Handreiking: Transfer Impact Assessment (TIA)

A. Samenvatting: Use Case 5. Onderwijs: Studieresultaten
Zie ook: Use Case 2. Onderwijsgegevens in de cloud (bijvoorbeeld portfolio's in Blackboard)

1. Beschrijving van het probleem
Het gebruik door een Nederlandse onderwijsinstelling van een cloud dienst van een in de Verenigde Staten (VS) gevestigde dienstenleverancier, voor de registratie van studieresultaten, betreft een verwerking van persoonsgegevens van studenten en medewerkers, inclusief een doorgifte van deze gegevens naar de VS, een zogenaamd '*derde land*'. Met de ongeldigverklaring van het *EU-US Privacy Shield* is voor deze doorgifte een andere juridische grondslag vereist. De betreffende onderwijsinstelling is verantwoordelijk voor het borgen van de bescherming van de persoonsgegevens, ook bij de doorgifte, en moet waarborgen, en kunnen aantonen, dat de bescherming van de persoonsgegevens een passend beschermingsniveau heeft, dat in essentie gelijk is aan de waarborgen zoals gesteld in de AVG.

Deze verplichting valt uiteen in *twee* samenhangende aspecten van de verwerking van persoonsgegevens:
(1) als onderdeel van de beoogde (primaire) werking van de dienst (o.a. aanbieden en volgen van onderwijs / toetsing etc) doorgifte van persoonsgegevens (voorbeeld: docent X, student Y, Opdracht A van docent X en Waardering B van student Y, etc), en
(2) als onderdeel van de secundaire verwerking van en gerelateerd aan deze persoonsgegevens, door de VS dienstenleverancier, vanwege diens verzameling van logbestanden, telemetrie, en andere meta-gegevens die persoonsgegevens kunnen bevatten en direct of indirect herleidbaar zijn tot studenten en docenten verbonden aan de NL onderwijsinstelling.

2. Identificeer het juridisch mechanisme voor doorgifte van persoonsgegevens op basis waarvan de doorgifte rechtmatig is.
Antwoord: AVG Art. 46, lid 2, sub d.: standaardbepalingen inzake gegevensbescherming die door een toezichthoudende autoriteit zijn vastgesteld en die door de Commissie volgens de in artikel 93, lid 2, bedoelde onderzoeksprocedure zijn goedgekeurd (*Standard Contractual Clauses*).
Zie voor onderbouwing de '*Root Cause' Analyse* hieronder: *MAATREGEL 1*.

3. Is het juridisch mechanisme in de praktijk effectief (*'in practice and in full'*) bij de VS organisatie die de NL data importeert?
Antwoord: Ja, **mits** de VS dienstverlener aantoonbaar voldoet aan de door de AVG gestelde waarborgen, zoals kan blijken uit een DPIA.
Zie voor onderbouwing de '*Root Cause' Analyse* hieronder: *MAATREGEL 3 en 4*.

4. Zijn aanvullende maatregelen nodig?
Antwoord: Ja, het is redelijk om te verwachten dat zowel de VS leverancier (data importeur) als ook de NL onderwijsinstelling (data exporteur) bepaalde maatregelen dient te nemen ten behoeve van de bescherming van persoonsgegevens bij de doorgifte van persoonsgegevens naar de VS (zie: *MAATREGEL 5*, hieronder.). Zie voor onderbouwing de '*Root Cause' Analyse* hieronder: *MAATREGEL 5*.
Zie ook de handreiking: Aanvullende maatregelen data-doorgiften naar de VS.

Disclaimer
De SURF Taskforce Beyond Privacy Shield heeft bovenstaand advies opgesteld naar aanleiding van de beschreven generieke use case. Dit advies is bedoeld als handreiking voor de onderwijsinstellingen die zelf deze afweging dienen te maken, voorafgaand aan een concrete verwerking. Er kunnen aan dit advies geen rechten worden ontleend. In de concrete verwerking kunnen specifieke aspecten van de verwerking aanleiding geven tot een andere afweging, en andere bijbehorende aanvullende maatregelen. De onderwijsinstelling blijft zelf verantwoordelijk voor deze afweging.

Handreiking: Transfer Impact Assessment (TIA)

PRODUCT/PROCES	5. Studieresultaten	DOOR	SURF Taskforce Beyond Privacy Shield	DATUM	September 2022

WAT IS HET PROBLEEM?

Het gebruik door een Nederlandse onderwijsinstelling van een cloud dienst van een in de Verenigde Staten (VS) gevestigde dienstenleverancier, voor onderwijsdoeleinden, en in het bijzonder de registratie van studieresultaten, betreft een verwerking van persoonsgegevens van studenten en medewerkers, inclusief een doorgifte van deze gegevens naar de VS, een zogenaamd 'derde land'. Met de ongeldigverklaring van het EU-US Privacy Shield is voor deze doorgifte een andere juridische grondslag vereist. De betreffende onderwijsinstelling is verantwoordelijk voor het borgen van de bescherming van de persoonsgegevens, ook bij de doorgifte, en moet waarborgen, en kunnen aantonen, dat de bescherming van de persoonsgegevens een passend beschermingsniveau heeft, dat in essentie gelijk is aan de waarborgen zoals gesteld in de AVG.

TE NEMEN MITIGERENDE MAATREGEL

WAAROM IS DIT EEN PROBLEEM?

