Schrems II: déjà vu all over again

Zwenne, G.J.; Eijk, B.D.P. van der

Schrems II: Deja Vu All Over Again

Prof mr. G-J. (Gerrit-Jan) Zwenne is hoogleraar Recht en de informatiemaatschappij te Leiden en advocaat te Den Haag en Mr. B.D.P. (Berend) Van der Eijk is advocaat te Den Haag. De beide auteurs zijn redacteur van dit tijdschrift.

De Schrems II uitspraak is uitgebreid besproken in verschillende vaktijdschriften en andere media.[1] De uitspraak was niet onverwacht maar leidde wel tot vele praktische en meer principiële vragen over wat we moeten met gegevensbescherming in een wereld waarin landsgrenzen er steeds minder toe doen. In deze bijdrage gaan we in op de uitspraak, geven we onze gedachten over de betekenis ervan en wat we ermee aan moeten.

§1. Inleiding

We doen Max Schrems tekort als we hem alleen maar opvatten als een privacy rockstar.[2] Ongetwijfeld is niet iedereen het eens is met zijn opvattingen over privacy en gegevensbeschermingsrecht, maar onomstreden is dat de door hem en zijn ngo 'none of your business' ("noyb") begonnen procedures grote impact hebben.[3] In zijn laatste zaak heeft het Hof van Justitie van de EU ("het Hof" en ook wel "HJEU") uitgemaakt dat PrivacyShield per direct ongeldig is, en ook dat de internationale doorgifte van persoonsgegevens niet zonder meer kan worden gebaseerd op de modelcontracten die zijn goedgekeurd door de Europese Commissie ("EC" en ook wel "de Commissie"). De uitspraak maakt het daarmee moeilijk, om niet te zeggen onmogelijk, om persoonsgegevens nog langer op de gebruikelijke wijze door te geven naar de ondernemingen in de VS en andere derde landen, die de diensten aanbieden waarvan velen van ons dagelijks gebruik maken. Dat is een probleem. Er is ons verzekerd dat er heel hard wordt gewerkt aan oplossingen. Of die er ook echt gaan komen, is de vraag. Wij laten ons graag verrassen maar hebben er een hard hoofd in. We vermoeden dat de EU en de VS, waar het gaat om de betekenis van privacyrechten, vooralsnog niet tot elkaar kunnen komen. We kunnen natuurlijk doen alsof dat wel kan, maar beter en realistischer lijkt het ons om er serieus rekening mee te houden dat ook de houdbaarheid van een opvolger Privacy Shield beperkt blijkt.

[1] Zie bijv. HJEU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559 mt. W.A.M. Steenbruggen en S.I. van Harten, *Computerrecht* 2020/183, afl. 5 en Ö. Zivali en E. Thole, Privacy & Informatie 2021/2 (nog te verschijnen).

[2] Zie bijv. David Carrol, 2019 Year Review, Medium 22 december 2019, te vinden via https://medium.com/@profcarroll/2019-year-review-5dda8a0e198f (laatst. geraadpl, 7 februari 2021)

[3] HJEU 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650; HJEU 25 januari 2018, C-498/16, ECLI:EU:C:2018:37; HJEU 16 juli 220, C-311/18, ECLI:EU:C:2020: 559

G-J. Zwenne & B.D.P.van der Eijk. 'Schrems II: déjà vu all over again'. Tijdschrift voor internetrecht 2021/1. p. 1-5

In deze bijdrage bespreken we eerst de achtergrond van het laatste Schrems-arrest (§2), waarna we ingaan op het eerste Schrems-arrest, zgn. Schrems I (§3) en vervolgens op het de laatste door hem uitgelokte arrest, Schrems II (§4). In de afsluitende paragraaf verkennen we wat we met de uitspraak aanmoeten (§5).

