LEGAL UPDATE

De consequenties van Schrems II voor de doorgifte van persoonsgegevens

Datum: 20 juli 2020

Inleiding
Op 16 juli 2020 heeft het Hof van Justitie van de Europese Unie ('HvJ EU') in de zaak C-311/18 ('Schrems II') het adequaatheidsbesluit van de Europese Commissie ('EC') voor de doorgifte van persoonsgegevens naar de Verenigde Staten op basis het zogenaamde 'Privacy Shield' ongeldig verklaard. Daarnaast heeft het HvJ EU overwogen dat de standaardbepalingen van de EC voor de doorgifte van persoonsgegevens naar derde landen ('SCC's') niet per definitie een passend beschermingsniveau waarborgen en het beschermingsniveau van een land per geval beoordeeld moeten worden. Dit arrest heeft grote gevolgen voor organisaties die persoonsgegevens doorgeven naar landen buiten de Europese Unie. In deze Legal Update worden Schrems II en de gevolgen van dit arrest voor de praktijk besproken.

Doorgifte van persoonsgegevens
Persoonsgegevens mogen alleen worden doorgegeven naar landen buiten de Europese Unie indien er wordt voldaan aan de voorwaarden van hoofdstuk 5 AVG. Doorgifte is onder meer mogelijk indien de EC heeft besloten dat een derde land een passend beschermingsniveau waarborgt, of, indien een dergelijk besluit ontbreekt, als er voor de doorgifte passende waarborgen worden geboden en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. Deze passende waarborgen kunnen worden geboden zonder toestemming van de toezichthouder door middel van een aantal instrumenten, waaronder SCC's en bindende bedrijfsvoorschriften ('BCR's'). In Schrems II bespreekt het HvJ EU wanneer er sprake is van een passend beschermingsniveau.

Hoe moet de mate van bescherming worden beoordeeld?
Het HvJ EU heeft de vraag beantwoord op welke manier de mate van bescherming moet worden getoetst en welke factoren overwogen moeten worden om de mate van bescherming in de context van een doorgifte te beoordelen. In het kort geeft het HvJ EU aan dat er niet aan nationale wetgeving van een lidstaat getoetst moet worden maar slechts aan het Handvest van de grondrechten van de Europese Unie ('Handvest'). Bij deze toets moet worden gekeken naar:

1. de overeenkomst tussen de partij in de EU die de gegevens doorgeeft (de verstrekker) en de partij buiten de EU waaraan de gegevens worden verstrekt (de ontvanger); en
2. de relevante aspecten van het rechtsstelsel van het derde land waar de persoonsgegevens zullen worden verwerkt. Hierbij dienen niet-limitatief de factoren in aanmerking worden genomen die zijn uiteengezet in artikel 45 lid 2 AVG (waaronder de rechtstatelijk, eerbiediging van de mensenrechten en de fundamentele vrijheden, effectief functioneren van toezichthoudende organen en internationale toezeggingen of overeenkomsten).

Privacy Shield
Met betrekking tot het Privacy Shield heeft het HvJ EU het rechtstelsel van de Verenigde Staten beoordeeld, in het bijzonder specifieke wetgeving met betrekking tot de bevoegdheden van de inlichtingendiensten (de Foreign Intelligence Surveillence Act, Executive Order 12333 en de Presidential Policy Directive 28). Het HvJ EU overweegt dat de rechten zoals uiteengezet in het Handvest niet absoluut zijn en dat een inbreuk op die rechten mogelijk is voor specifieke doeleinden en op de basis van een rechtmatige grondslag. Er moet dan wel sprake zijn van een zekere mate van proportionaliteit en verder moet de inbreukmakende maatregel zijn neergelegd in wetgeving die duidelijke en precieze regels stelt met betrekking tot de omvang en toepassing van de maatregel. Deze wetgeving dient een set aan minimale waarborgen te bieden om betrokkenen te beschermen. Volgens het HvJ EU wordt niet

aan deze vereisten voldaan: de wetgeving kent te weinig (i) beperkingen aan de macht die wordt gegeven en (ii) waarborgen om de rechten en vrijheden van niet-Amerikaanse burgers te beschermen. Betrokken hebben geen afdwingbare rechten en doeltreffende rechtsmiddelen tot hun beschikking. De Privacy Shield ombudsman heeft niet de bevoegdheid om bindende beslissingen te nemen waaraan inlichtingendiensten zich moeten houden. Om die reden heeft de EC niet de vereisten voor een passend beschermingsniveau in acht genomen en verklaart het HvJ EU het besluit van de Europese Commissie met betrekking tot het Privacy Shield ongeldig.