PRIMAIRE OORZAAK — ****OPMERKING: Als de laatste "Waarom?" geen beheersbare oplossing heeft, keer dan terug naar de vorige "Waarom?".** — **'ROOT CAUSE'**

Waarom gebeurt dit?	Waarom?	Waarom?	Waarom?	Waarom?
Met de ongeldig-verklaring van het EU-US Privacy Shield is een einde gekomen aan het juridisch mechanisme voor de rechtmatige doorgifte van persoonsgegevens van NL naar de VS. Dit betreft zowel (1) de verwerking van *persoonsgegevens* in het systeem als (2) de zogenaamde *diagnostische persoonsgegevens*, gegenereerd op basis van het gebruik van deze cloud dienst. NL onderwijs-instellingen zijn verantwoordelijk voor aantoonbare passende waarborgen voor hun doorgiften van persoonsgegevens naar VS diensten-leveranciers en hun onderaannemers.	De VS diensten-leverancier kan vanwege zogenaamde 'problematische nationale wetgeving' namelijk niet zonder meer geacht worden om aantoonbaar te voldoen aan diens contractuele verplichtingen uit de hoofd-overeenkomst en/of de *data processing agreement* met betrekking tot de bescherming van persoonsgegevens van de NL onderwijsinstelling. Nationale wetgeving heeft namelijk, voor de VS dienstverlener, voorrang op een contractuele overeenkomst.	De door het Hof van Justitie van de Europese Unie genoemde voorbeelden van problematische nationale wetgeving in de VS: Foreign Intelligence Surveillance Act (FISA)* en Executive order 12333 (EO12333)**. Leveranciers van clouddiensten vallen onder de scope van FISA: de "electronic communications service providers" (ECSPs)***. Op basis van FISA kan een VS dienst-leverancier namelijk verplicht worden alle persoons-gegevens van alle 'niet VS inge-zetenen' te verstrekken aan VS overheidsdiensten.	Deze FISA verplichting conflicteert met de AVG beginselen inzake verwerking van persoons-gegevens*, te weten: "doel-binding" en "proportionaliteit". Tevens kunnen studenten en/of docenten van de NL onderwijs-instelling hun AVG rechten niet effec-tief uitoefenen (Verhaals-mechanisme) bij de *privacyschild ombudsman***. Het Hof acht de onafhankelijkheid van de ombuds-man en diens bevoegdheid om bindende besluiten te nemen is namelijk niet verzekerd***.	De VS stelt andere eisen aan bescherming van persoonsgegevens dan de EU, en deze zijn in essentie *niet equivalent*, zoals de EU echter eist. AVG Art. 45 (Door-giften op basis van adequaatheids-besluiten) is voor EU-VS doorgiften van persoonsgegevens niet meer van toepassing.
* Zie: Bron 2: paragraaf 118, 201.		* Zie: Definitie 7. ** Zie: Definitie 8. *** Zie: Definitie 9.	* Zie: EU AVG Art 5. **Zie Bijlage III: Besluit (EU) 2016/1250). *** ibidem Art 4 lid 6	

MAATREGEL 1	OPMERKINGEN	OPMERKINGEN	REFERENTIE(S)
De EU-VS doorgifte van persoons-gegevens kan op basis van AVG Art. 46, lid 2, sub d, door gebruik te maken van de zogenaamde **Standard Contractual Clauses** (SCCs*), waar nodig aangevuld met aanvullende waarborgen**.	Op 4 juni 2021 heeft de Europese Commissie *nieuwe SCCs* vastgesteld. Dit heeft de volgende consequenties: (1) de *nieuwe SCCs* moeten per 27 september 2021 worden gebruikt voor nieuwe overeen-komsten (per die datum zijn de 'oude SCCs' niet meer geldig) en (2) per 27 december 2022 dient bij alle overeen-komsten van een organisatie (uitsluitend) de *nieuwe SCCs* te zijn gebruikt.	In deze nieuwe SCCs wordt in overweging 19 gesteld: "The transfer and processing of personal data under standard contractual clauses should not take place if the laws and practices of the third country of destination prevent the data importer from complying with the clauses." Om dit risico vast te stellen dient de instelling (de data exporter) een transfer impact assessment te doen*.	Zie voor de nieuwe SCCs: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en
* Bron 2: paragraaf 203 lid 4. ** Zie ook de Handreiking Aanvullende maatregelen.	* Zie: Art 4 * Commission Implementing Decision SCCs.	* Zie: 2.Juridisch kader: SCCs.	

Handreiking: Transfer Impact Assessment (TIA)

ONDERLIGGEND PROBLEEM | **'ROOT CAUSE'**

Waarom gebeurt dit?	Waarom?	Waarom?	Waarom?	Waarom?	**MAATREGEL 2**	OPMERKINGEN MBT HET RISICO ASSESSMENT	OPMERKINGEN MBT HET RISICO ASSESSMENT	REFERENTIE(S)
De instelling dient een inschatting te maken of de instelling in de VS redelijkerwijs geacht kan worden de verplichtingen zoals bepaald in de SCC in de praktijk volledig na te leven.	Nationale wetgeving kan VS instellingen dwingen gegevens van het onderwijs cloud platform ter beschikking te stellen aan VS veiligheidsdiensten, hetgeen in conflict is met de SCCs.	Echter, er zijn vanuit de VS randvoorwaarden voor een dergelijk dwingend verzoek aan instellingen, namelijk dat er voor de VS een reëel risico moet bestaan in deze onderwijs cloud dienst.	De US AG DNI dienen 'NI onderwijs' als risico in zogenaamde certificaten te benoemen. Toetsing door de FISC. Pas na akkoord FISC dwang tot verstrekking van gegevens.	Het is feitelijk onbekend wat de inhoud van de certificaten is. Zie ook bijvoorbeeld deze uitspraak van de FISC. Zie voor de inschat-ting van het risico ook de FISA Risicoprofielen.	**Schat de kans in** dat studieresultaten, als onderdeel van persoonsgegevens, van studenten en docenten uit Nederland, redelijkerwijs door de VS als risico kunnen worden bestempeld, bijvoorbeeld in een FISA Risicoprofiel.	In het 2020 jaarverslag van FISA staat dat in dat jaar het totaal aantal personen dat onderwerp was van FISA surveillance kleiner was dan 500.	De instelling kan vragen stellen aan de VS leverancier die dit risico in kaart brengen. Zie hiertoe bijvoorbeeld de vragenlijst van noyb.	noyb – ook bekend als: "European Center for Digital Rights" is de not-for-profit organisatie opgericht in 2018 door M. Schrems.

