Transfer Impact Assessment (TIA)

Use Case 1. *Studeren in de VS obv een uitwisselprogramma*

1. Beschrijving van het probleem
De doorgifte van persoonsgegevens van EU studenten naar de VS, ten behoeve van een uitwisselingsprogramma of stage bij een universiteit in de VS, vergt, sinds het privacy shield ongeldig is verklaard, aanvullende actie van de instelling van deze student, die namelijk moet waarborgen en aantonen dat de bescherming van de hierbij te verwerken persoonsgegevens een passend beschermingsniveau hebben, dat in essentie gelijk is aan de waarborgen zoals gesteld in de AVG.

2. Identificeer het juridisch mechanisme voor doorgifte van persoonsgegevens op basis waarvan de doorgifte rechtmatig is.
Antwoord: Standaardbepalingen inzake gegevensbescherming (Standard Contractual Clauses)
Zie voor onderbouwing de Root Cause Analysis hieronder: *Corrective Action 1*.

3. Is het juridisch mechanisme in de praktijk effectief (‘*in practice and in full*’) bij de organisatie die de data importeert?
Antwoord: Ja
Zie voor onderbouwing de Root Cause Analysis hieronder: *Corrective Action 2*.

4. Zijn aanvullende maatregelen nodig?
Antwoord: Neen (zie: *Corrective Action 3*, hieronder.)
Zie voor onderbouwing de Root Cause Analysis hieronder: *Corrective Action 3*.

Disclaimer
De SURF Taskforce Beyond Privacy Shield heeft bovenstaand advies opgesteld naar aanleiding van de generieke use case. Dit advies is bedoeld als handreiking voor de instellingen die zelf deze afweging dienen te maken. In de concrete verwerking kunnen specifieke aspecten van de verwerking aanleiding geven tot een andere afweging. De instelling blijft zelf verantwoordelijk voor deze afweging.

ROOT CAUSE ANALYSIS

PRODUCT/PROCESS	1. Studeren in de VS obv een uitwisselprogramma	COMPLETED BY	SURF Taskforce Beyond Privacy Shield	QUALITY REVIEW BY	Quality Assurance CSCs d.d.	DATE	5 VII 2021

DEFINE THE PROBLEM

De doorgifte van persoonsgegevens van EU studenten naar de VS, ten behoeve van een uitwisselingsprogramma of stage bij een universiteit in de VS, vergt, sinds het privacy shield ongeldig is verklaard, aanvullende actie van de instelling van deze student, die namelijk moet waarborgen en aantonen dat de bescherming van de hierbij te verwerken persoonsgegevens een passend beschermingsniveau hebben, dat in essentie gelijk is aan de waarborgen zoals gesteld in de AVG.

WHY IS THIS A PROBLEM?

PRIMARY CAUSE — ****NOTE: If the final "Why" has no controllable solution, return to the previous "Why."** — **ROOT CAUSE**

Why is it happening?	Why is that?	Why is that?	Why is that?	Why is that?
Met de ongeldigverklaring van het Privacy Shield is een einde gekomen aan een juridisch mechanisme om gegevens uit te wisselen tussen EU en VS. Instellingen moeten hun afspraken met VS instellingen herzien en aanpassen.	De VS kan namelijk niet geacht worden om aantoonbaar voldoen aan de afspraken rondom bescherming van persoonsgegevens van EU studenten, vanwege conflicterende nationale wetgeving zoals FISA, voor de diensten die onder de scope van FISA vallen.	FISA vereist dat instellingen desgevraagd alle persoonsgegevens van alle niet VS ingezetenen verstrekken aan VS overheidsdiensten. Dit conflicteert met de AVG op de principes van doelbinding en proportionaliteit. Tevens kunnen EU studenten hun AVG rechten niet effectief uitoefenen.	Er is voor het Privacy Shield framework weliswaar een ombudsman, maar deze heeft niet de juiste bevoegdheden die het voor EU ingezetenen mogelijk maakt hun zogenaamde rechten van betrokkenen uit te oefenen.	De VS stelt andere eisen aan bescherming van persoonsgegevens dan de EU, en deze zijn in essentie niet equivalent, zoals de EU eist. AVG Art. 45 (Doorgiften op basis van adequaatheidsbesluiten) is voor EU-VS doorgiften van persoonsgegevens niet meer van toepassing.

* Bron 2: paragraaf 118, 201.

CONTRIBUTING PROBLEM — **ROOT CAUSE**

Why is it happening?	Why is that?	Why is that?	Why is that?	Why is that?
De instelling dient een inschatting te maken of de instelling in de VS redelijkerwijs geacht kan worden de verplichtingen zoals bepaald in de SCC volledig na te leven.	Nationale wetgeving kan VS instellingen dwingen gegevens van de uitwisselstudenten ter beschikking te stellen aan VS veiligheidsdiensten, in conflict met de SCCs	Echter, er zijn randvoorwaarden voor een dergelijk dwingen verzoek aan instellingen, namelijk dat er een reëel risico moet bestaan tav Nederlandse uitwisselstudenten.	De US AG DNI dienen 'uitwisselstudenten' als risico in zogenaamde certificaten te benoemen. Toetsing door de FISC. Pas na akkoord dwang tot verstrekking van gegevens.	Het is feitelijk onbekend wat de inhoud van de certificaten is. Zie ook bijvoorbeeld deze uitspraak van de FISC.