Bieden de SCC's een passende bescherming?
In het kort geeft het HvJ EU aan dat de SCC's een geldig instrument zijn om een doorgifte van persoonsgegevens naar een derde land mogelijk te maken. Echter, door het sluiten van de SCC's is niet per definitie sprake van een passend beschermingsniveau. De verstrekker dient, waar passend, met de ontvanger te bepalen of ook in de praktijk een passend beschermingsniveau kan worden geboden. Daarvoor dient te worden beoordeeld of er sprake is van wetgeving in het desbetreffende land waardoor de ontvanger wordt verhinderd om aan de SCC's te kunnen voldoen. Daarbij is ook van belang dat onder de SCC's de ontvanger, kort gezegd, de verplichting heeft om de verstrekker te informeren indien de verstrekker niet (meer) kan voldoen aan zijn verplichtingen onder de SCC's. Op basis hiervan kan de verstrekker vervolgens besluiten de doorgifte op te schorten, de overeenkomst te beëindigen en de verstrekker te verzoeken om vernietiging van de gegevens. De SCC's kunnen dus passende waarborgen bieden voor de doorgifte van persoonsgegevens volgens het HvJ EU, maar dit moet wel in de praktijk per geval getoetst worden.

Mag een toezichthouder de doorgifte verbieden?
Wat is nu precies de taak van de nationale toezichthouder, zoals de Autoriteit Persoonsgegevens ('AP')? Mag deze toezichthouder zelfstandig bepalen dat een bepaald land geen passend beschermingsniveau biedt en om die reden een doorgifte opschorten of verbieden? Het HvJ EU overweegt dat de toezichthouder de adequaatheidsbesluiten van de EC dient te respecteren en, totdat een dergelijk besluit ongeldig is verklaard, een toezichthouder geen maatregelen mag nemen die het adequaatheidsbesluit ondermijnen. Echter, de toezichthouder heeft volgens het HvJ EU wel ruimte om, bijvoorbeeld in kader van een klacht van een betrokkene, te onderzoeken of er in die specifieke situatie wel een passend beschermingsniveau wordt geboden en op basis van die bevindingen te handhaven.
Het bovenstaande is met name met betrekking tot de SCC's van belang. Het HvJ EU overweegt dat de toezichthouder wel mag onderzoeken of er door de ontvanger van de persoonsgegevens kan worden voldaan aan de SCC's. Indien blijkt dat de wetgeving in het land van de ontvanger zodanig is dat de ontvanger onder die wetgeving niet kan voldoen aan de normen, zoals uiteengezet in de SCC's (welke een passend beschermingsniveau moeten waarborgen), mag de toezichthouder de doorgifte opschorten of verbieden of op andere wijze handhaven. Daarbij merkt het HvJ EU wel op dat als een toezichthouder van mening is dat een doorgifte naar een bepaald land in het algemeen verboden dient te worden, hiervoor eerst de European Data Protection Board ('EDPB') gevraagd moet worden om een opinie te geven, om te voorkomen dat elk land een ander standpunt inneemt. De EDPB kan vervolgens een bindend besluit hierover nemen.

Betekenis voor de praktijk
Schrems II heeft directe, verregaande gevolgen voor de praktijk. Allereerst dat er geen persoonsgegevens mogen worden doorgegeven op basis van het Privacy Shield. Echter, een potentieel nóg ingrijpender gevolg is dat het nog maar zeer de vraag is of een doorgifte van persoonsgegevens naar de Verenigde Staten of andere derde landen op grond van de SCC's of BCR's nog wel is toegestaan.

Een doorgifte op basis van SCC's kan namelijk alleen als er in de praktijk wel een passend beschermingsniveau kan worden geboden door partijen. Het is aannemelijk dat een dergelijke norm ook geldt voor BCR's. Het Hof van Justitie geeft aan dat het beschermingsniveau aan dezelfde normen moet worden getoetst als de normen waaraan de EC het passend beschermingsniveau van een land moet

beoordelen (artikel 45 lid 2 AVG). Nu er door de HvJ EU, in het algemeen, is geoordeeld dat de wetgeving in de Verenigde Staten geen passend beschermingsniveau biedt en betrokkenen niet over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken, is het maar de vraag of in dit, in een specifiek geval, onder de SCC's (of bij BCR's) anders is.

