs als zij aansluiten op de voorwaarden van SURF en SIVON, dus niet volledig steunen op alle overwegingen in de hier uitgevoerde DPIA. Waar onderwijsinstellingen bijvoorbeeld in een andere context, of waar zij andere 'soorten' persoonsgegevens gaan verwerken, zal door deze onderwijsinstellingen moeten worden getoetst welke elementen in de hier uitgevoerde DPIA passend zijn voor de situatie waarin zij de applicaties wensen te gaan inzetten. Indien onderwijsinstellingen menen dat er voorafgaande aan de inzet van Google G Suite for Education er sprake is van resterende hoge *rest*risico's, dan zijn deze verplicht om een verzoek om voorafgaande raadpleging aan te vragen bij de AP. Indien sprake is van gezamenlijke verwerkingsverantwoordelijkheid voor deze resterende hoge restrisico's bij de geïdentificeerde verwerkingen, is het daarbij noodzakelijk dat onderwijsinstellingen samen met Google *gezamenlijk* een nieuw verzoek om voorafgaande raadpleging aanvragen.[5] Indien uit de risico-inschattingen geen hoge restrisico blijken, zijn onderwijsinstellingen niet verplicht een voorafgaande raadpleging aan te vragen.

6. Eventuele discrepantie tussen documentatie en feitelijke situatie

In het geval dat de verwerking in de praktijk wezenlijk anders is dan uit de overgelegde stukken blijkt en waarop dit advies is gebaseerd, of dat een gewijzigde/nieuwe werkwijze leidt tot een wezenlijk andere verwerking dan waarop dit advies ziet, dient u te beoordelen of u de gewijzigde respectievelijk nieuwe verwerking opnieuw dient te beoordelen ingevolge artikel 35 van de AVG.

Dit advies laat onverlet dat klachten of andere informatie over de verwerking er alsnog toe kunnen leiden dat de AP nadere inlichtingen inwint of een onderzoek start.

[5] Zie ook het advies aan de minister van Justitie en Veiligheid (z2021-03260).