* Bron 2: paragraaf 34

* Zie: Def 7: FISA

* Zie: Def 10: FISA Risicoprofielen

* Zie ook: Definitie 10

ONDERLIGGEND PROBLEEM | **'ROOT CAUSE'**

Waarom gebeurt dit?	Waarom?	Waarom?	Waarom?	Waarom?	**MAATREGEL 3**	OPMERKINGEN MBT HET RISICO ASSESSMENT	OPMERKINGEN MBT HET RISICO ASSESSMENT	REFERENTIE(S)
De instelling dient een inschatting te maken of, naast de SCCs, aanvullende waarborgen vereist zijn voor de EU-VS doorgifte van *persoonsgegevens*.	Voor de verwerking van persoonsgegevens kan gelden: - gebrek aan *doelbinding,* een *rechtmatige grondslag*, en *opslagbeperking* - gebrek aan controle (oa audit) op verwerking	De VS dienstleverancier is niet altijd 100% transparant over het bestaan, of de aard en omvang en de doelen van deze verwerking van diagnostische persoonsgegevens.	Een dienstleverancier zal bepaalde informatie nodig hebben voor de uitoefening van kwaliteitszorg en gebruikersonder-steuning. Vraag is wat doelmatig en proportioneel is.	Persoonsgegevens kunnen zonder dat de instelling hier weet van heeft - of toestemming voor geeft - worden verwerkt voor onbekende doelen door de dienstverlener en evt sub processors in derde landen.	**Vraag de leverancier om transparantie** over de verwerking van diagnostische persoonsgegevens. Toets* in een **DPIA** of deze informatie correct en volledig is, oa door analyse van log bestanden.	Maak op basis van deze DPIA afspraken met de leverancier over de rechtmatige verwerking van diagnostische persoonsgegev ens en over het staken van onrechtmatige verwerkingen.	Dergelijke DPIAs zijn recentelijk met positief resultaat uitgevoerd door SLM Rijk, ism oa SURF tbv de instellingen. Het is voor een individuele instelling lastig dit resultaat zelfstandig te bereiken.	Zie: https://slmmicrosoftrijk.nl/sdm_categories/dpia/

* Bron 2: paragraaf 34

* Zie ook de Handreiking Aanvullende maatregelen.

Handreiking: Transfer Impact Assessment (TIA)

	ONDERLIGGEND PROBLEEM				'ROOT CAUSE'				
	Waarom gebeurt dit?	Waarom?	Waarom?	Waarom?	Waarom?	**MAATREGEL 4**	OPMERKINGEN	OPMERKINGEN MBT HET RISICO ASSESSMENT	REFERENTIE(S)
	De instelling dient een inschatting te maken of, naast de SCCs, aanvullende waarborgen vereist zijn voor de EU-VS doorgifte van *diagnostische persoonsgegevens* (telemetrie en geautomatiseerde metadata).	Voor de verwerking van diagnostische persoonsgegevens kan gelden: - gebrek aan *doelbinding*, een *rechtmatige grondslag*, en *opslagbeperking* - gebrek aan controle (oa audit) op verwerking	De VS dienstleverancier is niet altijd 100% transparant over het bestaan, of de aard en omvang en de doelen van deze verwerking van diagnostische persoonsgegevens.	Een dienstleverancier zal bepaalde informatie nodig hebben voor de uitoefening van kwaliteitszorg en gebruikersonder-steuning. Vraag is wat doelmatig en proportioneel is.	Persoonsgegevens kunnen zonder dat de instelling hier weet van heeft - of toestemming voor geeft - worden verwerkt voor onbekende doelen door de dienstverlener en evt sub processors in derde landen.	**Vraag de leverancier om transparantie** over de verwerking van diagnostische persoonsgegevens. Toets, bijvoorbeeld in een **DPIA,** of deze informatie correct en volledig is.	Maak op basis van deze DPIA afspraken met de leverancier over de rechtmatige verwerking van diagnostische persoonsgegev ens en over het staken van onrechtmatige verwerkingen.	Dergelijke DPIAs zijn recentelijk met positief resultaat uitgevoerd door SLM Rijk, ism oa SURF tbv de instellingen. Het is voor een individuele instelling lastig dit resultaat te bereiken.	Zie: https://slmmicrosoftrijk.nl/sdm_categories/dpia/

* Bron 2: paragraaf 34

Handreiking: Transfer Impact Assessment (TIA)

