AUTORITEIT
PERSOONSGEGEVENS

Advies gebruik applicatie [VERTROUWELIJK] door [een onderwijsinstelling]

1 Inleiding

Op 20 juli 2023 heeft [een onderwijsinstelling (hierna: de Onderwijsinstelling)] – ingevolge artikel 36, eerste lid, van de Algemene Verordening Gegevensbescherming (AVG) – bij de Autoriteit Persoonsgegevens (AP) een verzoek om voorafgaande raadpleging (VR) ingediend. Het verzoek betreft een verwerking van persoonsgegevens door middel van het gebruik van de applicatie [VERTROUWELIJK].

Omdat het verzoek niet aan de formele eisen van artikel 36 van de AVG voldeed, heeft de AP het VR-verzoek buiten behandeling gesteld. Ondanks dat de AP niet gehouden is tot het geven van advies op basis van artikel 36 van de AVG, heeft de AP bij uitzondering toch de keuze gemaakt om naar aanleiding van uw VR-verzoek gebruik te maken van de bevoegdheid die de AP heeft in het kader van artikel 58, derde lid, onder b, AVG en u te adviseren met betrekking tot de bescherming van persoonsgegevens in het specifieke geval dat in uw VR-verzoek beschreven is.

De AP benadrukt dat dit advies tot stand is gekomen op basis van een specifieke door [de Onderwijsinstelling] beschreven verwerking en context en gaat uit van de juistheid van de bij haar aangeleverde informatie. Voor zover andere instellingen gebruik wensen te maken van dit advies is het aan hen om te bezien of hun verwerking overeenkomt met de door [de Onderwijsinstelling] beschreven verwerking. Daarbij dienen zij zelf een beschrijving te maken van alle omstandigheden van hun eigen, specifieke geval.

2 Samenvatting advies

Allereerst zal in hoofdstuk 3 van dit advies ingaan worden op het formele verloop van de procedure. Vervolgens zal in hoofdstuk 4 de feitelijke weergave van de verwerking, zoals deze uiteen is gezet door [de Onderwijsinstelling], worden geschetst. Uit de door [de Onderwijsinstelling] aangeleverde informatie blijkt tevens dat er een aantal hoge risico's aanwezig zijn wanneer met de verwerking zou worden gestart. Deze worden, samen met de maatregelen die [de Onderwijsinstelling] heeft geïdentificeerd, uiteengezet in hoofdstuk 5.

Het advies van de AP over deze verwerking wordt gegeven in hoofdstuk 6. Dit advies beslaat een viertal onderdelen, namelijk:

a. De rolverdeling tussen [de Onderwijsinstelling] enerzijds en [VERTROUWELIJK] anderzijds.
b. De verantwoordelijkheid van [de Onderwijsinstelling] voor de naleving van bewaartermijnen door [VERTROUWELIJK].
c. Het door [de Onderwijsinstelling] omschreven hoge restrisico: de doorgifte van persoonsgegevens naar [VERTROUWELIJK].[1]
d. De toestemming die betrokkenen geven aan [de Onderwijsinstelling] voor de verwerkingen.

Het advies van de AP op deze onderdelen is samengevat als volgt:

[1] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 32.

a. De AP beveelt [de Onderwijsinstelling] aan om opnieuw te onderzoeken welke partij voor welk deel van de verwerking (gezamenlijk) verwerkingsverantwoordelijk is.
b. Voor zover [de Onderwijsinstelling] (gezamenlijk) verwerkingsverantwoordelijk is, is [de Onderwijsinstelling] ook verantwoordelijk voor de naleving van de bewaartermijnen, inclusief de naleving daarvan door [VERTROUWELIJK].
c. Doorgifte naar [VERTROUWELIJK] is niet toegestaan zonder dat daarvoor voldoende passende waarborgen zijn getroffen. Op dit moment zijn deze er volgens [de Onderwijsinstelling] niet.
d. In dit geval is met name van belang dat de toestemming vrij, specifiek en geïnformeerd is. De AP beveelt [de Onderwijsinstelling] aan om hier nogmaals goed naar te kijken.

3 Procedureverloop

De AP heeft op 28 juli 2023 het verzoek om voorafgaande raadpleging van [de Onderwijsinstelling] ontvangen.

De AP heeft bij e-mail gedateerd op 31 juli 2023 de ontvangst hiervan bevestigd.

Bij brief van 22 augustus 2023 is de termijn, zoals bedoeld in artikel 36, tweede lid, AVG, met 6 weken verlengd.

Vervolgens heeft de AP bij brief van 14 september 2023 [de Onderwijsinstelling] om aanvullende informatie verzocht.

[de Onderwijsinstelling] heeft deze informatie op 10 oktober 2023 aangeleverd.

Op basis van deze informatie heeft de AP bij brief van 19 oktober 2023 het VR-verzoek buiten behandeling gesteld, omdat het verzoek niet aan de formele vereisten uit artikel 36 AVG voldeed. In dezelfde brief heeft de AP aangekondigd, bij uitzondering, toch advies te geven over deze verwerking op grond van artikel 58, derde lid, onder b, AVG.

Met dit advies is de procedure beëindigd.

De AP heeft haar advies gebaseerd op de door [de Onderwijsinstelling] aangeleverde informatie en gaat daarbij uit van de juistheid van de door [de Onderwijsinstelling] aangeleverde informatie en documentatie.

De AP heeft geen feitenonderzoek uitgevoegd.

4 Feitelijke weergave van de verwerking

De verwerking betreft het gebruik van de applicatie [VERTROUWELIJK] door [de Onderwijsinstelling] voor marketingdoeleinden. [VERTROUWELIJK] is een applicatie die wordt ontwikkeld door een derde partij; [VERTROUWELIJK].[2] [de Onderwijsinstelling] omschrijft de verwerking als volgt (antwoord 1 – formulier verzoek voorafgaande raadpleging):

"[de Onderwijsinstelling] wil [VERTROUWELIJK] als kanaal inzetten door met inzet van betaalde en organische content potentiele studiekiezers te helpen in het maken van een goede studiekeuze. Daarnaast biedt

[2] Zie [VERTROUWELIJK].

[VERTROUWELIJK] een goede mogelijkheid om het onderwijsaanbod onder de aandacht te brengen en juist ook de beleving van andere studenten te delen. [VERTROUWELIJK]"

Dit wordt verder toegelicht in de DPIA ([Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 6):

"[De Onderwijsinstelling] is voornemens om gebruik te maken van [VERTROUWELIJK] als social mediakanaal voor marketing en communicatiedoeleinden. [VERTROUWELIJK] Aan de andere kant is [de Onderwijsinstelling] bewust van de negatieve nieuwsberichten rondom [VERTROUWELIJK]. De verantwoordelijken voor security en privacy binnen de dienst [VERTROUWELIJK] hebben een privacytoets uitgevoerd, waaruit volgde dat een Data Protection Impact Assessment (DPIA) in deze context verplicht is. Vervolgens heeft [de Onderwijsinstelling] aan [een cybersecurity-bedrijf] de opdracht gegeven om de DPIA uit te voeren op de wijze van mogelijke inzet van [VERTROUWELIJK] door [de Onderwijsinstelling]."

