STICHTING H3O
opvang en onderwijs

Postbus 151
3300 AD Dordrecht
Kolfstraat 120
T 078 890 50 00
secretariaat@H3O.nl
www.H3O.nl
NL33ABNA 0495584606
KvK S41120110

Onderwerp:	actualisatie procedure software en applicaties verwerking persoonsgegevens
Auteur:	M. van Heumen
Bestemd voor:	College van Bestuur
Aanleiding notitie:	standaard modelcontract EC (27 juni 2021)
Beoogd resultaat:	positief besluit
Voorgenomen bestuursbesluit:	geen
Inspraakorgaan:	geen

Definitief bestuursbesluit:	
Datum:	12-10-2021
Handtekening:	
Publicatie:	Afas Insite (alle medewerkers) Via e-mail naar alle directeuren
Evaluatie:	n.v.t.

STICHTING H3O
opvang en onderwijs

Adviesnotitie

Voor: College van Bestuur
Van: Marcel van Heumen
Onderwerp: actualisatie procedure software en applicaties verwerking persoonsgegevens
Datum: 30 september 2021

Inleiding
Onze FG heeft half september de notitie 'standaard modelcontract en aanvullende maatregelen' gepubliceerd. In deze notitie schetst zij de ontwikkelingen na het ontbinden van het Privacy Shield (werd ingezet voor de verwerking van persoonsgegevens in 'een derde land' zoals bijv. de USA).
Naar aanleiding van deze notitie is een actualisatie en interne publicatie van onze procedure omtrent verwerking persoonsgegevens noodzakelijk.

Stand van zaken
De notitie maakt duidelijk dat de Europese Commissie vanaf 27 juni 2021 duidelijkheid heeft gegeven over de verwerkingen in 'een derde land'. Naar aanleiding van dit besluit stelt Van Heumen voor om de huidige procedure voor het voorgenomen gebruik van software, applicaties (waarbij ook inbegrepen apps voor tablets) te actualiseren op basis van het onderstaande:

- De school maakt vooraf melding van het voorgenomen gebruik via privacy@h3o.nl
- Vindt de verwerking plaats binnen de EER?
    - Ja, in dat geval is de model verwerkersovereenkomst voortkomende uit het privacy convenant noodzakelijk om het gebruik mogelijk te maken.
    - Onderzoek naar de privacyrisico's van de verwerking ('de DPIA').
- Vindt de verwerking buiten de EER plaats?
    - Ja, onderzoek moet worden opgestart:
        - Valt het land waar de verwerking plaatsvindt onder het adequaatheidsbesluit[1]?
            - Ja? Dan is de Engelstalige versie van de model verwerkersovereenkomst noodzakelijk om het gebruik mogelijk te maken. Onderzoek naar de privacyrisico's van de verwerking.
            - Nee? Dan moet H3O vooraf aanvullende maatregelen toetsen o.a. betreffende encryptie en pseudonimisering. Na dit onderzoek moet het modelcontract (vastgelegd door de EC) door de aanbieder worden ondertekend.
                - Een dergelijk onderzoek wordt als onrealistisch en niet haalbaar gezien.

[1] *In het adequaatheidsbesluit heeft de EC geconcludeerd dat deze landen een vergelijkbaar passend beschermingsniveau voor persoonsgegevens hanteren. De landen zijn: Andorra, Argentinië, Canada (alleen commerciële organisaties), Faeröer Eilanden, Guernsey, Isle of Man, Israël, Japan, Jersey, Nieuw-Zeeland, Uruguay, Verenigd Koninkrijk en Zwitserland.*

Het bovenstaande is samengevat in een beslisprocedure, dit document is als bijlage toegevoegd aan dit memo.

Voorstel
Aan het college van bestuur wordt het volgende voorgesteld:

- de notitie van de FG waarderen als zijnde het brondocument voor de nieuwe mogelijke inregelingen van verwerkingen persoonsgegevens voor software, cloudapplicaties en apps voor tablets,
- het eventuele onderzoek naar een mogelijke verwerking buiten de EER en binnen een land anders dan zoals genoemd in het adequaatheidsbesluit niet opstarten,
    - een dergelijke verwerking is derhalve niet mogelijk.
- de notitie en de beslisprocedure publiceren binnen Afas Insite en delen met alle directeuren,
- het informeren van onze functionaris voor de gegevensbescherming.

STICHTING H3O
opvang en onderwijs

Beslispunt
Met dit memo wordt derhalve aan het college van bestuur voorgesteld om akkoord te geven op het bovengenoemde voorstel.