ONDERLIGGEND PROBLEEM				'ROOT CAUSE'				
Waarom gebeurt dit?	Waarom?	Waarom?	Waarom?	Waarom?	**MAATREGEL 5**	OPMERKINGEN	OPMERKINGEN MBT HET RISICO ASSESSMENT	REFERENTIE(S)
De instelling dient een inschatting te maken van de risico's voor de student, en de docent gegeven 'de inhoud en de duur van de overeenkomst, de aard van de door te geven gegevens, het soort ontvanger, het doel van de verwerking'* van de persoonsgegevens betrokken bij de betreffende verwerking.	Voor de doorgifte van persoons-gegevens van NL studenten en docenten aan een dienstenleverancier in het derde land de VS, kan de NL instelling zich sinds Case C-311/18 niet meer beroepen op het adequaat-heidsbesluit. Wel kan de instelling de doorgifte doen op basis van SCCs (AVG Art 46), mits op basis van bijvoorbeeld een DPIA is vastgesteld dat geen onrechtmatige verwerking van (diagnostische) persoonsgegevens plaatsvindt.	SCCs kunnen redelijkerwijs geacht worden nageleefd te worden door de VS dienstenleverancier. Doorgifte van persoonsgegevens kan dus plaatsvinden, 'as a rule', op basis van SCCs - en de in de SCCs opgenomen verplichting tot het bredere security- en privacy assessment mbt de verwerking van persoonsgegevens.			De NL instelling kan zich, 'as a rule' beroepen op de **SCCs** als mechanisme voor doorgifte van (diagnostische) persoonsgegevens. Wel kunnen op basis van een DPIA **aanvullende maatregelen** worden geïdentificeerd bijvoorbeeld mbt het gebruik of de standaardinstel-lingen van de betreffende dienst.	Hierbij valt te denken aan aanvullende maatregelen zoals: - 'anonieme telemetrie' bij de leverancier, - bij de instelling telemetrie-verkeer naar bekende eindpunten blokkeren - end-to-end versleutelde communicatie van persoons-gegevens naar de leverancier (in transit) en - versleuteling van data bij de leverancier (in rest). - borgen in de VO dat uitsluiten vastgestelde rollen bij de leverancier voor gedocu-menteerde doelen en alleen op basis van *need to know* toegang hebben tot EU persoons-gegevens. - alleen gedocu-menteerde doorgiften naar derden van EU persoonsgege vens.	SLM Rijk (pg 1) constateert: "Op grond van een technische analyse van het telemetriegege vensverkeer concludeert dit rapport dat Microsoft via de telemetrie op het Beveiligings-niveau weinig persoonsgegev ens verwerkt, en geen persoons-gegevens van gevoelige aard. Daarom zijn er géén hoge dataprotectie-risico's als het telemetrienivea u op Beveiliging wordt gezet, of het telemetrie-verkeer wordt geblokkeerd." Zo ook zal een analyse van de telemetrie van een cloud dienst ten behoeve van onderwijs inzicht geven in de aard en omvang van de aard van de persoons-gegevens, op basis waarvan het gerela-teerde AVG compliancy risico.	SLM Rijk: 1. Data protection impact assessments DPIA's Office 365 ProPlus, Windows 10 Enterprise, Office 365 online and mobile apps. 2. DPIA Google G Suite Enterprise 3. Zie ook: Autoriteit Persoons-gegevens: "Advies: Google G Suite for Education".

* Bron 6: overweging 20

Handreiking: Transfer Impact Assessment (TIA)

B. Definities

1. **Doorgifte**: De term “doorgifte” is niet gedefinieerd in de AVG. De Europese toezichthouder stelt dat met het begrip doorgifte wordt gedoeld op het ter kennis brengen van de gegevens aan een persoon die zich bevindt in een derde land. Van doorgifte is sprake wanneer persoonsgegevens worden doorgegeven/delen of anderszins ter beschikking wordt gesteld van/door een bedrijf/organisatie in het ene land naar het andere land of van, naar en/of tussen een internationale organisatie. Dit kan zowel gaan om het delen van persoonsgegevens binnen de Europese Unie als buiten de Europese Unie. Wanneer wordt gesproken over doorgifte wordt expliciet gedoeld op *cross border transfers*. Dit kan gaan om de doorgifte tussen zowel (sub)verwerkers als in concernverband. Binnen de EER (zie hieronder: “*Derde land/EER*”) geldt eenzelfde beschermingsniveau voor persoonsgegevens zodat doorgifte – mits is voldaan aan alle overige eisen voor het rechtmatig delen van persoonsgegevens – is toegestaan. Voor doorgifte van persoonsgegevens buiten de EER – ook wel derde landen genoemd – geldt dat dit alleen is toegestaan wanneer sprake is van een passend beschermingsniveau. **Bron 10, pg 215, 216.**

2. **Derde land/EER**: Onder een derde land wordt verstaan een land buiten de rechtsmacht van één van de landen van de Europese Unie. De AVG is tevens verbindend verklaard voor de landen die geen lid zijn van de Europese Unie maar wel behoren tot de Europese Economische Ruimte (EER), te weten: Noorwegen, IJsland en Liechtenstein.

3. **Privacy Shield**: De EU-VS en Zwitsers-VS Privacy Shield Frameworks zijn ontworpen door respectievelijk het Amerikaanse Ministerie van Handel, de Europese Commissie en de Zwitserse regering om bedrijven aan beide zijden van de Atlantische Oceaan een mechanisme te bieden om te voldoen aan de vereisten voor gegevensbescherming bij doorgifte van persoonsgegevens vanuit de Europese Unie en Zwitserland naar de Verenigde Staten ter ondersteuning van de transatlantische handel.

