# Schrems II: welke mitigerende maatregelen moet je nemen?

## En welke maatregelen moet je treffen als gevolg van deze uitspraak?

In dit artikel nemen we jullie mee in de gevolgen van de Schrems II-uitspraak.

- Daarvoor gaan we eerst in op de privacy by design afwegingen die je opnieuw moet maken;
- Vervolgens introduceren we het stappenplan van de European Data Protection Board (EDPB) aanbeveling 01/2020 & EPDB aanbeveling 02/2020;
- Ten slotte sluiten we af met een checklist waarmee je een inschatting kunt maken van de impact van de Schrems II-uitspraak voor jouw organisatie. De checklist is gebaseerd op de ISACA Privacy Principles.

Door: Menno Borst en Piet Dekker

# SCHREMS II

Schrems II refereert aan de uitspraak van het Hof van Justitie van de Europese Unie (HvJ-EU)) op de klacht van dhr. Schrems. Hij was van mening dat Facebook in onvoldoende mate de beveiliging van zijn persoonsgegevens kan garanderen zodra Facebook zijn persoonsgegevens transporteert van Ierland (EEU) naar Amerika, gebaseerd op het toenmalige transportmechanisme “Privacy Shield” tussen Europese Unie (EU) en Verenigde Staten (VS). Specifiek betreft het de mogelijkheid van de Amerikaanse overheidsinstanties om toegang te krijgen tot persoonsgegevens van Europese ingezetenen die door Amerikaanse organisaties worden verwerkt.
In juli 2020 heeft het Europese Hof van Justitie in de casus Schrems II (C-311/18) besloten dat het tot dan toe geldende “Privacy Shield” voor onbeperkte datatransport van persoonsgegevens tussen EU en de US niet langer voldeed aan de GDPR-vereisten. De Amerikaanse wetgeving biedt onvoldoende waarborgen om deze persoonsgegevens adequaat te beveiligen.

## ISACA Privacy Principles

Binnen onze beroepsorganisatie worden ook privacy-ontwikkelingen over de gehele wereld bijgehouden. Dit heeft in 2016 geleid tot de publicatie “ISACA Privacy Principles and Program Management Guide”. In deze publicatie zijn naast privacy risico’s ook de vereisten per regio en sommige landen opgenomen. Om zorg te blijven dragen voor een overzichtelijke aanpak van privacy is gekozen voor privacy principes die aansluiten bij het Cobit2019 Framework.
In dit artikel nemen we jullie mee in de gevolgen van Schrems II:

- Allereerst betekent dat het opnieuw maken van de privacy by design afwegingen.
- Vervolgens introduceren we het stappenplan van de European Data Protection Board (EDPB) aanbeveling 01/2020 & EPDB aanbeveling 02/2020;
- Ten slotte sluiten we af met een inschatting van de impact op basis van een pragmatische checklist gebaseerd op de ISACA Privacy Principles.

## Privacy by design

Alvorens in te gaan op de verschillende aanbevelingen blijft het voor elke organisatie de vraag of het daadwerkelijk nodig is om persoonlijke informatie te verwerken voor het primaire doel van de verwerkingsactiviteit. De wetgever nodigt iedere organisatie uit, om binnen de bedrijfsprocessen te controleren of het mogelijk is om zonder gebruik van de persoonsgegevens te werken, op een alternatieve wijze gebruik te maken van persoonsgegevens dan wel op een voldoende gelimiteerde wijze persoonsgegevens te verwerken.
Zodra er is vastgesteld dat deze verwerking adequaat, relevant en voldoende gelimiteerd is voor wat betreft de noodzaak tot het verwerken van persoonsgegevens dan dient overgegaan te worden tot het voldoen aan de wettelijke bepalingen voor de bescherming van de persoonsgegevens. Door de Schrems II-uitspraak van het HvJ-EU dient iedere organisatie zich af te vragen of persoonsgegevens per definitie nog verwerkt moeten worden in de VS.
Belangrijkste vragen die beantwoord moeten worden zijn:

- Is deze verwerking daadwerkelijk de potentiële risico's (reputatieverlies of boetes als gevolg van een datalek) voor de organisatie waard?
- Als de organisatie besluit om door te gaan met de verwerking, is dan het anonimiseren van persoonsgegevens nog een optie? (geen formele verwerking van persoonsgegevens)
- Indien het anonimiseren van persoonsgegevens vanwege kosten of technische haalbaarheid geen optie is, dan zijn er door de EDPB enkele aanbevelingen uitgebracht om te komen tot een gedegen analyse van het derde land (in deze casus Amerika).