Daarnaast zijn er nog wel een aantal andere landen denkbaar die waarschijnlijk geen passend beschermingsniveau kunnen bieden. Hoe moeten persoonsgegevens straks met deze landen worden uitgewisseld? Het gaat hier niet alleen om buitenlandse cloudoplossingen. Onze samenleving draait op het uitwisselen van persoonsgegevens tussen landen wereldwijd (van uitwisselingsstudenten en toerisme tot de zakelijke contacten, klantgegevens en werknemersgegevens van bedrijven ten behoeve van handel met die derde landen). Indien instrumenten zoals SCC's en de BCR's geen uitkomst bieden, worden de mogelijkheden om gegevens door te geven op grond van de AVG zeer beperkt en in bepaalde gevallen zelfs onmogelijk. Dit heeft verstrekkende politieke en economische gevolgen.

Het ligt in de lijn der verwachting dat de meeste bedrijven blijven vertrouwen op de SCC's (of BCR's) in de hoop dat de soep niet zo heet gegeten zal worden als die nu door het HvJ EU lijkt te zijn opgediend. Daarbij kan nog worden verwezen naar de bepaling in de SCC's waarin staat dat de ontvanger van de gegevens, kort gezegd, verplicht is om de verstrekker te informeren indien de verstrekker niet (meer) kan voldoen aan zijn verplichtingen onder de SCC's. Echter, als de ontvanger van de persoonsgegevens niet piept, betekent dat niet dat de verstrekker geen verantwoordelijkheid draagt. Volgens het HvJ EU ligt de verantwoordelijkheid voor de beoordeling of sprake is van een passend beschermingsniveau namelijk (ook) bij de verstrekker. Dit impliceert dat als de ontvanger zijn verplichtingen onder de SCC's niet nakomt doordat er geen passend beschermingsniveau kan worden geborgd, de verstrekker nog steeds verantwoordelijk kan worden gehouden door de toezichthouder voor een schending van de AVG door de verstrekker.

Uit Schrems II blijkt dat de toezichthouder (in Nederland: de AP) ruimte heeft om in specifieke gevallen doorgiftes naar derde landen te verbieden of op andere wijze te handhaven, zoals door het opleggen van een boete. Indien de AP besluit op basis van Schrems II (specifieke) doorgiftes naar derde landen te gaan onderzoeken, riskeren organisaties niet alleen dat de doorgifte zal worden verboden indien er geen passend beschermingsniveau kan worden geboden, maar (dus) ook (reputatie)schade en boetes. De basisboete voor het doorgeven van persoonsgegevens zonder passende waarborgen is EUR 525.000,- op grond van de beleidsregels van de Autoriteit Persoonsgegevens.

Het verdient om die reden aanbeveling om geen afwachtende houding aan te nemen maar zelf onderzoek te doen naar de passendheid van het beschermingsniveau. Ten eerste dient te worden geïnventariseerd of er sprake is van doorgifte van persoonsgegevens en op basis van welk instrument dit plaatsvindt. Indien doorgiftes worden gebaseerd op het Privacy Shield, SCC's of een ander instrument dat is opgesomd in artikel 46 lid 2 AVG, zoals BCR's, verdient het aanbeveling om het beschermingsniveau te onderzoeken. Daarbij dient het recht van het derde land te worden getoetst aan het Handvest. Met name dient te worden gekeken of de wetgeving een zekere mate van proportionaliteit kent en dat maatregelen die inbreuk maken op de rechten van betrokkenen in wetgeving is vastgelegd. Deze wetgeving dient duidelijke en precieze regels te stellen met betrekking tot de omvang en toepassing van de maatregel. Van belang is voorts dat betrokkenen afdwingbare rechten en doeltreffende rechtsmiddelen tot hun beschikking hebben. Indien hier geen sprake van is verdient het aanbeveling om te onderzoeken of het mogelijk is om de doorgifte te laten plaatsvinden op basis van een uitzonderingsgrond zoals vastgelegd in artikel 49 AVG, zoals toestemming van de betrokkenen of de noodzaak om de persoonsgegevens door te geven voor de uitvoering van de overeenkomst met betrokkene.

Indien u vragen heeft over doorgifte van persoonsgegevens kunt u altijd contact met ons opnemen.

Dit is een Legal Update van Elze ’t Hart.

Voor meer informatie:

Elze ’t Hart
+31 30 25 95 578
elzethart@vbk.nl