4. **Ongeldigverklaring Privacy Shield**: Op 12 juli 2016 oordeelde de Europese Commissie (Besluit (EU) 2016/1250) dat het EU-VS Privacy Shield Framework gepaste bescherming bood om gegevensoverdrachten onder EU-wetgeving mogelijk te maken. Op 16 juli 2020 heeft het Hof van Justitie van de Europese Unie het hierboven genoemde Besluit (EU) 2016/1250 van de Europese Commissie als "ongeldig" verklaard. Als gevolg van dat besluit is het EU-VS Privacy Shield Framework niet langer een geldig mechanisme om te voldoen aan de EU-vereisten voor gegevensbescherming bij de overdracht van persoonlijke gegevens van de Europese Unie naar de Verenigde Staten. Bron

5. **Standard Contractual Clauses (SCCs)**: Doorgifte van persoonsgegevens naar een derde land, mag, conform de AVG, bij ontstentenis van een adequaatheidsbesluit van de Commissie, alleen plaatsvinden indien de verantwoordelijke voor de doorgifte, samen met de organisatie in het derde land, passende waarborgen bieden voor de bescherming van deze persoonsgegevens, en betrokkenen (in dit geval: de studenten waarvan de studieresultaten van het reguliere onderwijs worden geregistreerd in een cloud dienst) over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. Die waarborgen kunnen worden geboden door standaardbepalingen inzake gegevensbescherming die door de Europese Commissie overeenkomstig zijn vastgesteld; de standaardcontractbepalingen, beter bekend met de Engelse aanduiding: *Standard Contractual Clauses* (SCCs).

6. **Aanvullende waarborgen, aanvullend op de SCCs**: In de door de Europese Commissie geactualiseerde SCCs staat hierover het volgende opgenomen (overweging 3):
“De rol van standaardcontractbepalingen is beperkt tot het garanderen van passende gegevensbeschermingswaarborgen voor internationale doorgiften van gegevens. Het staat de verwerkingsverantwoordelijke of verwerker die de persoonsgegevens naar een derde land doorgeeft (de “gegevensexporteur”) en de verwerkingsverantwoordelijke of verwerker die de persoonsgegevens ontvangt (de “gegevensimporteur”) derhalve vrij om die standaardcontractbepalingen in een breder contract op te nemen en om andere bepalingen of meer waarborgen toe te voegen, op voorwaarde dat deze niet direct of indirect in strijd zijn met de standaardcontractbepalingen en geen afbreuk doen aan de grondrechten of fundamentele vrijheden van de betrokkenen. Verwerkingsverantwoordelijken en verwerkers worden aangemoedigd om door middel van contractuele verplichtingen meer waarborgen te bieden in aanvulling op de standaardcontractbepalingen.”

7. **Foreign Intelligence Surveillance Act (FISA), sectie 702**: Sectie 702 is een belangrijke bepaling, als onderdeel van de 2008 wijziging van de FISA [wet betreffende het toezicht op buitenlandse inlichtingen], op basis waarvan de regering in de Verenigde Staten niet VS ingezetenen, die zich buiten de Verenigde Staten bevinden, gericht kan observeren, met de gedwongen hulp van aanbieders van elektronische communicatiediensten (**ECSPs**), om buitenlandse inlichtingen te verkrijgen. De regering van de Verenigde Staten gebruikt de informatie die is verzameld op basis van Sectie 702, om de Verenigde Staten en hun bondgenoten te beschermen tegen vijandige buitenlandse tegenstanders, waaronder terroristen en spionnen, en om hierover informatie te verstrekken aan de cyberbeveiliging in de Verenigde Staten. Om op basis van FISA sectie 702 informatie te kunnen verzamelen, dienen daartoe door de United States Attorney General (procureur-generaal van de Verenigde Staten) [AG] en de Director of National Intelligence (directeur nationale inlichtingen) [DNI] certificaten te worden opgesteld en te worden voorgelegd aan de Foreign Intelligence Surveillance Court (FISC - rechtbank voor buitenlandse-inlichtingensurveillance van de Verenigde Staten) die vervolgens op basis daarvan categorieën van buitenlandse inlichtingen specificeren, die mogen worden gebruikt om informatie te verzamelen. De FISC legt hierbij haar bevindingen schriftelijk vast in een 'opinion'. Na een approval van de FISC, inclusief 'targeting and minimization procedures', kunnen de procureur-generaal van de Verenigde Staten en de directeur van de Nationale Inlichtingendienst schriftelijke 'directives' uitvaardigen die Amerikaanse aanbieders van elektronische communicatiediensten dwingen om te helpen bij het verzamelen van de door de FISC geautoriseerde Sectie 702-doelen. Bron.

   Op grond van FISA sectie 702 geeft de FISC daarentegen geen toestemming voor individuele surveillancemaatregelen; de FISC geeft in plaats daarvan toestemming voor surveillanceprogramma's (zoals PRISM en Upstream) op basis van jaarlijkse certificeringen die door de AG van de Verenigde Staten en de (DNI) worden voorbereid. Deze certificeringen bevatten geen informatie over de individuele personen die het doelwit moeten worden, maar ze bepalen in plaats daarvan bepaalde categorieën van buitenlandse inlichtingen. De FISC beoordeelt dus niet – op grond van een redelijk vermoeden of een andere norm – of natuurlijke personen het juiste doelwit zijn om buitenlandse inlichtingen te verwerven, maar controleert de voorwaarde zelf; dat het verkrijgen van buitenlandse inlichtingen een significant doel is'. Bron: Case C-311/18, paragraaf 109.

   Noot: Verwijzing in de CJEU Case C-311/18 uitspraak paragraaf 60: "Volgens de vaststellingen in die uitspraak zijn de inlichtingenactiviteiten van de Amerikaanse autoriteiten met betrekking tot de naar de Verenigde Staten doorgegeven persoonsgegevens met name gebaseerd op section 702 FISA en op E.O. 12333.".

