Barsten in het EU-VS Privacy Shield

Het HvJ EU heeft het EU-VS Privacy Shield ongeldig verklaard. En nu?

Op 16 juli jl. heeft het Hof van Justitie van de Europese Unie (HvJ-EU) uitspraak gedaan in de langverwachte Schrems II zaak.[i] Het EU-VS Privacy Shield, wat de doorgifte van persoonsgegevens tussen Europa en de Verenigde Staten (VS) mogelijk maakt, is ongeldig verklaard. In deze factsheet staan wij stil bij de uitspraak van het HvJ-EU en bespreken we de mogelijke alternatieven voor organisaties.

In het kort

Het zal privacy professionals niet ontgaan zijn dat het HvJ-EU een baanbrekende uitspraak heeft gedaan over de uitwisseling van persoonsgegevens tussen de EU en de VS.[ii] Zij heeft het Amerikaans-Europese Verdrag Privacy Shield uit 2016 (EU-VS Privacy Shield) ongeldig verklaard.[iii] Deze uitspraak heeft vergaande gevolgen voor het bedrijfsleven, nu bedrijven zoals Facebook en Google de doorgifte van persoonsgegevens van hun Europese gebruikers op deze regeling hebben gebaseerd.

Het EU-VS Privacy Shield, waaronder de data-uitwisseling tussen de EU en de VS plaatsvindt, is ongeldig verklaard omdat dit verdrag niet voldoet aan de Europese regels voor databescherming. Het HvJ-EU is namelijk van mening dat de privacywetgeving die op dit moment geldt in de EU/EER de standaard zou moeten zijn indien persoonsgegevens naar landen buiten de EU/EER worden verstuurd. Dit betekent dat de Europese Commissie opnieuw in gesprek zal moeten gaan met de VS om tot een nieuw juridisch akkoord te komen dat de privacybescherming wel voldoende waarborgt. Daarnaast zullen bedrijven in kaart moeten brengen wat de alternatieven zijn om toch persoonsgegevens te kunnen blijven doorgeven aan de VS.

Wat is een doorgifte?

Een doorgifte kan worden omschreven als *"alle gevallen waarbij een verantwoordelijke een activiteit uitvoert met het doel persoonsgegevens beschikbaar te stellen aan een derde persoon die in een derde land is gevestigd"*.[iv] Duidelijk moet zijn dat een doorgifte veel breder moet worden gezien dan alleen het versturen van

persoonsgegevens van het ene naar het andere land. Bijvoorbeeld een persoon in een derde land die toegang heeft tot persoonsgegevens die zich in de EU/EER bevinden, valt ook onder een doorgifte. Belangrijk om te beseffen is dat de doorgifte van persoonsgegevens een verwerking is in de zin van de Algemene Verordening Gegevensbescherming (AVG).[v] Om te spreken van een rechtmatige verwerking, zal aan de vereisten vanuit de AVG moeten worden voldaan. Zo mag een doorgifte van persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden plaatsvinden en dient er een rechtsgeldige grondslag te zijn.

Voor lidstaten in de EU geldt dat het beschermingsniveau van persoonsgegevens tussen die lidstaten onderling gelijk is. Daarnaast hebben de landen die behoren tot de Europese Economische Ruimte (EER) ook een passend beschermingsniveau. Dit heeft tot gevolg dat doorgifte van persoonsgegevens binnen de EU/EER in beginsel is toegestaan. Voor landen buiten de EU/EER (ook wel 'derde landen' genoemd) gelden andere regels. Doorgifte van persoonsgegevens is dan alleen mogelijk indien dat derde land een passend beschermingsniveau waarborgt.

Hoofdstuk 5 van de AVG is gewijd aan doorgifte aan derde landen of internationale organisaties en stelt de voorwaarden waaronder het is toegestaan gegevens buiten de EU/EER te brengen.[vi] Derde landen die in hun nationale wetgeving een met de AVG vergelijkbaar beschermingsniveau bieden, worden geacht een passend niveau van gegevensbescherming te hebben.[vii] De Europese Commissie heeft de bevoegdheid om voor deze landen een adequaatheidsbeslissing te nemen.[viii] Deze beslissing kan voor het gehele land worden genomen, maar ook voor één of meerdere regio's of sectoren in een land.