§2. Achtergrond

Voor de bescherming van persoonsgegevens in de Europese Unie geldt de vuistregel: garantie tot aan de deur, en een beetje ook daarbuiten. De uniewetgever heeft alleen directe invloed op het beschermingsniveau van persoonsgegevens in de Europese Unie ("EU") en de Europese Economische Ruimte ("EER"). Om omzeiling van de regels in de EU en EER uit te sluiten, zijn er regels voor de doorgifte naar landen daarbuiten, de zgn. derdelanden. Deze komen erop neer dat, uitzonderingen daargelaten, ervan wordt uitgegaan dat er geen persoonsgegevens mogen worden doorgegeven naar derdelanden zonder een adequaat of passend beschermingsniveau.

Om te bepalen of een derdeland een passend beschermingsniveau biedt voorziet artikel 45 van de Algemene Verordening Gegevensbescherming (AVG) in de mogelijkheid van adequaatheidsbesluiten. In dergelijke besluiten stelt de Commissie vast dat een bepaald derdeland, of specifieke deel daaruit of een sector daarvan, voldoende waarborgen biedt voor een passend beschermingsniveau. Het resultaat is dat ernaar zo een derdeland wél persoonsgegevens kunnen worden doorgegeven zonder dat daarvoor extra beperkingen gelden of moet worden gezorgd voor aanvullende waarborgen, zoals goedgekeurde modelcontracten of bindende bedrijfsvoorschriften. Er zijn nu dertien adequaatheidsbesluiten, waarvan twaalf nog zijn vastgesteld onder de Richtlijn 95/46/EG en één onder de AVG. De betreffende derdelanden bevinden zich in een bont gezelschap van enerzijds economische grootmachten en belangrijke handelspartners van de EU, zoals Canada, Japan en Switzerland en anderzijds Europese ministaatjes zoals de Faeröer-eilanden, Jersey en Andorra.[4]

De Verenigde Staten (VS) zijn de grootste handelspartner van de EU. Om deze reden is er vooral behoefte aan een adequaatheidsbesluit voor de VS. Dat bleek echter nog niet zo gemakkelijk. Al snel na de introductie van de Richtlijn 95/46/EG kwam de Commissie tot de conclusie dat dit niet zonder meer mogelijk was. In de VS is geen sprake van federale omnibus privacywetgeving en zoals bekend beschikken de autoriteiten aldaar over verregaande bevoegdheden om toegang te verkrijgen tot persoonsgegevens. Dit, en de geringe bereidheid om daar iets aan te doen, maakten het onmogelijk voor de Commissie om te concluderen dat er in de VS kan worden gesproken van een passend beschermingsniveau. Uiteindelijk kwam er echter toch en adequaatheidsbesluit, niet voor de hele VS maar voor aldaar gevestigde ondernemingen die zichzelf op basis van 'Safe Harbour' hadden gecertificeerd. Een

[4] Zie voor meer achtergrondinformatie in dit tijdschrift: .BD.P. van der Eijk, 'De proeve van adequaatheid: over adequaatheidsbesluiten in het algemeen en het Japanse adequaatheidbesluit in het bijzonder', *TvIR* 1/2020.

G-J. Zwenne & B.D.P.van der Eijk. 'Schrems II: déjà vu all over again'. Tijdschrift voor internetrecht 2021/1. p. 1-5

doorgifte naar zo een onderneming werd opgevat als doorgifte naar een onderneming in een land met een passend beschermingsniveau.[5]

De gegevensdoorgifte naar derdelanden zonder adequaatheidsbesluit is onder voorwaarden mogelijk, maar vereist 'passende waarborgen'. De bekendste voorbeelden van dergelijke waarborgen zijn de modelcontracten (in het jargon: *Standard Contractual Clauses* of *SCC's*) en de bindende bedrijfsvoorschriften (*Binding Corporate Rules* of *BCR's*). Het doel van deze waarborgen is om de ontvangende partijen in derdelanden (d.w.z. de gegevensimporteurs) te committeren aan de privacybeginselen waarop de AVG is gebaseerd.

