INTERNATIONALE DOORGIFTE PERSOONSGEGEVENS

Analyse & stappenplan

Versie 1.0
Lucine Pogosian & Robin Kuijken

Cuccibu, auteurs Lucine Pogosian & Robin Kuijken
CucciBook Internationale doorgifte persoonsgegevens

Uitgegeven door Cuccibu, Nederland

INHOUD

Inhoud

INTRODUCTIE

Op 16 juli 2020 heeft het Hof van Justitie van de Europese Unie het EU-US Privacy Shield ongeldig verklaard. Hiernaast is besloten dat de Standard Contractual Clauses (SCC) een geldig instrument is om doorgifte van persoonsgegevens naar een derde land mogelijk te maken. Een kanttekening hierbij is dat het ondertekenen van een SCC niet automatisch een passend beschermingsniveau biedt.

In dit infoboekje wordt ingegaan op de zaak Schrems ll en de mogelijke gevolgen van de ongeldigheidsverklaring van het Privacy Shield. Daarnaast bevat dit infoboekje een stappenplan waarin wordt weergeven wat er op dit moment kan worden gedaan door organisaties die persoonsgegevens doorgeven aan, of uitwisselen met organisaties in de VS of andere derde landen buiten de Europese Unie (EU) of Europese Economische Ruimte (EER).

Reduce Risk. Create Value!

SCHREMS II

Wat houdt de zaak Schrems II in?
Het Hof van Justitie van de Europese Unie (hierna: het Hof) heeft uitspraak gedaan over onder andere het EU-US Privacy Shield, de opvolger van het Safe Harbor-regime. Het Safe Harbor-regime was in 2016 al ongeldig verklaard door het Hof (Schrems I) en nu ondergaat het Privacy Shield hetzelfde lot.

Het Privacy Shield was een adequaatheidsbesluit van de Europese Commissie waarmee doorgifte van persoonsgegevens naar de VS toegestaan was. Als hoofdregel van de Algemene verordening gegevensbescherming (hierna: AVG) geldt namelijk dat persoonsgegevens niet zomaar naar derde
landen mogen worden verstuurd. Adequaatheidsbesluiten voor Canada, Japan en Zwitserland blijven nog wel geldig.

Nationale wetgeving VS & waarborgen
In de zaak Schrems II is het Hof tot de conclusie gekomen dat het Privacy Shield onvoldoende mogelijkheden biedt aan betrokkenen uit de EU om hun rechten op het gebied van dataprotectie uit te oefenen. Daarnaast was het Hof kritisch op nationale wetgeving die conflicterend zou zijn met EU-wetgeving. Wetgeving als FISA 702 en EO 12.333 in de VS zijn voorbeelden van wetten die niet voldoen aan in de AVG vastgelegde waarborgen. Het Hof stelt dat bepaalde surveillance programma's overheidsinstanties toegang geven in persoonsgegevens vanuit de EU om veiligheidsredenen. Maar deze bevoegdheid heeft onvoldoende/geen beperking en bestaan er geen garanties voor betrokkenen buiten de VS. Betrokkenen uit de EU zouden namelijk geen mogelijkheid hebben om naar de Amerikaanse rechter te stappen, als zij denken dat hun persoonsgegevens onrechtmatig worden verwerkt door overheidsinstanties in de VS.