In de VS bestaat geen algemene wetgeving die de bescherming van persoonsgegevens regelt. Om die reden wordt de VS niet geclassificeerd als land met 'een passend beschermingsniveau', oftewel, vergelijkbaar met het beschermingsniveau van de EU. Voor de doorgifte van persoonsgegevens naar de VS geldt om die reden een speciale regeling. De Europese Commissie heeft in 2016 het EU-VS Privacy Shield vastgesteld met als doel om bij de uitwisseling van persoonsgegevens met de VS een beschermingsniveau te waarborgen dat in grote lijnen overeenkomt met het niveau binnen de EU.[ix] Organisaties in de VS kunnen zich hiervoor certificeren indien zij laten zien dat zij een passend beschermingsniveau willen en kunnen waarborgen. Grote Amerikaanse bedrijven, zoals Amazon Inc., Google en Facebook Inc. zijn EU-VS Privacy Shield geregistreerd en op de lijst terug te vinden.[x]

De zaak Schrems II

De Oostenrijkse privacy activist Maximilian Schrems (Schrems) heeft een klacht over Facebook Ireland ingediend vanwege de doorgifte van persoonsgegevens van Facebook Ireland naar de servers van moederbedrijf Facebook Inc., gevestigd in de VS. Schrems heeft de Ierse toezichthouder verzocht de doorgiften naar de VS te verbieden en voerde aan dat de VS geen passende bescherming zou bieden omtrent de

naar het land door te geven gegevens.[xi] “Schrems II” is de tweede zaak over de verwerking van persoonsgegevens en doorgifte daarvan naar de VS door Facebook Ireland.

In 2015 heeft het HvJ-EU de voorloper van het Privacy Shield onderuitgehaald: ‘Safe Harbor’. In die uitspraak oordeelde het HvJ-EU dat Safe Harbor geen passende waarborgen bood voor de bescherming van de persoonsgegevens in de VS.[xii] Het gevolg hiervan was dat onder andere Facebook, Inc. geen persoonsgegevens meer kon doorgeven aan de VS op basis van Safe Harbor en daarom op zoek moest naar alternatieven die wel in overeenstemming waren met Europese privacywetgeving.

In de tussentijd lag de klacht, na terugverwijzing door het Hof, weer bij de privacy-toezichthouder in Ierland. Schrems stelde dat er door de VS geen adequate bescherming werd geboden voor zijn persoonsgegevens en dat zijn gegevens dus niet op een geldige manier konden worden doorgegeven aan Facebook, Inc. Het Ierse Hooggerechtshof heeft op 4 mei 2018 hierover maar liefst elf prejudiciële vragen gesteld aan het HvJ-EU. Onderdeel hiervan waren onder andere de vragen of de Modelcontracten van de Europese Commissie (Standard Contractual Clauses of SCCs) wel genoeg bescherming kunnen bieden en in hoeverre het ondertussen door de Europese Commissie opgetuigde EU-VS Privacy Shield ook een passend beschermingsniveau kan bieden.

In het Schrems II- arrest heeft het HvJ-EU op 16 juli 2020 het EU-VS Privacy Shield in zijn totaliteit ongeldig verklaard, waardoor per direct elke doorgifte van persoonsgegevens van de EU/EER naar bedrijven in de VS die zich hadden gecertificeerd middels het EU-VS Privacy Shield, onrechtmatig [xiii]

Het HvJ-EU heeft wel de bestaande regels omtrent de SCCs in stand gelaten omdat zij vindt dat de SCCs een passend beschermingsniveau waarborgen zoals in de AVG is vereist. Gevolg is dat de doorgifte van persoonsgegevens naar de VS alsnog mogelijk blijft onder de voorwaarden van de SCCs. Het is dan aan de nationale privacy toezichthouders om toe te zien op naleving van de SCCs.

Wat nu?

Nu het EU-VS Privacy Shield ongeldig is verklaard, is het de vraag welke mogelijkheden bedrijven in de EU/EER hebben om alsnog persoonsgegevens te kunnen delen met de VS. De beslissing van het Hof heeft onmiddellijke werking wat betekent dat bedrijven per direct in actie moeten komen om de onrechtmatigheid van de huidige doorgiften te kunnen opheffen.[xiv] Daarnaast is het voor organisaties ook van belang om per direct het privacybeleid aan te passen wanneer zij momenteel persoonsgegevens delen met de VS, zodat betrokkenen geïnformeerd blijven in de zin van artikel 13 en 14 AVG. Bovendien zijn er nog andere oplossingen om de ontstane onrechtmatige situatie weg te nemen.