De op dit moment gebruikte modelcontracten piepen en kraken aan alle kanten. Ze zijn opgesteld in een andere tijd, zo'n tien tot vijftien jaar geleden, onder Richtlijn 95/46/EG, en ontberen een aantal van de waarborgen die inmiddels in de AVG verankerd zijn. Daarbij zien de modelcontracten alleen op de gegevensdoorgiften van verwerkingsverantwoordelijke naar verwerkingsverantwoordelijke (*controller-to-controller* d.w.z. C2C) en van verwerkingsverantwoordelijke naar verwerker (*controller-to-processor* d.w.z C2P), en niet op de doorgiften van verwerker naar verwerker (*processor-to-processor* d.w.z. P2C) of van verwerker naar verwerkingsverantwoordelijke (*processor-to-controller* d.w.z. P2C).[6]

Toch zijn de modelcontracten onverminderd populair en vinden veruit de meeste doorgiftes plaats op basis daarvan. Een verklaring daarvoor kan worden gevonden in de ogenschijnlijke eenvoud en het veronderstelde gebruiksgemak ervan. Er valt vrijwel niets te wijzigen aan de modelcontracten. Het enige wat partijen moeten opnemen is een kernachtige beschrijving van de gegevensverwerkingen (Annex 1) en de genomen beveiligingsmaatregelen (Annex 2).

Ten slotte geeft artikel 49 AVG nog een aantal derogaties of uitzonderingen voor de gevallen waarin er geen adequaatheidsbesluit is en waarin ook geen gebruik kan worden gemaakt van passende waarborgen. Een voorbeeld is de van de betrokkene te verkrijgen toestemming voor de doorgifte. Andere voorbeelden hebben betrekking op doorgiften die nodig zijn voor juridische procedures of voor uitvoering van een overeenkomst. Een beroep daarop is alleen mogelijk als er sprake is van Incidentele en niet-repetitieve doorgiften, wat uitsluit dat er in veel situaties gebruik van kan worden gemaakt.[7]

[5] Zie daarover O.L. van Daalen, 'Het Schrems/Facebook-arrest en de gevolgen voor internationale doorgifte', *NtER* 2016-3, p. 75-80.

[6] Voor doorgiften van verwerker naar verwerker of verwerkingsverantwoordelijke wordt ofwel gebruik gemaakt van vertegenwoordigingsconstructies, waarbij de verwerker namens de verwerkingsverantwoordelijke een modelcontract afsluit. Ook wordt wel gebruik gemaakt van een door toezichthouders goedgekeurd ad hoc modelcontract, zie bijvoorbeeld de door Microsoft aangepaste en door de Artikel 29 Werkgroep goedgekeurde modelcontracten, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf.

[7] EDPB, Richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679, 25 mei 2018.

§3. Schrems I

In 2013 ging er een schokgolf door de wereld na de onthullingen van Edward Snowden. Het was weliswaar allang algemeen bekend dat de autoriteiten in de VS, waaronder de National Security Agency (NSA), het Federal Bureau of Investigation (FBI) en de Central Intelligence Agency (CIA), op ongekend grote schaal online communicatie afluisteren,[8] maar zowel de omvang en de wijze waarop dit gebeurt verrasten alles en iedereen. Max Schrems, indertijd nog student, is op dat moment verwikkeld in een juridische strijd met Facebook. Gealarmeerd door de nieuwe onthullingen diende hij een klacht in bij de Ierse toezichthouder, de Irish Data Protection Commisioner (IDPC).[9] Schrems klaagde erover dat Facebook de persoonsgegevens van gebruikers in de unie doorgaf naar VS, waarna deze gegevens in voorkomende gevallen beschikbaar kwamen voor voornoemde autoriteiten. Schrems meende dat dat dit in strijd was met de beginselen van internationale doorgifte van persoonsgegevens onder de Richtlijn 95/46/EG.