[de Onderwijsinstelling] wil [VERTROUWELIJK] gaan inzetten om een groter bereik onder de doelgroep te bereiken (antwoord 4 – formulier verzoek voorafgaande raadpleging). Dit wordt bereikt door de volgende sub-doelen ([Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 9):

- "Delen en beschikbaar maken van content op [VERTROUWELIJK] voor de doelgroep van [de Onderwijsinstelling] die actief is op [VERTROUWELIJK];
- Advertenties tonen aan de doelgroep van [de Onderwijsinstelling] die actief is op [VERTROUWELIJK]; […]"

Daarvoor vinden volgens [de Onderwijsinstelling] een drietal verwerkingen plaats, namelijk de creatie van de content, het gebruik van [VERTROUWELIJK] door medewerkers en het plaatsen van de content op [VERTROUWELIJK] ([Onderwijsinstelling] DPIA [VERTROUWELIJK], Tabel 2). Bij deze verwerkingen worden, aldus [de Onderwijsinstelling], enkel "gewone" – en dus geen bijzondere – persoonsgegevens verwerkt.[3]

[de Onderwijsinstelling] onderscheidt twee verschillende groepen persoonsgegevens. Enerzijds de persoonsgegevens van personen die de advertentie of content te zien krijgt (een gebruiker van [VERTROUWELIJK]) en anderzijds persoonsgegevens van medewerkers van [de Onderwijsinstelling], indien zij gebruik maken van [VERTROUWELIJK] om marketingwerkzaamheden uit te voeren. De persoonsgegevens die hierbij door [VERTROUWELIJK] zullen worden verwerkt zijn ([Onderwijsinstelling] DPIA [VERTROUWELIJK], Tabel 1):

- "Device IDs
- Device related information
- IP addresses
- Performance metrics
- Advertising impression metrics
- Segment related information
- Information associated with end-user interaction with digital properties, including advertisements displayed in connection with the Services"

[3] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 7. Persoonsgegevens van strafrechtelijke aard komen in de DPIA niet aan bod.

Daarnaast zal ook [de Onderwijsinstelling] zelf persoonsgegevens verwerken. Het gaat hierbij om de persoonsgegevens van personen die herkenbaar in beeld komen, waaronder studenten en medewerkers van [de Onderwijsinstelling], in de content die [de Onderwijsinstelling] naar [VERTROUWELIJK] wenst te uploaden. Zodra het beeldmateriaal waar deze personen op te zien zijn wordt geüpload naar [VERTROUWELIJK], zal ook [VERTROUWELIJK] deze persoonsgegevens verwerken.

Ook zal [de Onderwijsinstelling] persoonsgegevens van hen verwerken in het kader van het toestemmingsformulier ([Onderwijsinstelling] DPIA [VERTROUWELIJK], Tabel 3 & Tabel 4). Voor deze verwerkingen wordt toestemming aan betrokkenen gevraagd ([Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 22-23). Het toestemmingsformulier luidt, voor zover relevant, als volgt:

"Via verhalen (beeld en/of geluidsmateriaal) wil [de Onderwijsinstelling] laten zien dat onze studenten bezig zijn met het vorm geven van hun toekomst. In deze verhalen maken we gebruik van jouw persoonsgegevens. Wij zijn blij dat je hieraan wilt meewerken. Jij laat zien dat studeren bij [de Onderwijsinstelling] interessant en leerzaam is, dat jij begeleid en gestimuleerd wordt om je talenten te ontwikkelen. […]

Met het ondertekenen van deze 'verklaring van geen bezwaar' verklaar je dat [de Onderwijsinstelling] de gemaakte beelden en/of geluidsmateriaal rechtenvrij mag gebruiken in haar communicatie-uitingen (zie hieronder voor een specificatie)) tot uiterlijk geldig 2 jaar* na ondertekening. Na genoemde datum zet [de Onderwijsinstelling] jouw beeld- en/of geluidsmateriaal niet meer actief in. Wees je er wel van bewust dat het mogelijk is dat na deze datum dit materiaal alsnog ergens terug te vinden is op de social kanalen. Voor vragen over het gebruik tijdens de bovengenoemde twee jaar mag je altijd contact met ons opnemen via [VERTROUWELIJK].

* Na genoemde datum zet [de Onderwijsinstelling] niet meer actief jouw beeld- en/of geluidsmateriaal in. Wees bewust dat het mogelijk is dat na deze datum alsnog jouw beeld- en/of geluidsmateriaal ergens terug te vinden is op de social media kanalen.

[De Onderwijsinstelling] mag mijn beelden en/of geluidsmateriaal gebruiken op de volgende kanalen:
Eigen [kanalen], zoals websites, direct mailings, print
[VERTROUWELIJK]"

In de DPIA wordt aangegeven dat [de Onderwijsinstelling] enkel persoonsgegevens zal opslaan binnen Nederland. Zodra de gegevens naar [VERTROUWELIJK] worden geüpload, worden de persoonsgegevens in [VERTROUWELIJK] en [VERTROUWELIJK]opgeslagen. [VERTROUWELIJK].

Ten slotte geeft [de Onderwijsinstelling] aan dat zij niet voornemens is om gedetailleerde advertentieprofielen te gebruiken. Daarover zegt de DPIA het volgende ([Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 19):

"[De Onderwijsinstelling] is gezamenlijk verwerkingsverantwoordelijk met [VERTROUWELIJK] voor de doelgroepkeuzes die [de Onderwijsinstelling] maakt, omdat deze keuzes gevolgen hebben voor de wijze waarop [VERTROUWELIJK] de gebruikersprofielen inzet. Uit de DPIA-interviews is naar voren gekomen dat [de Onderwijsinstelling] enkel keuzes maakt in de leeftijd en locatiegebied van [VERTROUWELIJK] gebruikers (bijv. [VERTROUWELIJK]) omdat de doelgroep jongeren zijn uit die gebieden die een studiekeuze moeten maken. Specifieke interesses zijn voor [de Onderwijsinstelling] niet interessant, omdat het om iedereen binnen de leeftijd en binnen het gebied relevant kan zijn. Er wordt vanuit [de Onderwijsinstelling] dan ook geen keuzes gemaakt op basis van interessegebieden."

5 Hoge risico's van – en maatregelen bij – de verwerking

Uit de door [de Onderwijsinstelling] aangeleverde informatie blijkt dat [de Onderwijsinstelling] 15 risico's heeft geïdentificeerd met betrekking tot de door haar voorgenomen verwerking. Daarvan zijn vier risico's als 'hoog risico' aangemerkt.[4] Dit zijn:[5]

- **R9**: "Medewerkers verliezen controle over hun persoonsgegevens wanneer zij [VERTROUWELIJK] gebruiken voor hun marketingwerkzaamheden bij [de Onderwijsinstelling] "
- **R11**: "Medewerkers die onderdeel worden van (advertentie)content verliezen controle over hun persoonsgegevens wanneer persoonsgegevens worden verwerkt zonder rechtsgeldige toestemming"
- **R12**: "[VERTROUWELIJK]"
- **R15**: "Betrokkenen verliezen controle over persoonsgegevens omdat ze niet geïnformeerd worden en geen toestemming kunnen geven voor verdere verwerkingen door [VERTROUWELIJK], die niet in lijn zijn met de doelen van [de Onderwijsinstelling]."