1. Per direct stoppen met het doorgeven van persoonsgegevens aan de VS

Maar laten we eerlijk zijn, dit is voor veel organisaties geen reële optie. Organisaties

zullen eerst moeten onderzoeken of zij persoonsgegevens aan de VS doorgeven en welk instrument zij daarvoor gebruiken. Pas wanneer blijkt dat het EU-VS Privacy Shield voor de doorgifte is gebruikt, zal er een alternatief instrument moeten worden aangewend of gestopt worden met de doorgifte. De voor- en nadelen van het per direct stoppen met delen van persoonsgegevens met de VS:

Voordeel:

- Je voldoet aan de eisen die de AVG stelt.

Nadelen:

- De gegevensverwerking kan in beginsel niet meer plaatsvinden.
- Het bestaande proces moet per direct worden aangepast om de impact op de dagelijkse bedrijfsvoering weg te nemen.

2. Doorgaan met het doorgeven van persoonsgegevens zonder verder iets te doen

Wanneer er op korte termijn geen reële alternatieven zijn kan ervoor worden gekozen vooralsnog niks te veranderen aan de huidige werkwijze en de ontwikkelingen in de politiek en bij de nationale privacy toezichthouders af te wachten. Organisaties lopen hiermee wel een juridisch risico omdat de Autoriteit Persoonsgegevens hierover onverwijld geïnformeerdedient te worden. De Autoriteit Persoonsgegevens kan namelijk een boete opleggen indien bij een doorgifte geen sprake is van een passend beschermingsniveau in een derde land. De basisboete voor het doorgeven van persoonsgegevens zonder passende waarborgen is €525.000 op grond van de beleidsregels van de Autoriteit Persoonsgegevens. Zeker voor kleine organisaties kan het risico voor een dermate hoge boete een overweging zijn om niet voetstoots door te gaan. De voor- en nadelen van het doorgaan met het delen van persoonsgegevens met de VS:

Voordelen:

- De gegevensverwerking gaat gewoon door.
- Er hoeven geen aanpassingen aan het proces plaats te vinden en de impact op de dagelijkse bedrijfsvoering is nihil.

Nadelen:

- Je dient de Autoriteit Persoonsgegevens onverwijld te informeren.
- Je voldoet niet aan de eisen die de AVG stelt.
- Je riskeert een (hoge) boete van de Autoriteit Persoonsgegevens.
- Je riskeert reputatieschade.

3. BCR (Binding Corporate Rules of Bindende Bedrijfsvoorschriften) afsluiten

Met BCR legt een organisatie intern geldende waarborgen vast voor de bescherming van persoonsgegevens bij doorgifte naar landen zonder passend beschermingsniveau, zoals de VS. Dergelijke BCR moeten in overeenstemming zijn met de AVG en de privacyregelgeving in elk land waarin verwerking van persoonsgegevens plaatsvindt. De Europese privacy toezichthouders moeten daarnaast de BCR voorafgaand goedkeuren.[xv] Het grote voordeel van BCR is dat hiermee een uniform geldende set van regels binnen een multinationale organisatie geldt en de organisatie niet steeds naar geldende regelgeving per land moet kijken. Er kleven echter ook nadelen aan BCR. Door de vereisten die aan BCR worden gesteld kan het

lang duren voordat BCR volledig is goedgekeurd. Alleen al in Nederland bedraagt de huidige doorlooptijd van BCR momenteel minimaal 5 jaar. Daarnaast zijn de kosten voor het samenstellen van BCR erg hoog en zeker kleine- en middelgrote dataverwerkingsbedrijven (65 procent van het totaal) hebben vaak niet de middelen om een door de EU goedgekeurde set van BCR op te stellen.[xvi] BCR zijn voor de meeste organisaties dan ook geen betaalbare optie. De voor- en nadelen van het gebruik van BCR's:

Voordeel:

- Geharmoniseerde set van privacyregels binnen verschillende (internationale) takken van organisaties en/of multinationals waarmee tevens voldaan wordt aan de AVG.

Nadelen:

- Geldt niet voor bedrijven of organisaties die geen deel uitmaken van dezelfde groep.
- Zeer tijdrovend om BCR op te stellen en goedgekeurd te krijgen.
- Het opstellen van BCR is erg kostbaar.

4. De betrokkene om uitdrukkelijke toestemming vragen[xvii]

Een betrokkene kan worden geïnformeerd over de risico's die verbonden zijn aan een doorgifte en het beschermingsniveau in het derde land waarna om diens toestemming als grondslag voor de doorgifte kan worden gevraagd.[xviii] De toestemming van betrokkene moet dan specifiek zien op de doorgifte van persoonsgegevens. De omstandigheid dat iemand bijvoorbeeld akkoord is met het verwerken van zijn persoonsgegevens voor marketingdoeleinden, wil niet zeggen dat diegene ook instemt met de doorgifte.[xix] De voor- en nadelen van toestemming:

Voordeel:

- Voldoet aan de vereisten van de AVG.