Besluit
Het college van bestuur is op ..... akkoord gegaan met het bovengenoemde beslispunt en geeft tevens opdracht aan Van Heumen om dit traject op te starten en te begeleiden.

Bijlagen
- Notitie FG
- beslisprocedure

Notitie

Aan	:	ICM-ers
Kopie	:	Rolf Ritsema
Van	:	Elke van Essen, Functionaris voor gegevensbescherming
Datum	:	8 september 2021
Betreft	:	Standaard modelcontract en aanvullende maatregelen

Inleiding
Wanneer persoonsgegevens de EER verlaten dient de verwerkingsverantwoordelijke organisatie er voor te zorgen dat de mate van bescherming die deze persoonsgegevens binnen de EER hebben, ook buiten de EER blijft bestaan. De mate van bescherming hoeft niet identiek te zijn, maar wel vergelijkbaar op essentiële onderdelen. In de AVG zijn bepalingen over verschillende mechanismen op basis waarvan internationale doorgifte van persoonsgegevens mogelijk is. Voorbeelden van dergelijke mechanismen zijn een adequaatheidsbesluit of een modelcontract.

Adequaatheidsbesluit
Er zijn een aantal landen die van de Europese Commissie (EC) een adequaatheidsbesluit hebben gekregen. Landen die dit besluit hebben gekregen beschikken over een vergelijkbaar passend beschermingsniveau voor persoonsgegevens als landen binnen de EER. Wanneer je persoonsgegevens aan een van deze landen wilt doorgeven kan dit op basis van het adequaatheidsbesluit. De landen waar dit voor geldt zijn Andorra, Argentinië, Canada (alleen commerciële organisaties), Faeröer Eilanden, Guernsey, Isle of Man, Israel, Japan, Jersey, Nieuw-Zeeland, Uruguay, Verenigd Koninkrijk en Zwitserland.

Modelcontract
Als er geen adequaatheidsbesluit is genomen voor het land waar je persoonsgegevens aan door wilt geven, dien je te zorgen voor een ander in de AVG genoemd mechanisme voor passende waarborgen bij de doorgifte van persoonsgegevens. Dat kan door het afsluiten van het modelcontract (ook wel standard contractual clauses of SCC's genoemd) dat door de Europese Commissie is vastgesteld. In het modelcontract zijn afspraken opgenomen die zorgen voor bescherming van persoonsgegevens bij doorgifte naar een derde land en dient ondertekende te worden door de exporterende partij en de importerende partij van de persoonsgegevens. Omdat de Europese Commissie dit contract heeft vastgesteld is het niet toegestaan de tekst van het contract te wijzingen of aan te vullen. Dan verliest het contract zijn geldigheid als doorgifte-mechanisme.

Gevolg uitspraak Europees Hof over Privacy Shield
Op 16 juni 2020 heeft het Europese Hof een uitspraak gedaan over het adequaatheidsbesluit dat de Europese Commissie een aantal jaren eerder had genomen voor de doorgifte van persoonsgegevens aan de Verenigde Staten, het zogenaamde Privacy Shield. In deze uitspraak heeft het Hof geoordeeld dat het Privacy Shield onvoldoende waarborgen geeft voor doorgifte van persoonsgegevens aan de Verenigde Staten. In dezelfde uitspraak is ook bepaald dat doorgifte van persoonsgegevens mogelijk blijf als organisaties het modelcontract afsluiten. Echter, alleen het afsluiten hiervan is niet meer voldoende voor het voldoende waarborgen van de bescherming van de persoonsgegevens. Het probleem hierbij is met name dat de modelcontracten alleen binden de partijen die deze

ondertekenen. De regering van het derde land is *niet* aan de afspraken in het modelcontract gebonden. Daarom zijn organisaties verplicht te beoordelen of de persoonsgegevens bij de doorgifte aan het derde land hetzelfde niveau van bescherming behouden als onder de AVG. Als dit niet zo is, moeten aanvullende maatregelen genomen worden. Wanneer het niet mogelijk blijkt aanvullende maatregelen te nemen, kan de doorgifte van persoonsgegevens naar het derde land niet doorgaan, zo zegt de European Data Protection Board (EDPB), de Europese toezichthouder. De reden hiervoor is dat je in dat geval als verwerkingsverantwoordelijke organisatie de persoonsgegevens niet voldoende kan beschermen, terwijl je wel verantwoordelijk blijft voor deze bescherming.