8. **Executive Order 12333 (E.O. 12333)**: Executive Order 12333 (1981) had als doel om de bevoegdheden en verantwoordelijkheden van Amerikaanse inlichtingendiensten uit te breiden en de 'heads of the US federal agencies' op te dragen volledig mee te werken aan informatieverzoeken van de CIA. "All departments and agencies shall cooperate fully to fulfill this goal." Bron. De hoofden van de 15 uitvoerende afdelingen: 'the Secretaries of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Labor, State, Transportation, Treasury, and Veterans Affairs, and the Attorney General'. Bron.

   Noot: Verwijzing in de CJEU Case C-311/18 uitspraak paragraaf 60: "Volgens de vaststellingen in die uitspraak zijn de inlichtingenactiviteiten van de Amerikaanse autoriteiten met betrekking tot de naar de Verenigde Staten doorgegeven persoonsgegevens met name gebaseerd op section 702 FISA en op E.O. 12333.".

9. **ECSP** Organisaties die gekenmerkt zijn als: "electronic communication service provider" vallen onder de wettelijke verplichtingen van FISA sectie 702. De definitie is breed want betreft:
   (A) a telecommunications carrier, as that term is defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);
   (B) a provider of electronic communication service, as that term is defined in section 2510 of title 18, United States Code;
   (C) a provider of a remote computing service, as that term is defined in section 2711 of title 18, United States Code;
   (D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored;
   (E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

10. **FISA Risicoprofielen** De certificaten van de AG en de DNI worden niet openbaar gemaakt (zie: Definitie 7 hierboven). Deze certificaten zouden in de context van een Transfer Impact Assessment inzicht kunnen geven in risicoprofielen zoals gehanteerd door de AG en de DNI en daarmee een goede onderbouwing voor de inschatting van de kans dat een bepaalde doorgifte als risicovol wordt gezien in de context van FISA sectie 702. Er is echter wel gedeclassificeerde informatie beschikbaar, zoals de “Release of Documents Related to the Fisa Section 702 Certifications”. Zie hier voor het jaar 2019 en hier voor 2020. Deze documenten zijn publiek gemaakt door de Office of the Director of National Intelligence (ODNI). De ODNI is een agentschap dat toezicht houdt op de inlichtingengemeenschap. Op basis van deze informatie kan de risico-inschatting op basis van FISA sectie 702 iets beter geïnformeerd plaatsvinden. Zo lezen we in Memorandum Opinion and Order [FISC, 6 december 2019], dat:

    - de 2019 certificaten grotendeels een continuering zijn van de 2018 certificaten (pg 5);
    - de VS overheid een persoon kan ‘*targeten*’, onder specifieke voorwaarden, en op grond van FISA sectie 702 door een of meer selectors (bijvoorbeeld identificatiegegevens voor e-mail of andere elektronische-communicatie accounts) die aan die persoon zijn gekoppeld, voor te dragen voor het verwerven van een of meer selectors, bijvoorbeeld '*upstream*' bij het onderscheppen van deze informatie van een internet-backbone-carrier, of '*downstream*' van systemen die worden beheerd door dienstverleners (pg 9).
    - ‘upstream’ informatievergaring de meeste beperkingen kent ten opzichte van ‘downstream’ informatievergaring (pg 14).
    - als voorwaarde voorwaarde voor targeting geldt dat vast moet staan dat de betreffende persoon geen VS ingezetene is (pg 4 en pg 8 (*III. The Targeting Procedures*))
    - tevens als voorwaarde geldt dat: ‘Een NSA-targeting beslissing moet ook worden ondersteund door een specifieke en op feiten gebaseerde beoordeling dat van het doelwit wordt verwacht dat deze buitenlandse inlichtingen bezit, ontvangt en/of zal doorgeven die relevant is voor het onderwerp van een geautoriseerde Sectie 702-certificering.’ (pg 9)

    Voor de helderheid wordt hier geciteerd uit de NSA's Section 702 Targeting Procedures, Sep. 17, 2019, “*(U) Assessment of the Foreign Intelligence Purpose of the Targeting*” (pg 4):

    “NSA must also reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory authorized for targeting under a certification or authorization executed by the Director of National Intelligence and the Attorney General in the manner prescribed by section 702. This assessment must be particularized and fact-based, informed by analytic judgment, the specialized training and experience of the analyst, as well as the nature of the foreign intelligence information expected to be obtained.”

    Ook in de 2020 Memorandum Opinion and Order [FISC, 18 december 2020] lezen we dat:
    - de 2020 certificaten grotendeels een continuering zijn van de 2019 certificaten (pg 4), die zelf feitelijk een continuering zijn van certificaten uit 2008 (pg 5).

    Concluderend zien we dat de de FISA certificaten grotendeels betrekking hebben op individuen waarvan feitelijk en specifiek door NSA en FBI aannemelijk kan worden gemaakt dat deze sinds 2008 beschikken over buitenlandse inlichtingen, deze ontvangt en/of zal doorgeven.

11. **Klantgegevens / functionele gegevens / diagnostische gegevens - telemetriegegevens (telemetrie)**
    Voor de definitie van deze typen van gegevens, verwijzen we naar de definities zoals gepresenteerd in de verschillende DPIA’s uitgevoerd in opdracht van SLM Rijk met betrekking tot de Google G Suite Enterprise (d.d. 9 juli 2020, met update op 12 februari 2021) en met betrekking tot Office 365 ProPlus, Windows 10 Enterprise, Office 365 online and mobile apps.
    Hieronder worden Nederlandse vertalingen van de Engelstalige brondocumenten geboden en zijn teksten voor het leesgemak geparafraseerd.