[de Onderwijsinstelling] heeft in totaal vijftien maatregelen geïdentificeerd om verschillende risico's bij de verwerking weg te nemen, danwel te beperken. Van die maatregelen beperkt een drietal de hiervoor benoemde hoge risico's:

- Volgens [de Onderwijsinstelling] kan risico R9 worden beperkt door het beheer van de activiteiten op [VERTROUWELIJK] te laten uitvoeren door een derde partij, zodat medewerkers van [de Onderwijsinstelling] geen gebruik hoeven te maken van [VERTROUWELIJK].[6]
- Risico R11 kan volgens [de Onderwijsinstelling] worden beperkt door het toestemmingsformulier[7] zodanig aan te passen zodat deze voldoet aan de voorwaarden van rechtsgeldige toestemming, waarbij rekening moet worden gehouden met de mogelijke verdere verwerkingen door [VERTROUWELIJK] voor doeleinden van [VERTROUWELIJK].[8]
- Risico R15 kan, aldus [de Onderwijsinstelling], worden beperkt door betrokkenen te informeren over mogelijke verdere verwerkingen door [VERTROUWELIJK] via het toestemmingsformulier.

Geen van de maatregelen vermindert echter het risico R12, waardoor dit risico ook na doorvoering van de verschillende maatregelen door [de Onderwijsinstelling] als hoog kwalificeert.

6 Advies Autoriteit Persoonsgegevens

[de Onderwijsinstelling] heeft de AP, middels een VR-verzoek, gevraagd om advies over het gebruik van de applicatie [VERTROUWELIJK]. Alhoewel het verzoek, zoals eerder benoemd, niet voldoet aan de formele vereisten van artikel 36 van de AVG, geeft de AP, bij uitzondering, wel advies. De AP heeft ervoor gekozen gebruik te maken van haar bevoegdheid uit artikel 58 derde lid onder b AVG. Deze keuze is onder andere ingegeven door het feit dat [VERTROUWELIJK] andere onderwijsinstellingen al gebruik maken van

[4] De DPIA noemt in totaal zes hoge risico's die zouden ontstaan bij de voorgenomen verwerking. [de Onderwijsinstelling] heeft echter besloten om hoe dan ook geen gebruik te maken van [VERTROUWELIJK].
[5] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 28.
[6] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 30.
[7] De AP begrijpt: het formulier waarmee medewerkers en studenten hun toestemming kunnen geven aan [de Onderwijsinstelling] om te verschijnen in de content van [de Onderwijsinstelling].
[8] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 30.

[VERTROUWELIJK].[9] De AP wil er met dit advies dan ook zorg voor dragen dat, naast [de Onderwijsinstelling], ook andere onderwijsinstellingen bekend worden met de eisen die gelden voor het gebruik van [VERTROUWELIJK] voor marketing- en communicatiedoeleinden. Daarnaast speelt ook een rol dat het onderwerp van dit advies binnen een van de onderwerpen (big tech) valt die genoemd zijn in het Jaarplan van de AP.[10]

Een nadere onderbouwing van de AP voor de inzet van haar adviesbevoegdheid is opgenomen in bijlage 1 bij dit advies.

Voorts merkt de AP op dat hoewel zij de bevoegde toezichthouder is voor [de Onderwijsinstelling], de AP dat niet is als het gaat om [VERTROUWELIJK]. Ten aanzien van [VERTROUWELIJK] is [VERTROUWELIJK] de leidende toezichthouder.[11] Dit laatste houdt in dat het in beginsel aan [VERTROUWELIJK] is om te bepalen of [VERTROUWELIJK] haar verwerkingen rechtmatig uitvoert.

Dit advies zal achtereenvolgens ingaan op een aantal verschillende aspecten van de verwerking:

a. De rolverdeling tussen [de Onderwijsinstelling] enerzijds en [VERTROUWELIJK] anderzijds.
b. De verantwoordelijkheid van [de Onderwijsinstelling] voor de naleving van bewaartermijnen door [VERTROUWELIJK].
c. Het door [de Onderwijsinstelling] omschreven hoge restrisico: de doorgifte van persoonsgegevens naar [VERTROUWELIJK].[12]
d. De toestemming die betrokkenen geven aan [de Onderwijsinstelling] voor de verwerkingen.

6.1 Het inschakelen van derde partijen

Veel organisaties schakelen derden in om hen te ondersteunen bij de verwerking van persoonsgegevens. Of deze derde partij als (gezamenlijk) verwerkingsverantwoordelijke of verwerker moet worden aangemerkt is afhankelijk van de omstandigheden van het specifieke geval. Hierbij moet (per verwerking) een feitelijke analyse worden gemaakt. Het enkele gegeven dat er in een overeenkomst tussen partijen iemand wordt aangewezen als verwerkingsverantwoordelijke of verwerker is niet doorslaggevend.[13]

Gezamenlijke verantwoordelijkheid voor de verwerking is het gevolg van gezamenlijke deelname van twee of meer entiteiten aan de vaststelling van het doel en de middelen van een verwerking. Gezamenlijke deelname kan de vorm aannemen van een gezamenlijk besluit van twee of meer entiteiten of het resultaat zijn van convergerende besluiten van twee of meer entiteiten, wanneer de besluiten elkaar aanvullen en noodzakelijk zijn om de verwerking op zodanige wijze te laten plaatsvinden dat zij een tastbaar effect hebben op de vaststelling van het doel en de middelen van de verwerking. Daarentegen kan een natuurlijke of rechtspersoon niet worden geacht verantwoordelijk te zijn voor verwerkingen die vroeger of later in de verwerkingsketen plaatsvinden en waarvan hij niet het doel of de middelen vaststelt.[14] Een belangrijk criterium is dat de verwerking niet mogelijk zou zijn zonder de deelname van beide partijen, in die zin dat

[9] [VERTROUWELIJK].
[10] Zie https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarplan-2023.
[11] Artikel 56 AVG.
[12] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 32.
[13] EDPB Guidelines 07/2020, nr. 12.
[14] HvJ EU 29 juli 2019, C-40/17 (*Fashion-ID*), § 74.

de verwerking door elke partij onlosmakelijk met die van de andere verbonden. De gezamenlijke deelname moet de vaststelling van het doel enerzijds en de middelen anderzijds omvatten.[15]

De vraag of sprake is van gezamenlijke verwerkingsverantwoordelijkheid zal een verwerkingsverantwoordelijke partij, mogelijk in overleg met de andere partij, zelf moeten beantwoorden. Dit kan per verwerking verschillen. Om te kunnen kwalificeren als verwerkingsverantwoordelijke is het tevens niet noodzakelijk dat de partij toegang heeft tot de persoonsgegevens die worden verwerkt.[16]