Aanbevelingen aanvullende maatregelen (EDPB)
De EDPB heeft Aanbevelingen[1] geschreven over welk aanvullende maatregelen je als verwerkingsverantwoordelijke kunt nemen om te zorgen voor een vergelijkbaar beschermingsniveau met de AVG. In de aanbevelingen staan meerdere mogelijke maatregelen, maar deze zijn niet allemaal geschikt voor KIEN en de leden. In deze notitie bespreek ik daarom alleen de meest geschikte maatregelen.

Voorbeelden van effectieve aanvullende technische maatregelen
De maatregelen die EDPB noemt en het meest geschikt zijn, zijn encryptie en pseudonimisering. Dit zijn technische maatregelen die met name nodig zijn in het geval dat door de wet van het derde land de data-importeur verplichtingen worden oplegt die ervoor zorgen dat geen gelijkwaardig niveau van bescherming zoals de AVG gewaarborgd kan worden. Wanneer deze maatregelen worden toegepast, moeten deze wel aan een aantal voorwaarden voldoen om ze ook daadwerkelijk effectief te laten zijn.

➢ *Encryptie*
Encryptie kan een goede maatregel zijn, bijvoorbeeld voor het laten hosten van data in een derde land. Daarbij moet de encryptie aan de volgende voorwaarden voldoen:

- De data moet encrypt worden *voordat* deze doorgegeven wordt aan de data-importeur, waarvan je de *identiteit geverifieerd* hebt;
- Het *algoritme* dat gebruikt wordt voor encryptie moet sterk genoeg zijn, rekening houdend met de stand van de techniek en de technische mogelijkheden waar het derde land over beschikt om toegang te kunnen krijgen tot de data;
- De sterkte van de encryptie en lengte van de *sleutel* moet lang genoeg zijn;
- Het encryptie algoritme is met *betrouwbare software* geïmplementeerd en geverifieerd (bijv. door certificering);
- De sleutels worden op betrouwbare wijze *beheerd* (gegenereerd, opgeslagen, ingetrokken);
- De sleutels worden *bewaard* door de data-exporteur of een derde partij die vertrouwd wordt door de data-exporteur in de EER of in een derde land met een vergelijkbaar niveau van bescherming.

➢ *Pseudonimisering*
Bij pseudonimisering pseudonimiseert de data-exporteur de persoonsgegevens eerst en geeft ze vervolgens door aan een derde land. Pseudonimisering moet aan de volgende voorwaarden voldoen:

[1] https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

- De data-exporteur bewerkt de persoonsgegevens om zo'n manier dat de persoonsgegevens *niet herleidbaar* zijn tot een persoon, zonder het gebruik van *aanvullende informatie*;
- Deze aanvullende informatie wordt *exclusief beheerd* door de data-exporteur en gescheiden bewaard in de EER of een derde land door een organisatie die een vergelijkbaar niveau van bescherming biedt.
- *Toegang* tot deze aanvullende informatie wordt voorkomen door passende technische en organisatorische maatregelen, waardoor verzekerd is dat de data-exporteur als enige de controle heeft over het algoritme of de opslagplaats van de aanvullende informatie, waarmee identificatie van personen mogelijk is.
- De data-exporteur heeft door middel van *onderzoek* van de betreffende persoonsgegevens – rekening houdend met eventuele informatie die de overheid van het ontvangende derde land heeft – vastgesteld dat de gepseudonimiseerde persoonsgegevens met deze informatie niet kunnen leiden tot een identificeerbaar persoon.

Voorbeelden waarbij geen sprake is van effectieve aanvullende maatregelen
Om wat meer duidelijkheid te geven volgen hier nog een aantal voorbeelden van aanvullende maatregelen die niet voldoende zijn om de bescherming van de persoonsgegevens voldoende te kunnen waarborgen.

- Het doorgeven van direct leesbare data aan een cloud service provider en deze data is niet encrypted of gepseudonimiseerd omdat voor het kunnen verwerken van de data deze direct leesbaar moeten zijn;
- De data in het derde land is encrypted en de sleutel van de data is ook in het bezit van het derde land, waardoor de overheid van dit derde land toegang tot de data heeft.
- Alleen contractuele afspraken maken over toegang tot de data. Je bent immers afhankelijk van de wetgeving in het derde land. Afspraken tussen de exporteur en importeur van de data zijn niet bindend voor de overheidsorganisatie die geen partij is in het contract en eigen wettelijke bevoegdheden heeft.