* Bron 2: paragraaf 34

* Zie: definitie 7: FISA

CORRECTIVE ACTION TO TAKE

CORRECTIVE ACTION 1	REMARKS	REMARKS	REFERENCES
EU-VS uitwisseling van persoonsgegevens kan wel op basis van AVG Art. 46, door gebruik te maken van de zogenaamde Standard Contractual Clauses (SCCs), waar nodig (zie: "Contributing Problem" hieronder) aangevuld met aanvullende waarborgen. AVG Art 46 lid 2.c.: 'Standaardbepalingen inzake gegevensbescherming die door de Commissie zijn vastgesteld'.			

* Bron 2: paragraaf 203 lid 4.

CORRECTIVE ACTION 2	REMARKS WITH REGARDS TO RISK ASSESSMENT	REMARKS WITH REGARDS TO RISK ASSESSMENT	REFERENCES
Redelijkerwijs kan de kans laag geacht worden dat uitwisselstudenten uit Nederland, immers een VS bondgenoot, door de AG en de DNI als risico worden bestempeld.	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.	Communicatie met een VS ingezetene (ontvanger / zender) mag *niet* onderschept worden op basis van FISA.	Zie FISA, section 702 lid b. sub 4: waarin de 'limitations' de rechten van de VS ingezetenen beschermen.

ROOT CAUSE ANALYSIS

CONTRIBUTING PROBLEM				ROOT CAUSE
Why is it happening?	Why is that?	Why is that?	Why is that?	Why is that?
De instelling dient een inschatting te maken of, naast de SCCs, aanvullende waarborgen vereist zijn voor de EU-VS doorgifte van persoonsgegevens.	zie hierboven	zie hierboven	zie hierboven	zie hierboven

* Bron 2: paragraaf 34

CORRECTIVE ACTION 3	REMARKS	REMARKS WITH REGARDS TO RISK ASSESSMENT	REFERENCES
Zie hierboven. Op basis daarvan zijn aanvullende maatregelen redelijkerwijs niet nodig. Data minimalisatie en encryptie tijdens transport en opslag zou redelijkerwijs moeten volstaan.	De instelling is gehouden (AVG art 5.1.a) om de betrokkene tijdig en volledig te informeren over de doorgifte van diens persoons-gegevens en de risico's hierbij voor de betrokkene.	De relatie tussen academische instellingen in de context van uitwisselprogram ma's is te kenmerken als wederzijds voordelig. Het is in het belang van de reputatie van de instellingen om elk	

CONTRIBUTING PROBLEM				ROOT CAUSE
Why is it happening?	Why is that?	Why is that?	Why is that?	Why is that?
De instelling dient een inschatting te maken van de risico's voor de student, 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 uitwisselstudenten aan een instelling 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), of, op basis van 'Afwijking-en voor specifieke situaties' (AVG art 49).	SCCs kunnen redelijkerwijs geacht worden nageleegd te worden door de VS instellingen tbv uitwisseling van studenten (zie hierboven). Doorgifte van persoonsgegevens kan dus plaatsvinden, 'as a rule', op basis van SCCs, en in uitzonderings-gevallen mogelijk op basis van expliciete toestemming van de NL uitwissel-studenten.		

* Bron 6: overweging 20

* Bron 1: AVG Hst V.

CORRECTIVE ACTION 4	REMARKS	REMARKS WITH REGARDS TO RISK ASSESSMENT	REFERENCES
De NL instelling kan zich, 'as a rule' beroepen op de SCCs als mechanisme voor doorgifte van persoonsgegevens. De NL instelling kan besluiten zich te beroepen op AVG Art 49: "Afwijkingen voor specifieke situaties", gegeven de aard en de omvang van de voorgenomen verwerking van persoonsgegevens tbv uitwisseling en de inschatting van de risico's voor de student.		Indien de instelling besluit zich voor de doorgifte van persoons-gegevens van de student (tbv uitwisseling en huisvesting) te beroepen op AVG art. 49 dan legt de instelling een groter deel van de verant-woordelijkheid van de verwer-king neer bij de student zelf, dan ten opzichte van het beroep op de SCCs (AVG art 46).	

ROOT CAUSE ANALYSIS

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 die deel willen nemen aan een uitwisselingsprogramma met een instelling in de VS) 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.”

ROOT CAUSE ANALYSIS

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, 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.".

ROOT CAUSE ANALYSIS

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.”

ROOT CAUSE ANALYSIS

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