Afhankelijk van de kwalificatie van de partijen die persoonsgegevens verwerken gelden er op grond van de AVG vereisten waar de partijen aan moeten voldoen. Zo moeten gezamenlijke verwerkingsverantwoordelijken afspraken maken waarin onder andere wordt bepaald hoe er wordt omgegaan met de rechten van betrokkenen.[17] Als partijen geen onderlinge afspraken hebben gemaakt betekent dat echter niet dat er geen sprake is van gezamenlijke verwerkingsverantwoordelijkheid.[18]

6.1.1 Verwerkingsverantwoordelijkheid en rolverdeling

[de Onderwijsinstelling] is in het onderhavige geval de partij die beeldmateriaal produceert en dit wenst te gebruiken voor marketing- en communicatiedoeleinden. [de Onderwijsinstelling] kiest daarbij (onder andere) voor [VERTROUWELIJK] als platform.[19] De DPIA stelt dat [de Onderwijsinstelling] zelfstandig verwerkingsverantwoordelijke is voor de content, totdat deze wordt gedeeld met [VERTROUWELIJK]. Daarna zou [VERTROUWELIJK] als enige verwerkingsverantwoordelijke zijn, aldus [de Onderwijsinstelling].[20]

De AP overweegt over de verwerkingsverantwoordelijkheid en rolverdeling het volgende.

Het begrip verwerkingsverantwoordelijke dient ruim te worden uitgelegd om zo te garanderen dat betrokkenen een doeltreffende en volledige bescherming toekomt.[21] Daarnaast moet in het achterhoofd worden gehouden dat actoren in verschillende stadia en in verschillende mate bij een verwerking betrokken kunnen zijn, zodat bij de beoordeling van het niveau van verantwoordelijkheid van ieder van hen rekening moet worden gehouden met alle relevante omstandigheden van het concrete geval.[22] Het is voor gezamenlijke verwerkingsverantwoordelijkheid dus niet vereist dat er sprake is van gelijkwaardige verantwoordelijkheid en andersom betekent gezamenlijke verwerkingsverantwoordelijkheid ook niet automatisch dat er sprake is van gelijkwaardige verantwoordelijkheid.[23]

De verwerking van persoonsgegevens wordt initieel door [de Onderwijsinstelling] in gang gezet, door het produceren van het beeldmateriaal. Vervolgens wordt dit doorgestuurd naar [VERTROUWELIJK]. Er is

[15] EDPB Guidelines 05/2021, p. 3-4.
[16] HvJ EU 5 juni 2018, C-210/16 (*Wirtschaftsakademie*), § 38.
[17] Artikel 26, eerste lid, AVG.
[18] HvJ EU 5 december 2023, C-683/21 (*Nacionalinis visuomenės sveikatos centras*), § 45.
[19] De AP merkt op dat uit de aangeleverde informatie niet blijkt dat [de Onderwijsinstelling] inzicht krijgt in – al dan niet geanonomimiseerde – statistieken over personen die de pagina van [de Onderwijsinstelling] op [VERTROUWELIJK] bezoeken, zie HvJ EU 5 juni 2018, C-210/16 (*Wirtschaftsakademie*), § 15. De AP gaat er in haar advies dan ook van uit dat dit niet het geval is.
[20] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 10.
[21] HvJ EU 29 juli 2019, C-40/17 (*Fashion-ID*), § 66.
[22] HvJ EU 29 juli 2019, C-40/17 (*Fashion-ID*), § 70.
[23] HvJ EU 5 juni 2018, C-210/16 (*Wirtschaftsakademie*), § 43.

daarom sprake van een beslissende invloed van [de Onderwijsinstelling] op het begin van de keten van gegevensverwerkingen die plaatsvindt door [de Onderwijsinstelling] en vervolgens [VERTROUWELIJK].[24]

[de Onderwijsinstelling] stelt dat zowel [de Onderwijsinstelling] als [VERTROUWELIJK] economische belangen hebben bij de verwerkingen.[25] Via [VERTROUWELIJK] hoopt [de Onderwijsinstelling] een jonge doelgroep[26] te bereiken die mogelijk, onder andere naar aanleiding van de content van [de Onderwijsinstelling], besluit om student te worden bij [de Onderwijsinstelling].[27] Volgens [de Onderwijsinstelling] heeft [VERTROUWELIJK] daarnaast ook, als advertentieplatform, eigen commerciële belangen.[28] Verwerkingen die in dit kader plaatsvinden zullen zowel worden verricht in het economische belang van [de Onderwijsinstelling] als in dat van [VERTROUWELIJK].[29] Voor de vaststelling van (gezamenlijke) verwerkingsverantwoordelijkheid is van belang dat deze belangen nauw met elkaar verbonden zijn of elkaar complementeren.[30]

Door het gebruik van [VERTROUWELIJK] lijkt [de Onderwijsinstelling], al dan niet impliciet, in te stemmen met de verdere verwerkingen die [VERTROUWELIJK] vervolgens zal uitvoeren voor haar eigen doelen.[31] Als deze verwerkingen ook plaatsvinden voor de doelen van [de Onderwijsinstelling], kan er bovendien sprake zijn van een gezamenlijk doel. De doelen van [VERTROUWELIJK] en [de Onderwijsinstelling] moeten elkaar dan wel onderling aanvullen, en moeten ook door [VERTROUWELIJK] en [de Onderwijsinstelling] gezamenlijk zijn vastgesteld. Dat zou betekenen dat er sprake is van gezamenlijke verwerkingsverantwoordelijkheid. Dit is anders indien er sprake is van een verwerking die niet plaatsvindt voor de gezamenlijke doeleinden van de betrokken partijen. Indien [VERTROUWELIJK] het beeldmateriaal verder verwerkt voor andere doelen dan de gezamenlijke doelen, is dus sprake van een verwerking voor eigen doeleinden van [VERTROUWELIJK] waarvoor [de Onderwijsinstelling] niet als verwerkingsverantwoordelijke kan worden aangemerkt.

Uit de DPIA blijkt dat [de Onderwijsinstelling] tot de conclusie komt dat [de Onderwijsinstelling] slechts verwerkingsverantwoordelijke is tot het moment dat het beeldmateriaal naar [VERTROUWELIJK] is geüpload.[32] Gelet op het bovenstaande is dit zonder nadere onderbouwing, welke in de DPIA ontbreekt, niet aannemelijk voor zover het gaat om verwerkingen die plaatsvinden voor de doelen van [VERTROUWELIJK] én [de Onderwijsinstelling].[33] Dit dient (per individuele verwerking) door [de Onderwijsinstelling] aanvullend te worden onderzocht, waarbij het bovenstaande in acht moet worden genomen.