    In de Samenvatting DPIA Windows 10 Enterprise wordt (pg 2, 3) de relatie tussen telemetrie en persoonsgegevens gelegd: ‘Microsoft verzamelt een beperkte hoeveelheid gegevens over het

individuele gebruik van de Windows 10 software. De verzamelde telemetriegegevens bevatten een aantal unieke identifiers. Die identifiers stellen Microsoft in staat om gegevens over een individuele gebruiker door de tijd heen te combineren. Microsoft beschikt over de technische middelen om een individuele gebruiker te identificeren. Daarom zijn de verzamelde telemetriegegevens ***persoonsgegevens*** als bedoeld in artikel 4(1) van de AVG.'.

In de DPIA on the use of Google G Suite (Enterprise) (pg 18 ev) wordt onderscheid gemaakt tussen: klantgegevens, functionele gegevens en diagnostische gegevens.

a. **Klantgegevens**. Op pg 24 wordt een onderscheid gemaakt tussen:
• "Klantgegevens": gegevens die via de *Core Services*[1] door de instelling of student/medewerker zijn ingediend, opgeslagen, verzonden of ontvangen (inclusief tekst, code, afbeeldingen, video en geluid).
• "Persoonlijke klantgegevens": de persoonlijke gegevens in de klantgegevens.

b. **Functionele gegevens -** Zie pg 26:
Functionele gegevens zijn gegevens die slechts voor een korte periode nodig zijn om te kunnen communiceren met de clouddiensten van Google. Voorbeelden van dergelijke functionele gegevens zijn de gegevens die door een e-mailserver worden verwerkt om de communicatie te leveren, en de gegevensstroom die nodig is om de eindgebruiker in staat te stellen zich te verifiëren of te verifiëren of de eindgebruiker een geldig Google-account heeft. Het belangrijkste verschil tussen functionele gegevens en diagnostische gegevens, is dat functionele gegevens van voorbijgaande aard zijn en onmiddellijk worden verwijderd of geanonimiseerd na voltooiing van de verzending van de communicatie.
Een voorbeeld van functionele gegevens is de inhoud bevatten van tekst die eindgebruikers willen laten vertalen of spellen. In deze gevallen is het nodig dat Google als cloudprovider de context verzamelt, voor betere spelling of vertaling zorgt.

c. **Diagnostische gegevens.** Zie pg 24:
'Google verzamelt op meerdere manieren diagnostische gegevens over het individuele gebruik van G Suite (Enterprise) for Education-services, bijvoorbeeld door het gebruik van cookies, door ***telemetriegegevens*** te verzamelen over het gebruik van mobiele apps en door door het systeem gegenereerde logs op eigen G Suite (Enterprise) for Education-cloudservers. Google verzamelt diagnostische gegevens bijvoorbeeld wanneer eindgebruikers documenten opslaan of openen in Gmail, Drive, Docs en andere cloudgebaseerde services.

Dergelijke diagnostische gegevens worden opgeslagen in gedetailleerde 'event log files' over de activiteiten en het gedrag van eindgebruikers. Deze logbestanden bevatten ook informatie over de activiteiten van de beheerders.'

Voorbeelden van *diagnostische gegevens* - zie pg 25:
• *apparaatinformatie*, zoals het hardwaremodel, de versie van het besturingssysteem, unieke apparaat-ID's en informatie over het mobiele netwerk, inclusief het telefoonnummer van de gebruiker;
• *loggegevens*, inclusief details over hoe een gebruiker onze service heeft gebruikt, informatie over 'device event information' en het IP-adres van de eindgebruiker;
• *locatie-informatie,* zoals bepaald door verschillende technologieën, waaronder IP-adres, GPS en andere sensoren;
• *applicaties-informatie*, zoals applicatieversienummer; en

[1] Zie pg 47: "The G Suite for Education Core Services ("Core Services") are listed in the Services Summary and include Gmail, Calendar, Classroom, Contacts, Drive, Docs, Forms, Groups, Sheets, Sites, Slides, Talk/Hangouts, Vault, and Chrome Sync. These services are provided to a school under its G Suite for Education agreement and, as applicable, Data Processing Amendment. (Users and parents can ask their school if it has accepted the Data Processing Amendment.)". Bron.

• *browser-informatie*, zoals voorkeurstaal en andere instellingen. Info wordt verzameld en opgeslagen door cookies of vergelijkbare technologieën.

Samengevat - zie pg 25:
"We verzamelen informatie over de apps, browsers en apparaten die u gebruikt om toegang te krijgen tot Google-services, waardoor we functies kunnen bieden zoals automatische productupdates en het dimmen van uw scherm als uw batterij bijna leeg is. De informatie die we verzamelen omvat unieke identifiers, browsertype en instellingen, apparaattype en instellingen, besturingssysteem, mobiele netwerkinformatie inclusief providernaam en telefoonnummer, en applicatieversienummer. We verzamelen ook informatie over de interactie van uw apps, browsers en apparaten met onze services, inclusief IP-adres, crashrapporten, systeemactiviteit en de datum, tijd en verwijzende URL van uw gebruik.

Tenslotte: in een Appendix[2] van de Office 365 ProPlus DPIA, wordt "**telemetrie**" onderverdeeld in vier categorieën, vanuit een transparantie perspectief:

1. Telemetrie over essentiële diensten waarvoor geen opt-out bestaat
2. Telemetrie over vereiste diagnostische gegevens
3. Telemetrie die waarschijnlijk bij een Connected Experience horen
4. Telemetrie waarvoor geen openbare documentatie kon worden gevonden.

[2] Zie: Appendix 1 – Office Telemetry Events Observed at Levels Required and Neither, behorend bij: *DPIA Office 365 ProPlus v. 1905* (June 2019). Data protection impact assessment on the processing of diagnostic data.