Concrete stappen
Om er als organisatie voor te kunnen zorgen dat de juiste mechanisme en maatregelen ingezet worden bij de doorgifte van persoonsgegevens aan een derde land, moeten er aantal stappen doorlopen worden. Deze stappen worden hieronder benoemd en toegelicht.

1. *Beoordeel of het derde land een adequaatheidsbesluit heeft*

Wanneer je als data-exporteur persoonsgegevens door wilt geven aan een land buiten de EER moet je eerst bekijken of dit land een adequaatheidsbesluit heeft. Als het land een dergelijk besluit heeft zijn er geen aanvullende maatregelen nodig. In geval er een adequaatheidsbesluit is hoeft je de volgende stappen niet te doorlopen. Wanneer je de persoonsgegevens doorgeeft aan een verwerker dient er uiteraard wel een verwerkersovereenkomst afgesloten te worden.

2. *Sluit een modelcontract af*

Wanneer er geen adequaatheidsbesluit is, moet er gebruik gemaakt worden van het modelcontract voor het doorgeven van persoonsgegevens aan een derde land. Beoordeel welk van de 4 modules van toepassing zijn aan de hand van de rol (verwerkingsverantwoordelijke/verwerker) die partijen hebben.

3. *Bepaal aanvullende maatregelen bij standaard modelcontract*

Vervolgens moet onderzocht worden of en welke aanvullende maatregelen nodig zijn om een vergelijkbaar niveau van bescherming van persoonsgegevens te kunnen waarborgen. Om dit te kunnen beoordelen, dien je de volgende acties te ondernemen:

a. Ken je verwerkingen

Om goed te kunnen bepalen welke aanvullende maatregelen nodig zijn, moet je weten welke persoonsgegevens je verwerkt en dus doorgeeft aan het derde land en of andere partijen persoonsgegeven verder verwerken in het derde land of een ander land (sub-verwerkers). Dan kun je ook de mate van gevoeligheid en de hoeveelheid persoonsgegevens bepalen en zodoende welke waarborgen nodig zijn. NB. Wanneer er toegang is vanuit het derde land tot persoonsgegevens opgeslagen in de EER is er ook sprake van doorgifte aan een derde land.

b. Onderzoek of het modelcontract alleen voldoende bescherming biedt

Onderzoek (indien mogelijk, samen met de importeur van de persoonsgegevens) of er bepalingen in de wet van het ontvangende land zijn die kunnen botsen met de bepalingen in het modelcontract en waardoor de persoonsgegevens onvoldoende worden beschermd in vergelijking met de bescherming die de AVG biedt. Je moet met name onderzoeken of overheidsinstanties in het derde land mogelijk toegang hebben tot de persoonsgegevens. Hierbij moet je rekening houden met de wet, wettelijke bevoegdheden, de praktijk en vastgelegde precedenten met betrekking tot de bescherming van persoonsgegevens.

Om te kunnen beoordelen welke wet of praktijk in het ontvangende land van toepassing is, dient je rekening te houden met de volgende specifieke omstandigheden:

- Het doel waarvoor de persoonsgegevens worden doorgegeven en verwerkt;
- De rol en soort organisatie betrokken bij de verwerking (publiek/privaat, verwerkingsverantwoordelijke/verwerker);
- Categorieën van persoonsgegevens (persoonsgegevens over kinderen kunnen onder een specifieke wet vallen in het derde land);
- Of de persoonsgegevens worden opgeslagen in het derde land of dat er op afstand toegang is tot data die in de EER is opgeslagen;
- De manier waarop de data wordt bewaard (encryptie/pseudonimisering);
- Mogelijkheid dat de data verder wordt doorgegeven aan een ander derde land.

Hoewel het onderzoeken naar de beoordeling hoe (de regering van) het derde land omgaat met persoonsgegevens met name gebaseerd dient te worden op de wet van het land, is het in de volgende situaties ook van belang om de omgang van persoonsgegevens in de *praktijk* van het land te onderzoeken:

- Formeel voldoet het derde land aan de waarborgen zoals in de EER, maar in de praktijk van de overheidsinstanties blijkt dat ze zich niet aan deze wet- en regelgeving houden;
- Er is geen relevante wetgeving aanwezig in het derde land. Ook dan moet je kijken naar welke waarborgen die in de praktijk worden gehanteerd;
- De wetgeving in het derde land levert problemen op en persoonsgegevens die doorgegeven worden aan dit land kunnen onder deze problematische wetgeving vallen, maar uit de praktijk blijkt dat deze wet niet wordt toegepast. In

dat geval dient vastgelegd te worden dat uit onderzoek blijkt dat de wet geen belemmering zal zijn voor de data-importeur om aan zijn verplichtingen van de AVG te voldoen.