[24] HvJ EU 29 juli 2019, C-40/17 (*Fashion ID*), § 78.
[25] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 13.
[26] Ten overvloede geeft de AP mee dat, wanneer de digitaledienstenverordening (DSA) van toepassing is, het niet is toegestaan om advertenties te tonen aan gebruikers die minderjarig zijn, wanneer het tonen van deze advertenties gebeurt aan de hand van profilering, zoals bedoeld in artikel 4, onder 4 AVG.
[27] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 13.
[28] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 14.
[29] HvJ EU 29 juli 2019, C-40/17 (*Fashion ID*), § 80.
[30] Zie A-G conclusie bij HvJ EU 29 juli 2019, C-40/17 (*Fashion ID*), nr. 105.
[31] Zie HvJ EU 29 juli 2019, C-40/17 (*Fashion ID*), § 80.
[32] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 10.
[33] HvJ EU 29 juli 2019, C-40/17 (*Fashion ID*), § 80.

Ten overvloede merkt de AP op dat zelfs als [de Onderwijsinstelling] na het uploaden geen toegang meer zou hebben tot de persoonsgegevens, dit niet automatisch betekent dat [de Onderwijsinstelling] geen verwerkingsverantwoordelijke meer is.[34]

Indien [de Onderwijsinstelling] kan worden aangemerkt als (gezamenlijk) verwerkingsverantwoordelijke, benadrukt de AP dat [de Onderwijsinstelling] op grond van artikel 5, tweede lid, AVG en artikel 24, eerste lid, AVG, (mede) verantwoordelijk is voor de naleving van de AVG en de naleving moet kunnen aantonen.[35] Als er sprake is van gezamenlijke verwerkingsverantwoordelijkheid is het daarnaast van belang dat de partijen onderlinge afspraken maken over wie verantwoordelijk is voor de naleving van de verschillende AVG-verplichtingen, waaronder met name de uitoefening van de rechten van betrokkenen, waaronder in ieder geval de wijze waarop zij informatie aan betrokkenen verstrekken. Deze regeling moet op transparante wijze worden gecommuniceerd aan betrokkenen, in het onderhavige geval bijvoorbeeld wanneer aan betrokkenen om toestemming wordt gevraagd.[36]

Ten slotte: het is aan [de Onderwijsinstelling] om te bepalen of de opvolgende verwerkingen, waarvoor [VERTROUWELIJK] andere doelen heeft dan die waarvoor [de Onderwijsinstelling] verwerkingsverantwoordelijke is, voor [de Onderwijsinstelling] maatschappelijk gewenst zijn. Verwerkingen die strikt genomen binnen het kader van de AVG mogen plaatsvinden kunnen vanuit het beoordelingskader van [de Onderwijsinstelling] mogelijk bezien vanuit die bril niet passend zijn.

6.1.2 Naleving bewaartermijnen derde partijen

[de Onderwijsinstelling] heeft in haar antwoorden aan de AP aangegeven dat zij zich afvraagt of de naleving van de bewaartermijnen door [VERTROUWELIJK] (ook) haar verantwoordelijkheid is.[37] De AP gaat er in dit geval van uit dat de vastgestelde bewaartermijnen een (juiste) invulling zijn van het beginsel opslagbeperking, zoals bedoeld in artikel 5, eerste lid onder e, AVG, maar heeft dit niet zelf onderzocht.

Gelet op hetgeen hiervoor is overwogen zou er sprake kunnen zijn van gezamenlijke verwerkingsverantwoordelijkheid voor de verwerkingen die [VERTROUWELIJK] uitvoert voor de gezamenlijke doelen van [VERTROUWELIJK] en [de Onderwijsinstelling].

Voor zover dat het geval is, stelt de AP dat het ook de verantwoordelijkheid van [de Onderwijsinstelling] is, als verwerkingsverantwoordelijke, om ervoor te zorgen dat er bewaartermijnen voor de te verwerken persoonsgegevens worden vastgesteld en door derde partijen worden nageleefd.[38] De AP adviseert [de Onderwijsinstelling] daarom om de bewaartermijnen en de naleving daarvan contractueel te borgen en op de naleving hiervan toe te zien.

Mocht er voorafgaand aan het contracteren van een derde partij nog twijfel bestaan over de borging van bewaartermijnen, dan kan dit problematisch zijn in het licht van artikel 5, tweede lid, AVG en artikel 24,

[34] HvJ EU 5 juni 2018, C-210/16 (*Wirtschaftsakademie*), § 38.
[35] Zie bijvoorbeeld Rb. Amsterdam 18 oktober 2023, ECLI:NL:RBAMS:2023:6530 (*Criteo*), r.o. 4.17.
[36] Artikel 26 AVG.
[37] Antwoord op vraag 9 – aanvullende vragen AP.
[38] Zie artikel 5, eerste lid onder e, AVG. Het is, aldus artikel 5, tweede lid, AVG de verantwoordelijkheid van de verwerkingsverantwoordelijke om deze verplichting na te leven. Verder blijkt uit artikel 82, tweede jo. vierde lid, AVG dat elke verwerkingsverantwoordelijke die bij de verwerking betrokken is aansprakelijk kan worden gehouden voor de schade.

eerste lid, AVG.[39] Alle verwerkingsverantwoordelijken zijn immers verantwoordelijk voor de naleving van de AVG en moeten dit kunnen aantonen.[40] Hiervoor is het overigens niet voldoende om pas in beweging te komen nadat een verwerkingsverantwoordelijke door een betrokkene op de hoogte is gesteld van een (mogelijke) schending van de AVG door een andere verwerkingsverantwoordelijke. Overeenstemming met de AVG dient vooraf te worden gewaarborgd door iedere verwerkingsverantwoordelijke.[41]

Samenvattend is [de Onderwijsinstelling] dus (ook) verantwoordelijk voor het op juiste wijze hanteren van de bewaartermijnen door [VERTROUWELIJK] voor zover er sprake is van een gezamenlijke verwerkingsverantwoordelijkheid.

6.2 Doorgifte naar derde landen

Persoonsgegevens moeten in beginsel binnen de Europese Economische Ruimte (EER) worden verwerkt. Als een verwerkingsverantwoordelijke toch besluit om persoonsgegevens buiten de EER te verwerken, zal hij er zorg voor moeten dragen dat deze persoonsgegevens goed beschermd blijven, ongeacht of hij zelf de persoonsgegevens verwerkt of dat dit plaatsvindt bij een andere partij. De AVG kent daarom aanvullende voorwaarden toe aan de doorgifte van persoonsgegevens naar landen buiten de EER, oftewel derde landen. Onverminderd de overige bepalingen uit de AVG mogen persoonsgegevens slechts worden doorgegeven indien er voldaan wordt aan de voorwaarden die in hoofdstuk V van de AVG zijn bepaald.[42] Daaruit volgt dat doorgifte naar derde landen alleen mag als de persoonsgegevens in dit derde land een beschermingsniveau genieten dat in grote lijnen overeenkomt met het binnen de EU gewaarborgde beschermingsniveau.[43]