Nadelen:

- Bij een grote groep betrokkenen leidt dit tot een zware compliance last vanwege het beheer en onderhoud van rechtsgeldige toestemmingen.
- Een toestemming kan te allen tijde ingetrokken worden door de betrokkene waardoor ook de doorgifte van diens persoonsgegevens per direct beëindigd moet kunnen worden.

5. Het afsluiten van SCCs[xx]

Het HvJ-EU oordeelt in Schrems II dat de SCCs een doeltreffend mechanisme is waarmee een passend beschermingsniveau kan worden gewaarborgd.[xxi] Het Hof benadrukt dat de SCCs
de ontvanger en verstrekker verplichten om na te gaan of het beschermingsniveau in het derde land inderdaad kan worden gewaarborgd. Hiermee verbonden is de compliance verplichting dat indien
de ontvanger niet in staat blijkt het vereiste beschermingsniveau te kunnen naleven, hij de verstrekker hiervan in kennis dient te stellen. In dat geval is de verstrekker verplicht tot het opschorten en/of beëindigen van de overeenkomst met de ontvanger, waardoor de doorgifte van persoonsgegevens alsnog per direct moet worden gestopt.[xxii] Elke organisatie zal dus steeds voor zichzelf moeten beoordelen of de ontvanger in de VS een adequaat beschermingsniveau kan bieden.[xxiii] Een dergelijke inhoudelijke beoordeling is in deze tijden van snelle digitalisering en cloud computing echter niet

op eigen kracht haalbaar. Overigens moet worden opgemerkt dat de huidige SCCs nog gebaseerd zijn op de privacyrichtlijn uit 1995 en niet op de AVG. De Europese Commissie zal dus op korte termijn ook met een oplossing moeten komen voor deze tekortkoming.

De voor- en nadelen van het gebruik van SCCs:

Voordeel:

- Voldoet aan de vereisten van de AVG.

Nadelen:

- De SCCs zijn nog gebaseerd op de privacyrichtlijn uit 1995 en niet op de AVG.[xxiv]
- Elke verstrekker heeft een onderzoeksplicht en moet voor zichzelf beoordelen of de ontvanger in de VS een adequaat beschermingsniveau kan bieden.
- Niet elke ontvanger kan of wil instemmen met het gebruik van SCCs.

6. Migreren van persoonsgegevens naar de EU/EER bij dezelfde of een andere leverancier

Organisaties kunnen persoonsgegevens bij dezelfde leverancier laten migreren van de VS naar de EU/EER. Ook kunnen organisaties de persoonsgegevens laten migreren naar een andere leverancier binnen de EU/EER. Een risico bij dit laatste is echter wel dat in de EU/EER gevestigde serviceproviders hun diensten vaak weer uitbesteden met het oog op de kosten of om alsnog 24/7 services te kunnen leveren.[xxv] Dit kan ook naar derde landen, waaronder zelfs weer de VS zijn. Ook wanneer de gegevens zich op een server in de EU/EER bevinden, dient er gecontroleerd te worden of er niet alsnog onbedoeld doorgifte naar de VS plaatsvindt.[xxvi]

De voor- en nadelen van het migreren van persoonsgegevens:

Voordeel:

- Er is geen sprake meer van een doorgifte waardoor de onrechtmatigheid van de doorgifte is weggenomen.

Nadelen:

- Migratie bij dezelfde leverancier binnen de EU/EER is niet altijd mogelijk en dus geen keuze.
- In de EU/EER wordt niet altijd een vergelijkbare dienst aangeboden of tegen dezelfde kosten. Het is daardoor niet altijd mogelijk migratie naar een andere leverancier toe te passen of de migratie heeft vanwege de hogere kosten significante impact op de bedrijfsvoering.
- Doordat serviceproviders hun diensten vaak weer uitbesteden dient er gecontroleerd te worden of er niet alsnog onbedoeld een doorgifte naar de VS plaatsvindt.
- Een migratie voorbereiden kost tijd en dus geld.
- Een migratie kan tot fouten leiden in de overdracht van persoonsgegevens waardoor de kwaliteit van de persoonsgegevens wordt aangetast.