c. *Neem aanvullende maatregelen*

Als onder 2. duidelijk geworden is dat er aanvullende maatregelen nodig zijn, moet onderzocht worden welke maatregelen nodig zijn. Bij het bepalen van maatregelen die het meest effectief zijn tegen de bescherming van doorgifte van de persoonsgegevens aan overheidsinstanties spelen de volgende (niet-limitatieve) factoren een rol:

- Format waarin de data wordt doorgegeven (plain tekst/ gepseudonimiseerd of encrypted;
- Soort persoonsgegevens (gewone of bijzondere/gevoelige);
- De lengte en complexiteit van de verwerking van de persoonsgegevens, het aantal organisaties die bij de verwerking betrokken zijn en onderlinge relatie daarvan;
- De wijze waarop het derde land de eigen wet in de praktijk toepast;
- De mogelijkheid dat de persoonsgegevens verder doorgegeven worden binnen het derde land of een ander derde land.

In de gevallen dat het niet mogelijk is adequate aanvullende maatregelen te nemen om de persoonsgegevens voldoende te kunnen beschermen, kan de doorgifte niet doorgaan. Wanneer je al een contract hebt met een dergelijke partij moet je bekijken of het mogelijk is de doorgifte van de data stop zetten. Vervolgens moet je ook alle data die deze partij reeds heeft verwerkt laten retourneren, inclusief eventuele kopieën van de data.

d. *Procedurele stappen als je hebt bepaald welke aanvullende maatregelen effectief zijn.*

Zorg er voor dat je kunt aantonen dat de aanvullende maatregelen die je hebt genomen geen afbreuk doen aan de bescherming die de bepalingen in het modelcontract bieden. Houd hierbij in gedachten dat een wijziging van de bepalingen van het modelcontract niet is toegestaan. Een wijziging zorgt er voor dat je je niet langer op het modelcontract kunt baseren voor de doorgifte van persoonsgegevens. Hierdoor wordt de doorgifte onrechtmatig.

e. *Monitoren*

Blijf de ontwikkelingen die effect kunnen hebben op de bij het afsluiten van de overeenkomst vastgestelde bescherming van de persoonsgegevens in het derde land, volgen. Zorg er voor, indien mogelijk, dat je de doorgifte van data kunt stoppen op het moment dat duidelijk wordt dat het derde land niet langer een gelijkwaardig niveau van bescherming kan bieden met de aanvullende maatregelen.

Afsluiten nieuw modelcontract

Afgelopen zomer heeft de Europese Commissie (EC) een nieuw modelcontract[2] goedgekeurd en vastgesteld dat geldig is vanaf 27 juni 2021. De tekst van het eerdere standaard modelcontract was voor het laatst herzien in 2010. Bij het afsluiten van nieuwe

[2] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32021D0914&from=EN

overeenkomsten met partijen in derde landen, dient het nieuwe modelcontract gebruikt te worden. Voor de partijen (veelal verwerkers) waar de organisatie eerder een standaard modelcontract heeft afgesloten geldt dat het oude modelcontract vervangen moet worden voor het nieuwe modelcontract. Om er voor te zorgen dat de persoonsgegevens die doorgegeven worden goed beschermd worden dienen partijen daarbij ook te onderzoeken of aanvullende maatregelen nodig zijn zoals hiervoor beschreven. Het vervangen en ondertekenen van dit nieuwe modelcontract dient binnen 18 maanden na 27 juni 2021 te gebeuren. Na die datum verliest het oude modelcontract zijn geldigheid.

Het nieuwe modelcontract bestaat uit 4 verschillende modules. Doorgifte van persoonsgegevens naar een derde land door:

- verwerkingsverantwoordelijke aan een andere verwerkingsverantwoordelijke;
- verwerkingsverantwoordelijke aan verwerker;
- verwerker aan verwerkingsverantwoordelijke ;
- verwerker aan verwerker.

Afhankelijk van de rol van partijen (verwerkersverantwoordelijken en/of verwerkers) dien je de van toepassing zijnde module te kiezen. Dit zal meestal de tweede module zijn.

Beslisprocedure verwerking persoonsgegevens (versie 30 september 2021)