De AVG geeft in dit hoofdstuk een (limitatief) aantal situaties waarin doorgifte naar een derde land op grond hiervan is toegestaan. In beginsel mag een internationale doorgifte van persoonsgegevens volgens de genoemde voorwaarden alleen plaatsvinden naar landen waarvoor een adequaatheidsbesluit geldt.[44] Als er geen adequaatheidsbesluit geldt voor een doorgifte, is er nog een aantal andere situaties waarin de internationale doorgifte wel zou zijn toegestaan. Een internationale doorgifte is dan bijvoorbeeld mogelijk als er standaardcontractbepalingen (Standard Contractual Clauses, hierna: SCC's) aanwezig zijn die voldoende garanties bieden met betrekking tot de bescherming van de door te geven persoonsgegevens.[45] De op dit moment vastgestelde SCC's zijn te vinden op de website van de Europese Commissie.[46]

Het enkele feit dat er tussen de partijen SCC's worden overeengekomen, betekent echter niet dat elke doorgifte van persoonsgegevens naar het derde land is toegestaan. Zoals is opgenomen in overweging 19 van de SCC's mogen de SCC's niet worden gebruikt indien de wetten en praktijken van het derde land van bestemming (van de persoonsgegevens) de gegevensimporteur beletten om aan de bepalingen van de

[39] Voor zover het gaat om een derde partij die wordt ingeschakeld aan een verwerker, zoals bedoeld in artikel 4, onder 8, AVG, is dit tevens problematisch op grond van artikel 28, eerste lid, AVG.
[40] Artikel 24, eerste lid, AVG. Zie ook Rb. Amsterdam 18 oktober 2023, ECLI:NL:RBAMS:2023:6530 (*Criteo*), r.o. 4.16.
[41] Rb. Amsterdam 18 oktober 2023, ECLI:NL:RBAMS:2023:6530 (*Criteo*), r.o. 4.19.
[42] In de onderhavige casus zijn met name de artikelen 45, eerste lid, AVG en 46, eerste en tweede lid onder c, AVG van belang. De AP beperkt zich dan ook bij de bespreking van dit risico tot deze artikelen.
[43] HvJ EU 16 juli 2020, C-311/18 (*Schrems II*), § 96.
[44] Artikel 45 AVG.
[45] Artikel 46, tweede lid onder c, AVG.
[46] Zie https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:32021D0914.

SCC's te voldoen.[47] De SCC's vereisen daarom dat de partijen garanderen dat er voor hen geen reden is om aan te nemen dat de wetten en praktijken die op de gegevensimporteur van toepassing zijn hier niet aan voldoen.[48] Dit alles blijkt ook uit rechtspraak van het Hof van Justitie.[49] Om hier een goed beeld van te krijgen kan het voor de verwerkingsverantwoordelijke noodzakelijk zijn om een Data Transfer Impact Assessment (DTIA) uit te voeren.[50] Een DTIA zal periodiek moeten worden herhaald.[51]

Als er geen sprake is van een (geldig) adequaatheidsbesluit, noch van SCC's die voldoen aan de vereisten, dan kan de doorgifte niet plaatsvinden. Doorgifte van persoonsgegevens naar derde landen is in die gevallen in strijd met de AVG en dus onrechtmatig.

Ten overvloede merkt de AP op dat er ook sprake is van een doorgifte naar een derde land indien er vanuit dat derde land toegang tot persoonsgegevens die binnen de EU zijn opgeslagen wordt verkregen, bijvoorbeeld wanneer er persoonsgegevens door of namens een overheid van een derde land worden geraadpleegd.[52] In die gevallen moet dus ook worden voldaan aan de voorwaarden van Hoofdstuk V van de AVG.[53]

6.2.1. Toepassing in onderhavige casus

[de Onderwijsinstelling] heeft in haar DPIA beoordeeld of doorgifte naar [VERTROUWELIJK] volgens haar toegestaan is.[54] De conclusie hiervan is negatief, [VERTROUWELIJK].[55]

[VERTROUWELIJK].[56]

Omdat de AP geen onderzoek naar de doorgifte in deze specifieke situatie heeft gedaan, wenst zij nogmaals te benadrukken dat zij zich in dit advies enkel heeft gebaseerd op de informatie die [de Onderwijsinstelling] heeft aangeleverd. Het is in eerste instantie de verantwoordelijkheid van een verwerkingsverantwoordelijke om te beoordelen of er al dan niet voldaan is aan de eisen die de AVG stelt aan doorgifte van persoonsgegevens naar derde landen.[57]

Ten overvloede merkt de AP op dat de DPIA met name in gaat op de doorgifte van persoonsgegevens naar [VERTROUWELIJK], maar niet (uitgebreid) op doorgifte van persoonsgegevens naar [VERTROUWELIJK] en [VERTROUWELIJK]. De AP beveelt aan dat [de Onderwijsinstelling], alvorens er wordt gestart met deze doorgifte, beoordeelt of deze doorgifte rechtmatig kan plaatsvinden, gelet op de vereisten die Hoofdstuk V van de AVG stelt. [VERTROUWELIJK].

[47] SCC's binden overheden van derde landen immers niet, zie HvJ EU 16 juli 2020, C-311/18 (*Schrems II*), § 125.
[48] Overweging 19 SCC's en Clause 14 SCC's.
[49] HvJ EU 16 juli 2020, C-311/18 (*Scherms II*), § 105.
[50] Zie EDPB Recommendations 01/2020, nr. 28 e.v.
[51] EDPB Recommendations 01/2020, nr. 67.
[52] EDPB Guidelines 05/2021, nr. 16.
[53] Zie bijvoorbeeld EDPB Recommendations 01/2020, nr. 105-117.
[54] [VERTROUWELIJK].
[55] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 15-17.
[56] [VERTROUWELIJK].
[57] HvJ EU 16 juli 2020, C-311/18 (*Scherms II*), § 134-135.

6.3 Grondslag voor de verwerking

Ten slotte wenst de AP nog in te gaan op de grondslag voor de verwerking van persoonsgegevens. Uit de door [de Onderwijsinstelling] aangeleverde informatie blijkt dat voor alle verwerkingen een beroep wordt gedaan op toestemming.[58] Deze toestemming wordt verkregen middels een daarvoor ontworpen toestemmingsformulier.[59]

Om toestemming als grondslag voor de verwerking te kunnen gebruiken, zoals bedoeld in artikel 6, eerste lid onder a, AVG, moet er voldaan zijn aan een aantal vereisten. Zo moet de toestemming vrij, specifiek, geïnformeerd en ondubbelzinnig zijn.[60] Voldoet de toestemming niet aan een (of meerdere) van deze vereisten? Dan is de toestemming ongeldig.

De AP zal hierna kort ingaan op de eisen die gelden voor toestemming, waarna zij mogelijke knelpunten schetst voor toestemming in het geval van [de Onderwijsinstelling].