Handreiking: Transfer Impact Assessment (TIA)

C. Juridisch kader: AVG
Het algemeen beginsel van de bescherming van persoonsgegevens bij doorgifte van persoonsgegevens vanuit de EU naar de VS ten behoeve van internationale samenwerking;

AVG Recital 101:

> “Verkeer van persoonsgegevens van en naar landen buiten de Unie en internationale organisaties is noodzakelijk voor de ontwikkeling van het internationale handelsverkeer en de internationale samenwerking. De groei van dit verkeer brengt nieuwe uitdagingen en aandachtspunten met zich voor de bescherming van persoonsgegevens. Wanneer persoonsgegevens echter van de Unie aan verwerkingsverantwoordelijken, verwerkers of andere ontvangers in derde landen of internationale organisaties worden doorgegeven, mag dit niet ten koste gaan van het beschermingsniveau waarvan natuurlijke personen in de Unie door deze verordening verzekerd zijn, ook in gevallen van verdere doorgiften van persoonsgegevens van het derde land of de internationale organisatie aan verwerkingsverantwoordelijken, verwerkers in hetzelfde of een ander derde land of in dezelfde of een andere internationale organisatie. Doorgifte aan derde landen en internationale organisaties mag in ieder geval alleen plaatsvinden in volledige overeenstemming met deze verordening. Een doorgifte kan alleen plaatsvinden indien de verwerkingsverantwoordelijke of de verwerker, onder voorbehoud van de andere bepalingen van deze verordening, de bepalingen van deze verordening met betrekking tot de doorgifte van persoonsgegevens aan derde landen of internationale organisaties naleeft.”.

AVG Recital 102:

> “Deze verordening doet geen afbreuk aan internationale overeenkomsten die de Unie en derde landen met elkaar hebben gesloten om de doorgifte van persoonsgegevens te regelen en waarin passende waarborgen voor de betrokkenen zijn opgenomen. De lidstaten kunnen internationale overeenkomsten sluiten over de doorgifte van persoonsgegevens naar derde landen of internationale organisaties, op voorwaarde dat dergelijke overeenkomsten deze verordening of andere bepalingen van Unierecht onverlet laten en een adequaat beschermingsniveau bieden voor de grondrechten van de betrokkenen.”

AVG Artikel 44:

> “Persoonsgegevens die worden verwerkt of die zijn bestemd om na doorgifte aan een derde land of een internationale organisatie te worden verwerkt, mogen slechts worden doorgegeven indien, onverminderd de overige bepalingen van deze verordening, de verwerkingsverantwoordelijke en de verwerker aan de in dit hoofdstuk neergelegde voorwaarden hebben voldaan; dit geldt ook voor verdere doorgiften van persoonsgegevens vanuit het derde land of een internationale organisatie aan een ander derde land of een andere internationale organisatie. Alle bepalingen van dit hoofdstuk worden toegepast opdat het door deze verordening voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd.”

Juridisch kader: SCCs
SCC’s Recital 20

> “The parties should take account, in particular, of the specific circumstances of the transfer (such as the content and duration of the contract, the nature of the data to be transferred, the type of recipient, the purpose of the processing), the laws and practices of the third country of destination that are relevant in light of the circumstances of the transfer and any safeguards put in place to supplement those under the standard contractual clauses (including relevant contractual, technical and organisational measures applying to the transmission of personal data and its processing in the country of destination).” Bron: Standard contractual clauses for international transfers, EN Standard Contractual Clauses.

Handreiking: Transfer Impact Assessment (TIA)

D. Bronnen

1. Algemene Verordening Gegegevensbescherming (AVG). 27 april 2016.
   Online: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=en

2. Arrest van het Hof van Justitie van De Europese Unie (CJEU), 16 juli 2020. Zaak: Case C-311/18. ECLI:EU:C:2020:559. *De 'Schrems 2' uitspraak.*
   Online: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=NL&mode=lst&dir=&occ=first&part=1&cid=9745404

3. European Data Protection Board (EDPB), Roadmap: Applying the principle if accountability to data transfers in practice.
   Ensuring compliance with the level of protection required under EU law of personal data transferred to third countries. Infographic.
   Online: https://twitter.com/EU_EDPB/status/1326538247980249092?s=20 en https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/infographic_data_transfers.pdf

4. European Data Protection Board (EDPB), *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.*
   Adopted on 10 November 2020. Online: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

5. European Data Protection Board (EDPB), *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*.
   Version 2.0 Adopted on 18 June 2021. Online: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

6. Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad. *De "SCCs".*
   Online: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32021D0914&from=EN

7. Christopher Kuner, *The Schrems II judgment of the Court of Justice and the future of data transfer regulation*. 17 juli 2020.
   Online: https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

8. Christopher Kuner, *Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection*.
   University of Cambridge Faculty of Law Research Paper No. 20/2021. Online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827850

9. Kuner, Christopher and Bygrave, Lee A. and Docksey, Christopher and Drechsler, Laura and Tosoni, Luca, *The EU General Data Protection Regulation: A Commentary.*
   Update of Selected Articles (May 4, 2021). Available at SSRN: https://ssrn.com/abstract=3839645 or http://dx.doi.org/10.2139/ssrn.3839645

10. Tekst & Commentaar. *Privacy- en gegevensbeschermingsrecht*, Onder redactie van: prof. mr. G.J. Zwenne en prof. mr. H.R. Kranenborg. Wolters Kluwer, 7e druk, 2020.
    Tevens geraadpleegd: de online versie, gebaseerd op de zevende druk, publicatie januari 2021, bijgewerkt tot en met ten minste 1 april 2021.

11. Congressional Research Service, *Foreign Intelligence Surveillance Act (FISA): An Overview*. April 6, 2021. Online: https://fas.org/sgp/crs/intel/IF11451.pdf