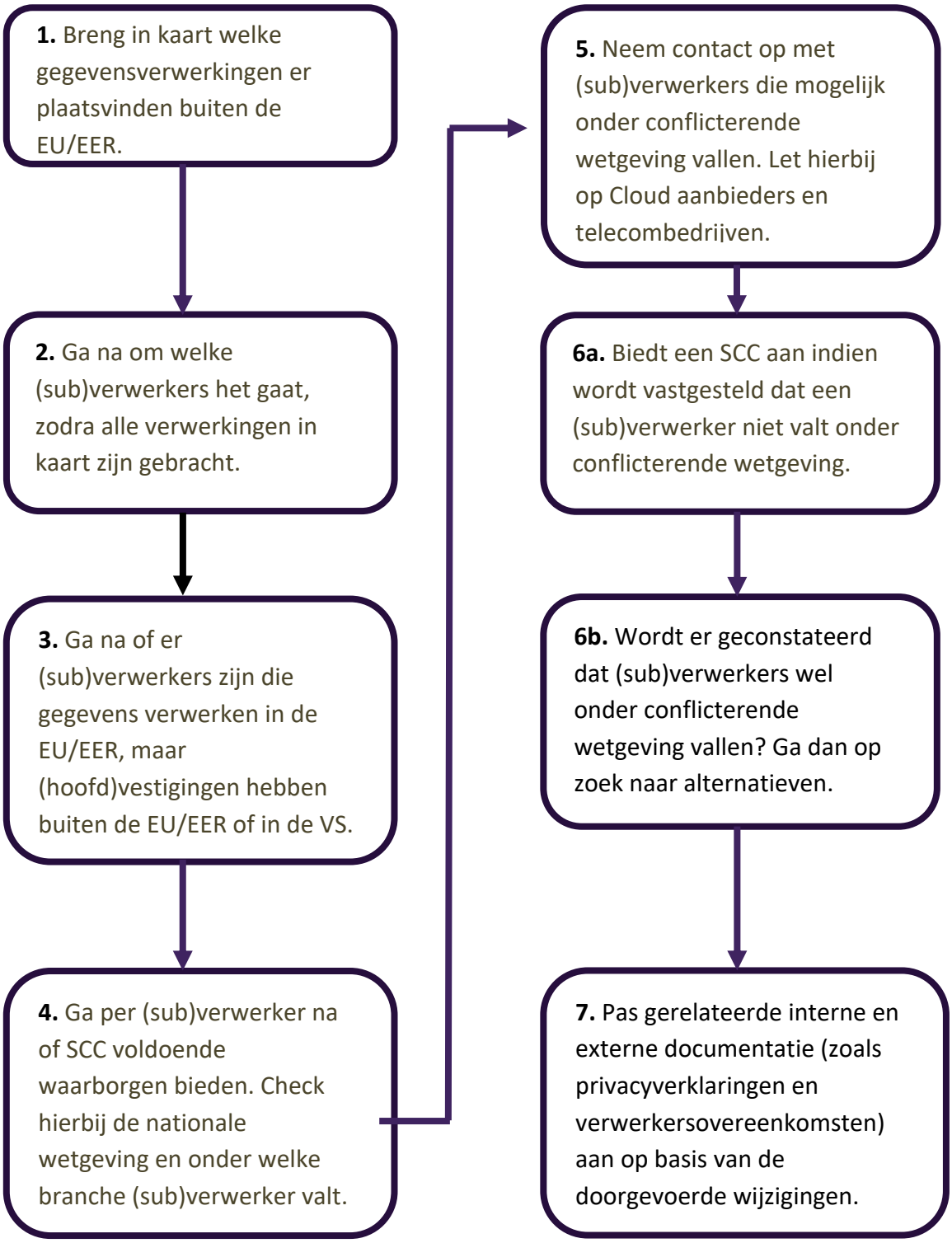
Standard Contractual Clauses
Naast het Privacy Shield heeft het Hof ook de SCC's beoordeeld. Het Hof heeft bepaald dat SCC's wel een geldig doorgiftemechanisme blijven. Wel moet rekening worden gehouden met het feit dat ook SCC's niet zonder meer gebruikt kunnen worden voor doorgifte naar de VS en landen buiten de EER. Er dient namelijk alsnog onderzocht te worden per geval of er voldoende waarborgen worden geboden. Hierbij geldt dat het beschermingsniveau van nationale wetgeving van het derde land in acht moet worden genomen. Er zouden volgens het Hof anders additionele maatregelen genomen moeten worden, maar wat die maatregelen precies inhouden is vooralsnog onduidelijk.

Uitzonderingen artikel 49 AVG
Artikel 49 AVG bevat uitzonderingen voor specifieke gevallen die onder omstandigheden gebruikt kunnen worden om doorgifte te laten plaatsvinden naar een derde land dat niet voldoende waarborgen biedt. Een kanttekening hierbij is dat vrijwel geen van de uitzonderingen uit artikel 49 AVG geschikt zijn voor herhaalde of systematische verwerkingen.

Wat voor gevolgen heeft de uitspraak en wat kun je nu doen?
Nu er - ook blijkend uit het advies van de European Data Protection Board (EDPB) - geen overgangsfase bestaat, zijn alle doorgiftes naar de VS onder het Privacy Shield per direct onrechtmatig. Dit houdt in dat organisaties direct alle doorgiftes onder het Privacy Shield onder de loep moeten nemen en moeten bepalen of zij doorgifte op basis van een ander mechanisme kunnen laten plaatsvinden.

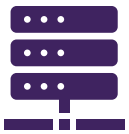
STAPPENPLAN

Onderstaand stappenplan kan gebruikt worden door organisaties die persoonsgegevens doorgeven aan, of uitwisselen met organisaties in de VS of landen buiten de EU/EER, om te kijken of doorgifte naar deze landen voldoen aan de regels.



UITWERKING STAPPENPLAN

1. Maak een **inventarisatie** van jouw internationale data transfers. Hierbij is het van belang om vast te stellen of er sprake is van doorgifte van persoonsgegevens en op basis van welk instrument dit plaatsvindt. Stel een team op en betrek zo nodig afdeling Inkoop, IT, privacy en/of legal om dit samen te doen.