Facebook en de IDPC zagen dat anders. Voor de doorgifte maakte Facebook gebruik van het eerdergenoemde Safe Harbour regeling en volgens de Commissie bood die een passend beschermingsniveau. Het Hof kon zich daarin niet vinden en verklaarde dat Safe Harbour ongeldig, onder andere omdat deze regeling overheidsinmenging niet afdoende beperkt, niet voorziet in rechtsmiddelen voor personen die toegang willen krijgen tot op hun betrekking hebbende gegevens of die gegevens willen laten wissen of wijzigen.

§4. Schrems II

Velen, waaronder wellicht Max Schrems zelf, meenden dat de Ierse privacytoezichthouder, na de ongeldigverklaring van Safe harbour, actie moest ondernemen tegen de doorgifte van persoonsgegevens door Facebook naar de VS en deze gegevensdoorgifte moest verbieden. Wat Schrems niet wist, maar wellicht wel had kunnen weten,[10] was dat Facebook voor de gegevensdoorgifte naar de VS ook gebruik maakte van modelcontracten. Toen dit duidelijk werd herformuleerde Max Schrems, inmiddels afgestudeerd in Wenen, zijn klachten. Zijn standpunt was dat ook de modelcontracten geen passende bescherming kunnen bieden en dat deze daarom geen basis kunnen bieden voor de gegevensdoorgifte. Onder verwijzing naar artikel 4 van het besluit 2010/87 van de Commissie voor de modelcontracten (verantwoordelijke-verwerker), deed Schrems aan de IDPC het verzoek om de doorgifte van Facebook naar de VS te verbieden

In het onderzoek en ontwerpbesluit dat daarop volgde, heeft de IDPC de bevindingen van Schrems grotendeels overgenomen. De toezichthouder kwam tot de voorlopige conclusie

[8] Zie bijvoorbeeld de NSA surveillance scene in: '*The Simpsons Movie'* (Gracie Films 20th Century Fox 2007), alsmede Tim Wu, *The Masterswitch*, Atlantic Books, 2010.

[9] Zie www.europe-v-facebook.org, geraadpleegd op 17 januari 2021.

[10] De IDPC zou dit al sinds 2013 weten, beweert NOYB, de door Max Schrems opgerichte NGO zie https://noyb.eu/en/project/eu-us-transfers, geraadpleegd op 1 november 2020.

dat de modelcontracten inderdaad onvoldoende waarborgen bieden tegen privacyaantastingen die de autoriteiten in de VS kunnen begaan op grond van de aldaar geldende surveillance-wetgeving. Echter, in de Schrems I zaak had het Hof van Justitie al uitgemaakt dat het niet aan toezichthouders is om een bindend oordeel te geven over de geldigheid van adequaatheidsbesluiten en de SCC-besluiten. De IDPC maakte daarom een procedure aanhangig bij het Ierse Hooggerechtshof, het High Court, dat vervolgens uiteindelijk elf prejudiciële vragen stelde aan het HvJEU. De antwoorden op deze vragen volgden op 16 juli 2020, in het arrest dat de we inmiddels aanduiden als Schrems II.

Modelcontracten.

Als het Safe Harbour-besluit ongeldig is omdat het geen passende bescherming kan bieden, moet dat dan ook niet gelden voor het besluit waarin de Europese Commissie de modelcontracten goedkeurde die worden gebruikt om persoonsgegevens door te geven naar de VS? Max Schrems vond van wel en velen met hem. Zo ver gaat het Hof evenwel niet. Het laat de modelcontracten in stand, maar legt wel een zware last op de schouders van organisaties die ervan gebruik maken, de zgn. gegevensexporteurs. Voorafgaand aan de gegevensdoorgifte moeten zij het recht en de praktijk van het betrokken derdeland (*"the law and practices in force in the third country concerned*') beoordelen, in het bijzonder wanneer in dat derdeland de autoriteiten wordt toegestaan in te grijpen in de rechten van de betrokkenen en er niet is voorzien in de 'passende waarborgen, 'afdwingbare rechten' en 'doeltreffende rechtsmiddelen' die artikel 46 AVG verlangt. In deze situaties moeten de gegevensexporteurs aanvullende maatregelen nemen die verder gaan dan die welke in de modelcontracten zijn vervat, om op die wijze het noodzakelijke passende beschermingsniveau te waarborgen.