6.3.1. Vrije toestemming

Het element "vrij" impliceert werkelijke keuze en controle voor de betrokkenen. Als algemene regel schrijft de AVG voor dat als een betrokkene geen werkelijke keuze heeft, zich gedwongen voelt om toestemming te geven of het voor hem negatieve gevolgen zal hebben als hij niet toestemt, de toestemming niet geldig is.[61] Dit geldt des te meer indien er sprake is van twee ongelijke partijen, zoals een werkgever en werknemer of een school en een student. In die gevallen is de betrokkene immers afhankelijk van de partij die om toestemming voor de verwerking vraagt.[62]

Een dienst kan meerdere verwerkingsactiviteiten voor meerdere doeleinden omvatten. In dergelijke gevallen zouden de betrokkenen vrij moeten kunnen kiezen welk doeleinde zij accepteren, in plaats van toestemming te moeten verlenen voor een pakket verwerkingsdoeleinden. Zo kan het volgens de AVG nodig zijn om voor meerdere zaken toestemming te verkrijgen voordat met het aanbieden van een dienst kan worden begonnen.[63] De toestemming wordt geacht niet vrijelijk te zijn verleend indien geen afzonderlijke toestemming kan worden gegeven voor verschillende persoonsgegevensverwerkingen ondanks het feit dat dit in het individuele geval passend is.[64]

6.3.2. Specifieke toestemming

De eis dat de toestemming "specifiek" moet zijn, beoogt te zorgen voor een zekere mate van controle door en transparantie voor de betrokkene. Deze eis is nauw verbonden aan de eis van "geïnformeerde" toestemming. Tegelijkertijd moet dit worden geïnterpreteerd in overeenstemming met de eis van granulariteit om "vrije" toestemming te verkrijgen. Kortom, wil de toestemming "specifiek" zijn, dan moet de verwerkingsverantwoordelijke zorgen voor: [65]

I. specificatie van doeleinden als een bescherming tegen "function creep",
II. granulariteit in toestemmingsverzoeken, en

[58] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 22-23.
[59] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 23.
[60] Artikel 4 onder 11 AVG.
[61] EDPB Guidelines 05/2020, nr. 13.
[62] Zie overweging 43 AVG.
[63] EDPB Guidelines 05/2020, nr. 42.
[64] Overweging 43 AVG.
[65] EDPB Guidelines 05/2020, nr. 55.

III. een duidelijk onderscheid tussen informatie over het verkrijgen van toestemming voor verwerkingsactiviteiten en informatie over andere zaken.

6.3.3. Geïnformeerde toestemming

Op basis van artikel 5 van de AVG is de eis van transparantie een van de fundamentele beginselen en nauw verwant aan de beginselen van behoorlijkheid en rechtmatigheid. Het verstrekken van informatie aan de betrokkenen voorafgaand aan het verkrijgen van hun toestemming is noodzakelijk om hen in staat te stellen geïnformeerde beslissingen te nemen, te begrijpen waarmee ze instemmen en bijvoorbeeld hun recht tot intrekking van hun toestemming uit te oefenen. Indien de verwerkingsverantwoordelijke geen toegankelijke informatie verstrekt, wordt de controle van de betrokkene slechts schijn en is toestemming een ongeldige grond voor verwerking.[66]

Om er voor te zorgen dat een betrokkene geïnformeerde toestemming kan geven is het ten minste nodig om de betrokkene de volgende informatie (voorafgaand aan de toestemming) te verstrekken:[67]

I. de identiteit van de verwerkingsverantwoordelijke,
II. het doel van de verwerking,
III. welke soort persoonsgegevens worden verwerkt,
IV. het feit dat een betrokkene diens toestemming kan intrekken,
V. informatie over de risico's van doorgifte naar derde landen, en
VI. indien van toepassing: informatie over het bestaan en gebruik van geautomatiseerde besluitvorming.[68]

De AP merkt op dat indien meerdere gezamenlijke verwerkingsverantwoordelijken zich op de gevraagde toestemming willen baseren of als de gegevens zullen worden doorgegeven aan – of verwerkt door – andere verwerkingsverantwoordelijken en die zich op de oorspronkelijke toestemming willen baseren, al deze organisaties moeten worden genoemd. Hetzelfde geldt voor alle doelen waarvoor men toestemming wenst te vragen, waarbij rekening moet worden gehouden met de overige eisen voor geldige toestemming, zoals dat toestemming vrij en specifiek moet zijn.[69]

Afhankelijk van de specifieke omstandigheden van het geval kan het daarnaast noodzakelijk zijn dat meer informatie nodig is om de betrokkene in staat te stellen de betreffende verwerkingsactiviteiten goed te begrijpen.[70]

Gelet op het feit dat de verwerkingsverantwoordelijke de betrokkene moet informeren over de verwerking, is het noodzakelijk dat ook de verwerkingsverantwoordelijke zelf goed begrijpt welke verwerkingen er precies plaatsvinden. Dit geldt ook als deze verwerkingen plaatsvinden bij een derde partij waarvoor hij nog (gezamenlijk) verwerkingsverantwoordelijke voor is.

[66] EDPB Guidelines 05/2020, nr. 62.
[67] Dit staat los van informatie die eventueel op grond van artikel 13 AVG of artikel 14 AVG moet worden verstrekt aan een betrokkene.
[68] EDPB Guidelines 05/2020, nr. 64.
[69] EDPB Guidelines 05/2020, nr. 65.
[70] EDPB Guidelines 05/2020, nr. 65.

6.3.4. Ondubbelzinnige wilsuiting

Als laatste is voor geldige toestemming van belang dat er sprake is van een ondubbelzinnige wilsuiting van de betrokkene. Aan deze voorwaarde kan enkel zijn voldaan wanneer de betrokkene met een actieve gedraging duidelijk blijk geeft van zijn toestemming.[71] Stilzwijgen of inactiviteit van de betrokkene kan dus nooit voldoen aan de eisen van geldige toestemming.[72] Hetzelfde geldt voor standaard aangevinkte selectievakjes.[73]

In samenhang met het vereiste dat toestemming specifiek moet zijn is ook vereist dat de handeling waarmee toestemming wordt verleend duidelijk kan worden onderscheiden van andere handelingen, zoals het instemmen met een overeenkomst.[74]

6.3.5. Toepassing in onderhavige casus

Zoals gezegd vraagt [de Onderwijsinstelling] toestemming aan betrokkenen. Uit de aangeleverde documentatie blijkt niet dat er een andere grondslag van toepassing is voor de verwerking.

[de Onderwijsinstelling] geeft in haar documentatie aan dat er mogelijk ook andere verwerkingen plaatsvinden dan die waarvoor zij toestemming vraagt. Zo is in de DPIA te lezen dat, door het uploaden van het beeldmateriaal en akkoord te gaan met [VERTROUWELIJK]'s voorwaarden, [de Onderwijsinstelling] [VERTROUWELIJK] toestaat om het beeldmateriaal te gebruiken om de diensten van [VERTROUWELIJK] te ontwikkelen, te onderzoeken, aan te bieden, te promoten en te verbeteren.[75] Los van de vraag wie er verantwoordelijk is voor deze verwerkingen, merkt de AP op dat betrokkenen geen toestemming geven voor deze verwerkingen voor deze doeleinden en dat daarmee een grondslag voor de verwerking lijkt te ontbreken. Het is dan ook aan de verwerkingsverantwoordelijke van die verwerking, ongeacht of dit [VERTROUWELIJK], [de Onderwijsinstelling] of beiden is, om er zorg voor te dragen dat er wel sprake is van (geldige) toestemming.