2. Zorg dat alle **verwerkers**, maar ook **subverwerkers** in kaart worden gebracht.

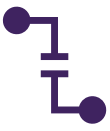
3. Het is van belang dat ook (sub)verwerkers die **(hoofd)vestigingen** hebben in de VS of buiten de EU/EER worden meegenomen in dit proces.

4. Check per (sub)verwerker of zij vallen onder nationale wetgeving die conflicteert met de AVG. Voor de VS geldt dat **telecomproviders** en **Cloud aanbieders** in ieder geval vallen onder **conflicterende wetgeving**. Dit zijn (in ieder geval) FISA 702 en EO12.333.

5. Zorg ervoor dat (sub)verwerkers **schriftelijk** bevestigen of ontkennen dat zij onder conflicterende wetgeving vallen. Vergeet niet om na te gaan of een (sub)verwerker gebruik maakt van bijvoorbeeld een Cloud aanbieder die wel onder conflicterende wetgeving valt (zie ook stap 3).

6a. Als na onderzoek blijkt dat een (sub)verwerker niet valt onder conflicterende wetgeving, kan het gebruik van **SCC** (of Binding Corporate Rules) een oplossing bieden.

6b. Valt een (sub)verwerker wel onder conflicterende wetgeving? Zorg ervoor dat de data transfer wordt **stopgezet**. Hierbij is het van belang dat er een **exit-plan** komt. In geval van subverwerkers kan er contact opgenomen worden met de verwerker om bezwaar te maken.



7. Zorg ervoor dat **interne documenten** geüpdatet worden waar nodig. Communiceer ook intern dat dit is gebeurd.

TIPS

Hieronder volgen nog enkele tips bij het stappenplan en bij het aangaan van nieuwe overeenkomsten waarbij doorgifte plaatsvindt naar derde landen.

- Probeer om niet noodzakelijke doorgifte richting de VS en andere niet-EU/EER landen, waarvoor geen adequaatheidsbesluit bestaat, zoveel mogelijk te beperken.

- In sommige gevallen zijn cloudoplossingen buiten de EU/EER goedkoper dan die binnen de EU/EER. Echter moet worden aangetoond dat je als organisatie een actieve rol hebt ingenomen in het onderzoeken en controleren van voldoende waarborgen in de jurisdictie van de andere partij. Houd hierbij dus rekening met de extra compliance kosten die erbij komen kijken.

De basisboete voor het doorgeven van persoonsgegevens zonder passende waarborgen is €525.000!

- Zorg ervoor dat je kunt aantonen dat er een actieve rol is geweest in het onderzoeken of er voldoende waarborgen zijn als je toch besluit om in zee te gaan met partijen buiten de EU/EER of uit de VS.

- Check bij bestaande verwerkingen de hele keten. Dit houdt in verwerkers en hun subverwerkers. Let vooral ook op de eventuele Cloud aanbieders die verwerkers gebruiken.

Andere (duurdere) alternatieven voor hosting in Europa? Ga voor Europese aanbieders.

- Hoe zit het met grote bedrijven die vestigingen in Europa hebben (Amazon, Google, Microsoft)? Organisaties zijn verantwoordelijk voor het vaststellen dat bedrijfsinterne datastromen richting de VS/niet-EU/EER land, voldoen aan de AVG. Dit houdt in dat er actief gevraagd moet worden of en hoe deze datastromen plaatsvinden.

SLOTWOORD

De (EDPB) heeft guidelines en een FAQ gepubliceerd naar aanleiding van de uitspraak van het Hof in de zaak Schrems II. De verwachting is dat de Europese Commissie in de toekomst meer duidelijkheid zal geven, maar tot die tijd wordt alle verantwoordelijkheid gelegd bij organisaties zelf. Om de gevolgen en risico's te beperken is het advies om niet meer te wachten, maar om direct te handelen.

Wil je meer informatie over de gevolgen en risico's van de uitspraak Schrems II of over wat je als organisatie nu al kunt doen?

Neem dan contact op via **info@cuccibu.nl | +31 (0) 85 303 2984.**

Reduce Risk, Create Value!

In een wereld die in toenemende mate digitaliseert, zorgt Cuccibu ervoor dat de onbegrensde mogelijkheden van deze wereld worden benut op een verantwoorde en veilige manier. Cuccibu helpt organisaties met vraagstukken op het vlak van informatiebeveiliging, privacy, cyber security en audit/compliance. Onze professionals op deze gebieden hebben de achtergrond en ervaring om met creatieve en heldere oplossingen iedere organisatie, groot of klein, te helpen!