Het doel van dergelijke aanvullende maatregelen is dat de gegevensexporteur en -importeur tekortkomingen in de gegevensbescherming van een derde land compenseren. Dit om een beschermingsniveau te waarborgen dat 'in grote lijnen overeenkomst met' ('*are essentially equivalent'*) het niveau dat wordt gewaarborgd door de AVG. Het Hof pas daarmee dezelfde toets toe als in het Schrems I arrest, waarin was geoordeeld dat een adequaatheidsbesluit de toets doorstaat wanneer de gegevensbescherming van het voorgenoemde niveau is, en verwijst daarbij 'ter inspiratie' voor het beoordelen van de rechtsbescherming van dat derde land naar artikel 45, tweede lid, AVG, de bepaling op grond waarvan de Commissie kan beoordelen in hoeverre een derdeland een passend beschermingsniveau biedt. Het Hof zegt dus met zoveel woorden dat de bescherming op grond van modelcontracten, al dan niet aangevuld met verdere maatregelen, niet mag onderdoen aan de bescherming van doorgifte naar een derde land waarvan het beschermingsniveau door de Commissie adequaat wordt geacht. In het geval van een doorgifte onder de modelcontracten moet deze beoordeling echter niet zoals bij de adequaatheidsbesluiten door de Commissie worden gedaan maar door de organisaties die gebruik wensen te maken van de modelcontracten.

Afsluitend concludeert het Hof onder verwijzing naar de AG, die volgens het Hof tot dezelfde conclusie komt, dat een bevoegde toezichthouder verplicht is om een doorgifte naar een derde land op grond van modelcontracten op te schorten of te verbieden, wanneer hij meent dat de modelcontracten niet worden nageleefd of kunnen worden nageleefd in het

derdeland en de door het unierecht vereiste bescherming niet kan worden gewaarborgd met andere middelen. Opmerkelijk is dat het Hof daarbij voorbij lijkt te gaan aan een nuancering die de AG in zijn conclusie maakte, namelijk dat bevoegde toezichthouders 'in een voorkomend geval' daartoe gehouden zijn. Zo een nuancering lijkt toezichthouders in de praktijk meer ruimte geven om al dan niet op te treden tegen een mogelijk onrechtmatige gegevensdoorgifte naar een derdeland.

Privacy Shield

Waar Schrems II het gebruik van de modelcontracten nog toelaatbaar acht, zij het onder voorwaarden, is het Hof onverbiddelijk over Privacy Shield. Anders dan de AG komt het Hof van Justitie tot het oordeel dat PrivacyShield, evenals haar voorganger SafeHarbour, onmiddellijk ongeldig is. Dit omdat de waarborgen voor de toegang tot en gebruik van uit Europa afkomstige persoonsgegevens door Amerikaanse overheidsinstanties niet overeenkomen met de minimumwaarborgen uit het unierecht. De surveillance programma's PRISM en Upstream volgend uit Section 702 Foreign Intelligence Surveillance Act[11] (FISA) en Executive Order 12333[12] (E.O. 12333) zijn niet in overeenstemming met het evenredigheidsbeginsel en niet beperkt tot hetgeen strikt noodzakelijk is. En daarbij stelt deze Amerikaanse wetgeving geen beperkingen aan de bevoegdheid om surveillanceprogramma's ten behoeve van inlichtingendiensten uit te voeren, en evenmin waarborgen bevatten voor niet-Amerikaanse personen tegen wie deze programma's mogelijk zijn gericht. Zo verlenen zij Europese betrokkenen geen voor de rechter afdwingbare rechten jegens de Amerikaanse autoriteiten.