Voor zover de verwerkingen die plaatsvinden wel onder de toestemmingsvraag vallen geldt het volgende.

Gelet op het feit dat de toestemming wordt gevraagd aan medewerkers en studenten van [de Onderwijsinstelling], is het extra van belang dat er geen negatieve gevolgen zijn verbonden aan het weigeren van de toestemming én dat medewerkers en studenten hier op worden gewezen. [de Onderwijsinstelling] erkent dit risico ook en heeft hiervoor mitigerende maatregelen opgesteld.[76]

Ook moet het voor betrokkenen mogelijk zijn om wel toestemming te geven voor bepaalde doelen, zoals verwerkingen voor promotiedoeleinden van [de Onderwijsinstelling], maar hierbij niet automatisch toestemming te geven voor andere verwerkingen, bijvoorbeeld eventuele opvolgende verwerkingen die [VERTROUWELIJK] voor eigen doeleinden zou laten plaatsvinden. Ook moeten de doelen vooraf voldoende gespecificeerd zijn, om te voorkomen dat er twijfel kan bestaan over de vraag voor welke verwerkingen een betrokkene precies toestemming heeft gegeven. Hierbij moet men in het achterhoofd

[71] HvJ EU 1 oktober 2019, C-673/17 (*Planet 49*), § 54.
[72] EDPB Guidelines 05/2020, nr. 79.
[73] HvJ EU 1 oktober 2019, C-673/17 (*Planet 49*), § 57
[74] EDPB Guidelines 05/2020, nr. 84.
[75] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 24.
[76] [Onderwijsinstelling] DPIA [VERTROUWELIJK], p. 28 en p. 30.

houden dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verwerkt en dat een niet-verenigbare, verdere verwerking (zonder nieuwe grondslag) onrechtmatig is.[77] Afhankelijk van de specifieke omstandigheden van het geval, welke de AP in het kader van deze adviesaanvraag niet nader heeft onderzocht, zou het zo kunnen zijn dat door een mogelijke combinatie van deze toestemmingsvraag er geen sprake meer is van vrije en specifieke (en dus geldige) toestemming, zoals bedoeld in de AVG, voor de verwerkingen die onder de verantwoordelijkheid van [de Onderwijsinstelling] vallen.

Verder is van belang dat toestemming geïnformeerd is. Hiervoor is het van belang dat betrokkene goed geïnformeerd worden over de risico's die aan een specifieke verwerking verbonden zijn. Om betrokkenen op een juiste wijze deze risico's te kunnen mededelen, kan het noodzakelijk zijn voor de verwerkingsverantwoordelijke om een volledig beeld te krijgen van de verwerking, om zo de risico's te kunnen beschrijven.

Ten slotte blijkt uit de documentatie die [de Onderwijsinstelling] heeft aangeleverd dat betrokkenen zelf kunnen aangeven via welke kanalen hun persoonsgegevens worden verwerkt. Daarvoor dienen de betrokkenen zelf de desbetreffende selectievakjes aan te kruisen. Daarmee wordt voldaan aan het vereiste dat er sprake moet zijn van een ondubbelzinnige wilsuiting.

Al met al beveelt de AP [de Onderwijsinstelling] aan om er zorg voor te dragen dat de toestemming die zij vraagt aan betrokkenen voldoet aan de eisen van de AVG. Gelet op de aangeleverde documentatie is het hierbij met name van belang om extra te letten op de vraag of de toestemming wel vrij, specifiek en geïnformeerd is.

7 Samenvattend advies

Gelet op het bovenstaande adviseert de AP u niet te starten met de verwerking dan nadat met het voorgaande rekening is gehouden en u na aanpassingen heeft kunnen vaststellen dat er in voldoende mate maatregelen zijn genomen om de risico's te mitigeren.

8 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 en eventueel op grond van artikel 36, eerste lid van de AVG opnieuw dient te verzoeken om voorafgaande raadpleging.

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.

[77] Zie artikel 5, eerste lid onder b, AVG en artikel 6, vierde lid, AVG.

9 Bijlage 1- Motivatie voor het in behandeling nemen van uw verzoek

Deze bijlage bevat de motivatie van de AP bij het in behandeling nemen van uw verzoek. Deze motivatie bevat geen advies of oordeel van de AP over de verwerking.

9.1 Rol AP en scope

Uw verzoek ziet op artikel 58 derde lid onder b AVG. Dat artikel geeft de AP: "alle autorisatie- en adviesbevoegdheden om:

…

b) op eigen initiatief dan wel op verzoek, aan het nationaal parlement, aan de regering van de lidstaat, of overeenkomstig het lidstatelijke recht aan andere instellingen en organen alsmede aan het publiek advies te verstrekken over aangelegenheden die verband houden met de bescherming van persoonsgegevens".

Nu de AP wel de bevoegdheid, maar niet zoals ex artikel 36 lid 2 AVG de plicht, heeft een advies te verstrekken over aangelegenheden die verband houden met de bescherming van persoonsgegevens overweegt zij het volgende.

9.2 Uitstralend effect van dit advies

Hoewel de AP het verzoek heeft ontvangen van [de Onderwijsinstelling], is het de AP ambtshalve bekend dat er ook door andere onderwijsinstellingen in Nederland gebruik wordt gemaakt van [VERTROUWELIJK]. In zoverre overweegt de AP dat er een breder effect zal uitgaan van een advies van de AP inzake de inzet van [VERTROUWELIJK].

9.3 Positie van kinderen

De AP merkt op dat er in de keten van verwerkingen sprake kan zijn van het verwerken van persoonsgegevens van kinderen. Wellicht niet nu bij [de Onderwijsinstelling] maar mogelijk wel bij andere onderwijsinstellingen. De AP is van oordeel dat dit extra zorgvuldigheid vergt bij de afweging om een verwerking al dan niet uit te voeren.

9.4 Positie van werknemers

De inzet van [VERTROUWELIJK] leidt tot verwerkingen van medewerkers van [de Onderwijsinstelling]. Aangezien er bij deze verwerkingen een machtsverhouding bestaat, van werkgever ten opzichte van medewerkers, vergt dit een extra zorgvuldige omgang met deze persoonsgegevens.

9.5 Jaarplan AP

Zoals in het AP Jaarplan 2023: "Toezichthouden in een digitaliserende samenleving" is beschreven: "legt de AP extra nadruk op een juiste omgang met persoonsgegevens door bigtechbedrijven, in samenwerking met toezichthouders in andere landen." De AP heeft overwogen of uw verzoek ook in dat kader past.[78]

9.6 Doorgifte

Daarnaast geldt dat er door de inzet van [VERTROUWELIJK] sprake zal zijn van internationale doorgifte. Bijvoorbeeld in het kader van artikel 28 lid 3 onder a AVG dient dit goed te worden geborgd.

9.7 Inwilliging van uw verzoek

Dit alles overwegende heeft de AP besloten in te gaan op uw verzoek om een advies te geven. U vindt het advies van de AP eerder in dit document.

[78] https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarplan-2023