Tot slot

Schrems II heeft hoe dan ook per direct impact op organisaties die persoonsgegevens doorgaven onder de werking van het EU-VS Privacy Shield. Er zijn een aantal oplossingsrichtingen om de ontstane onrechtmatige situatie weg te nemen of de impact ervan te beperken. Iedere organisatie zal voor zichzelf moeten bepalen welke

oplossingsrichting het meest wenselijk en haalbaar is. Het meest aanbevelenswaardig lijkt het om überhaupt allereerst te onderzoeken of er doorgiften plaatsvonden onder het EU-VS Privacy Shield. Vervolgens kan er worden beoordeeld of met dezelfde ontvanger in de VS de SCCs kunnen worden afgesloten. Zijn de SCCs niet haalbaar dan is het raadzaam om te beoordelen of persoonsgegevens kunnen worden gemigreerd naar de EU/EER bij dezelfde of bij een andere ontvanger. Is geen van de genoemde stappen haalbaar, dan dient de Autoriteit Persoonsgegevens geïnformeerd te worden dat doorgiften blijven plaatsvinden zonder waarborgen. Het ligt overigens niet voor de hand dat de Autoriteit Persoonsgegevens er meteen met een 'gestrekt been' in zal vliegen bij organisaties die tot nog toe vertrouwden op de geldigheid van het EU-VS Privacy Shield.

Het voorgaande wordt bevestigd door de FAQ die het Europees Comité voor Gegevensbescherming publiceerde op 23 juli 2020 omtrent de praktische gevolgen van de uitspraak en de eventuele te nemen vervolgacties.[xxvii] Het laatste woord is echter nog niet gesproken omdat er op termijn nog verdere guidance vanuit het Comité zal worden gepubliceerd. Wij zullen u in ieder geval op de hoogte houden van de ontwikkelingen! Mocht u in de tussentijd vragen hebben over de gevolgen van de uitspraak van het HvJ-EU op uw organisatie, u kunt ons hiervoor altijd bereiken.

Gezonde groet,

Legal2Practice B.V.
+31 (0) 26 848 3118
info@legal2practice.nl

Geraadpleegde bronnen

[i] HVJ EU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).
[ii] Idem.
[iii] Uitvoeringsbesluit (EU) 2016 /1250 van de Commissie van 12 juli 2016 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming.
[iv] D. Alonso Blas, 'Nota derde landen. De doorgifte van persoonsgegevens naar derde landen in het kader van de WBP', *College Bescherming Persoonsgegevens* Den Haag februari 2003, p. 6/7.
[v] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46.
[vi] Art. 44-50 AVG.
[vii] Handleiding Algemene Verordening Gegevensbescherming (AVG), *Ministerie van Veiligheid* 22 januari 2018.
[viii] Art. 45 AVG.
[ix] Uitvoeringsbesluit (EU) 2016 /1250 van de Commissie van 12 juli 2016 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming.
[x] Privacy Shield List, Privacyshield.gov.
[xi] HvJ EU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).
[xii] HvJ EU 6 oktober 2015, C-362-14, ECLI:EU:C:2015:650 (*Schrems I*).
[xiii] HVJ EU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).
[xiv] Van Doorne, 'Steps organizations need to take for international data transfers following the Schrems II ruling', *Van Doorne* 22 juli 2020.
[xv] Autoriteit Persoonsgegevens, 'Binding corporate rules', Autoriteitpersoonsgegevens.nl.
[xvi] N. van Bemmel, 'EU-Hof tikt Commissie op de vingers: gegevens Europeanen in Amerika niet veilig', *Volkskrant.nl* 16 juli 2020.
[xvii] Art. 49 lid 1 onder a AVG
[xviii] Autoriteit Persoonsgegevens, 'Doorgifte binnen en buiten de EU', Autoriteitpersoonsgegevens.nl
[xix] Handleiding Algemene verordening gegevensbescherming (AVG), *Ministerie van Veiligheid en Justitie* 22 januari 2018.
[xx] Art. 46 lid 2 onder c AVG.
[xxi] HVJ EU 16 juli 2020, C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).
[xxii] Idem.
[xxiii] M. Pols, 'Hoogleraar over 'baanbrekende' EU-uitspraak delen persoonsdata: te grote opgave voor bedrijven', *Fd.nl*, 16 juli 2020.
[xxiv] Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
[xxv] Van Doorne, 'Steps organizations need to take for international data transfers following the Schrems II ruling', *Van Doorne* 22 juli 2020.
[xxvi] Idem.
[xxvii] Autoriteit Persoonsgegevens, 'Privacy Shield voor doorgifte naar VS ongeldig verklaard', *Autoriteitpersoonsgegevens.nl* 20 juli 2020.
European Data Protection Board, ´Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems´, https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf, 23 juli 2020.