Het Hof stelt ook vast dat de door de Amerikanen in het leven geroepen 'Privacy Shield Ombudsman' niet in staat is de door de Commissie zelf vastgestelde leemten in de effectieve rechterlijke bescherming van Europese betrokkenen op te vullen. Zo is de onafhankelijkheid van de Ombudsman als onderdeel van het Amerikaanse ministerie van Buitenlandse Zaken onvoldoende gewaarborgd. En hoewel de Ombudsman schendingen van het Privacy Shield kan vaststellen, blijkt nergens uit dat de Ombudsman in staat is om bindende beslissingen te nemen in dat kader.

[11] 50 U.S.C. § 1881. *Section 702* FISA maakt het mogelijk om buitenlandse inlichtingen te verkrijgen via personen die buiten de VS verblijven en vormt als gezegd de grondslag voor de bewakingsprogramma's PRISM en UPSTREAM. In het kader van het PRISM-programma zijn internetproviders verplicht de NSA alle communicatie van en naar een "*selector*" (zoals een bepaald email adres of profiel) te verstrekken, waarvan sommige gegevens ook aan de FBI en de CIA worden doorgegeven. Het UPSTREAM-programma concentreert zich op telecommunicatiebedrijven en de infrastructuur die zij beheren en exploiteren. Deze bedrijven moeten de NSA in staat stellen om gegevens en internetverkeersstromen te kopiëren en te filteren teneinde communicatie te verkrijgen van, naar of over een niet-Amerikaans persoon die in verband wordt gebracht met een "*selector*".

[12] E.O. 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8 December 1981). E.O. 12333 geeft de NSA toegang tot gegevens "*in transit*" naar de Verenigde Staten, door toegang te verkrijgen tot onderzeese kabels op de bodem van de Atlantische Oceaan, en deze gegevens te verzamelen en te bewaren voordat zij in de Verenigde Staten aankomen en aldaar aan FISA worden onderworpen.

§5. It's Deja Vu All Over Again[13]

In Schrems I werd Safe Harbour ongeldig verklaard. In Schrems II gebeurde hetzelfde met de opvolger daarvan: Privacy Shield. In de beide gevallen hebben we gezien hoe de Commissie vrijwel meteen opgewekt en enthousiast met het Department of Commerce in de VS in overleg treedt over het optuigen van nieuwe kaders voor de doorgifte van persoonsgegevens naar de VS. En vanzelfsprekend gebeurt dat weer in nauwe samenwerking (*'working closely together'*) met alle gegevensbeschermingsautoriteiten in de unie, en met het Comité voor gegevensbescherming (beter bekend onder de Engelse aanduiding "European Data Protection Board" of "EDPB"). We twijfelen er niet aan dat er inderdaad op termijn gaan komen met een nieuw arrangement dat vast en zeker weer wordt bekendgemaakt onder een vertrouwenwekkende aanduiding (wat denkt u van DataProtectionShelter? Of PrivacyGuard? PrivacyProphylactics?).

De vraag is of hoe duurzaam zo een nieuw arrangement gaat zijn. Wij hebben er een hard hoofd in. Waarom? Omdat het ons voorkomt dat de EU en de VS het op een nogal fundamenteel niveau niet eens zijn over de betekenis en het belang van privacybescherming, met als te verwachten gevolg dat ook de opvolger van PrivacyS hield wederom een moeilijk te verdedigen compromis gaat worden. De nieuwe oplossing voorziet ongetwijfeld in nieuwe en misschien wel heel innovatieve waarborgen, die met een beetje goede wil zo kunnen worden uitgelegd dat er inderdaad sprake is van 'een beschermingsniveau dat in grote lijnen overeenkomt met dat binnen de rechtsorde van de unie'. Maar we weten dat de praktijk weerbarstig is, en dat het Hof gelet op de overwegingen in Schrems II, niet geneigd is erg soepel om te gaan met de door de uniewetgever vastgelegde minimumnormen. Wij voorzien dat, als puntje bij paaltje komt, ook het nieuwe arrangement de verwachtingen niet gaat waarmaken.

Wat dan? Wij denken dat het beter is te erkennen dat de EU en de VS het niet eens zijn. En om te onderkennen dat een nieuw arrangement daarin weinig tot niets gaat veranderen. We moeten ermee leren leven dat de EU alleen regels kan stellen voor de EU-lidstaten en soms ook voor landen daarbuiten, maar niet voor alle landen in de hele wereld en al helemaal niet voor landen met een vergelijkbare of grotere economische of geopolitieke betekenis in de wereld. Voor vele landen kan de EU onderhandelen vanuit een overwichtspositie en dat kan haar in staat stellen om de voorwaarden af te dwingen die maken dat onze persoonsgegevens worden beschermd op een wijze die wij passend achten. Voor enkele landen moeten we met tegenzin erkennen dat de onderhandelingspositie van de EU niet zodanig is dat er in alle gevallen een passend beschermingsniveau kan worden bereikt. De EU kan er dan voor kiezen om alle gegevensdoorgifte naar dat derdeland te verbieden. Maar dat zal niet altijd haalbaar, ook al wordt af en toe wel gesuggereerd van wel -- u herinnert zich mis-

[13] De uitdrukking wordt toegeschreven aan baseball-speler Yogi Berra, bekend om zijn Yogi-isms. Zie https://en.wikipedia.org/wiki/Yogi_Berra#"Yogi-isms"

G-J. Zwenne & B.D.P.van der Eijk. 'Schrems II: déjà vu all over again'. Tijdschrift voor internetrecht 2021/1. p. 1-5

schien hoe de voorzitter van onze eigen nationale privacytoezichthouder, na Schrems I, dapper riep dat hij, als de VS niet onmiddellijk zou inbinden, al onze iPhone's op zwart zou zetten.[14]

Het is, denken wij, ondenkbaar dat de EU de gegevensdoorgifte naar de VS gaat stopzetten. Ook niet als er geen vervanging komt voor Privacy Shield. En ook niet of als een beoordeling van 'het recht en de praktijk' van de VS uitwijst dat er geen sprake is van een gegevensbescherming die in grote lijnen overeenkomt met die in de unie. We kunnen dan natuurlijk doen alsof. We kunnen weer een nieuw arrangement a la Privacy Shield en Safe Harbour optuigen, in de wetenschap dat ook dat nieuwe arrangement niet echt leidt tot het gewenste passende beschermingsniveau en met als onvermijdelijk gevolg dat ook dat arrangement over vijf-zes jaren door het Hof van Justitie ongeldig wordt verklaard.

Dat lijkt ons niet de weg vooruit. Wij denken dat het beter is om geen nieuw arrangement te hebben, dan te vertrouwen op een arrangement dat, als het erop aankomt, niet de bescherming biedt die het zegt te bieden en die het volgens het Hof wél moet bieden. Het is beter dat we ermee leren leven dat er landen zijn waar onze gegevens niet goed zijn beschermd. En dat we onderkennen dat, als onze gegevens naar deze landen worden doorgegeven, er risico's zijn dat die gegevens worden gebruikt op een wijze die wij in de unie niet zouden accepteren. Voor wie gelooft in gegevensbescherming is dat ontnuchterend. Maar door te doen alsof er wel sprake is van passende bescherming houden we onszelf voor de gek. En daarbij ontnemen we onszelf de mogelijkheid om zowel gegevensexporteurs en -importeurs als privacytoezichthouders erop aan te spreken dat onze gegevens in voorkomend geval toch niet goed worden beschermd.

De vraag is of het politiek-bestuurlijk haalbaar is dat Commissie en het Department of Commerce in de loop van dit jaar níet komen met de opvolger van Privacy Shield. Wat dat betreft maken we ons geen illusies. Het ligt in de lijn der verwachtingen dat er nog dit jaar een nieuw arrangement wordt bekendgemaakt. En we kunnen ervan uitgaan dat de Commissie weer met kracht van argumenten zal uiteenzetten dat dit arrangement deze keer wél een beoordeling door het Hof van Justitie kan doorstaan. We weten echter dat de Commissie, ondanks haar grote expertise en een omvangrijk juridisch apparaat, er inmiddels twee keer naast heeft gezeten.[15] We doen er daarom goed aan ons zijn minst erop voor te bereiden dat ook het nieuwe arrangement kwetsbaar is.

Voor gegevensexporteurs en -importeurs geldt dat ze ermee rekening moeten houden dat beschermingsniveaus in derdelanden kunnen tekortschieten, zelfs als gebruik wordt gemaakt van de waarborgen waarin de verordening voorziet en mogelijk zelfs als de Commissie

[14] Privacywaakhond CBP: 'Als het aan ons ligt zou je iPhone op zwart gaan' RTL-nieuws, 28 oktober 2015, te vinden via <www.rtlnieuws.nl/tech/artikel/3986751/privacywaakhond-cbp-als-het-aan-ons-ligt-zou-je-iphone-op-zwart-gaan>

[15] En het is ook de vraag of sommige andere adequaatheidsbesluiten de toets van het Hof (nog) kunnen doorstaan. Zo telt het adequaatheidsbesluit ten aanzien van Argentinië slechts vier pagina's aan overwegingen, wat mager afsteekt tegen de 58 pagina's van het Japanse adequaatheidsbesluit. Zie voor meer kritische overwegingen Paul Schwartz, 'Global Data Privacy: The EU Way', New York University Law Review 771/2019, p. 23.

heeft bepaald dat het desbetreffende derdeland een passend beschermingsniveau biedt. In dergelijke gevallen zijn er aanvullende maatregelen nodig. De EDPD heeft daarvoor suggesties gedaan. Het meest lijkt de EDPB te vertrouwen op technische maatregelen, zoals het met behulp van pseudonimisering onmogelijk maken dat de gegevens in het derdeland toegankelijk kunnen worden gemaakt. De gedachte is dan dat alleen de gegevensexporteur in de unie beschikt over de sleutel waarmee toegang kan worden verkregen tot de gegevens die zijn doorgegeven naar de gegevensinporteur in het derdeland.[16] Of daarmee de gegevens inderdaad voldoende zijn beschermd is vooralsnog onduidelijk, al was het maar omdat we ons kunnen voorstellen dat de gegevensimporteur in het derdeland door de autoriteiten aldaar wordt gedwongen om de gegevensexporteur in de unie te bewegen de sleutel zo nodig toch te verstrekken. En daarbij kunnen we ervan uitgaan dat deze pseudonimisering in veel gevallen ten koste gaat van functionaliteit.

Intussen zien we dat de gegevensdoorgiften naar derdelanden worden beperkt of beëindigd, niet zozeer omdat er is vastgesteld omdat daar geen sprake is van een passend beschermingsniveau, maar veeleer omdat dat vooralsnog onduidelijk is. Er is op dit moment daarom vooral behoefte aan informatie over welke derdelanden wel of niet een beschermingsniveau hebben dat in grote lijnen overeenkomt met dat in de unie, en welke soort van maatregelen gegevensexporteurs en importeurs kunnen nemen om de tekortkomingen in verschillende in derdelanden te verhelpen. We zijn er vooralsnog niet van overtuigd dat daarin gaat worden voorzien in de nieuwe door de Europese Commissie voorbereidde modelcontracten.[17]

[16] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf en, p. 22 ev.

[17] EC Draft Commission implementing decision (EU) …/… of XXX on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Brussels, XXX […](2020), te vinden via: < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries> (laatst. geraadp. 10 februari 2021)