## Stap 1&2 Identificeer transporten en bepaal transportmechanisme[1]

Gebaseerd op de uitspraken van de EDPB is het van belang om vast te stellen dat er daadwerkelijk persoonsgegevens worden getransporteerd naar derde landen (buiten de EU). Zodra is komen vast te staan dat de persoonsgegevens daadwerkelijk verwerkt worden in het derde land, moet worden vastgesteld op welke transportmechanisme dit is gestoeld. Hiermee bedoelen we de juridische onderbouwing van de afspraken zoals vermeld in hoofdstuk 5 van de GDPR. De verschillende transportmechanismen zijn:

- bindende bedrijfsvoorschriften (tijdens publicatie nog onderwerp van discussie binnen EDPB);
- goedgekeurde gedragscode;
- goedgekeurd certificeringsmechanisme;
- standaardcontractbepalingen.

Indien een derde land reeds adequaat is bevonden door de Europese Commissie, dan hoeft er geen verdere actie te worden ondernomen. Als dit niet het geval is, moet worden bekeken welke van de transportmechanismen van toepassing kan worden verklaard, indien het transport regulier en herhalend plaatsvindt.

[1] edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (europa.eu)

## Ad hoc, niet regelmatig, maar noodzakelijk transport

Als het transport van persoonsgegevens slechts ad hoc en niet regelmatig voorkomt, dan kan er gesteund worden op één van de mogelijke afwijkingen zoals gedefinieerd binnen de Algemene verordening gegevensbescherming (AVG), artikel 49, als aan de benoemde voorwaarden wordt voldaan.

## Stap 3 Beoordeling van het derde land

Het is aan de verwerkingsverantwoordelijke om een privacyrisicobeoordeling uit te voeren op het derde land en haar rechtstaat. Specifiek voor deze casus moet worden beoordeeld of er iets in de Amerikaanse wet of toepassing daarvan voorkomt, dat afbreuk doet aan de effectiviteit van de noodzakelijke privacywaarborgen van het gekozen transportmechanisme. Bij deze risicobeoordeling moet minimaal gekeken worden naar:

- De mate waarin het derde land toegang tot persoonsgegevens kan gebruiken voor toezichtdoeleinden, zeker als het derde land dubbelzinnig en/of onvoldoende transparant is in haar uitingen hieromtrent;
- De beschikbare wetgeving in het derde land. Als deze ontbreekt of onvoldoende aanwezig is, dan moet er worden gekeken naar andere relevante en objectieve factoren voor de onderbouwing van de effectiviteit van de waarborgen. Er mag daarbij niet worden uitgegaan van subjectieve factoren (b.v. de kans dat er inderdaad toegang wordt afgedwongen, het risicoprofiel van de persoonsgegevens of het blootstellen van eenvoudige openbaar toegankelijke persoonsgegevens). NB. Dit is een aanzienlijke beperking om voor de beoordeling een risicogebaseerde aanpak te volgen.

Bovenstaande risicobeoordeling dient met gepaste zorgvuldigheid te worden uitgevoerd en volledig te worden gedocumenteerd. Dit vanwege de verantwoordelijkheid die een organisatie heeft voor de beslissingen die op basis van deze risicobeoordeling worden genomen.

## Stap 4 Aanvullende maatregelen

Zodra een derde land door de eerdergenoemde privacyrisicobeoordeling als ongeschikt voor verwerken van persoonsgegevens wordt verklaard, kan gezocht worden naar mitigerende maatregelen op die onderdelen die in de beoordeling als onvoldoende waarborgen naar voren komen. In het geval dat de aanvullende maatregelen niet voldoende waarborgen kunnen bieden zal de verwerkingsverantwoordelijke moeten besluiten om de persoonsgegevens niet te transporteren naar het betreffende derde land of over te gaan tot het anonimiseren van de persoonsgegevens.
Aanvullende maatregelen kunnen technisch, contractueel of organisatorisch van aard zijn. Contractuele en organisatorische maatregelen alleen zullen over het algemeen de overheidsinstanties er niet van weerhouden, zich toegang te verschaffen tot de persoonsgegevens. Dit onderschrijft het belang van adequate technische maatregelen. Een grote rol is hierin weggelegd voor encryptie, vooropgesteld dat deze voldoet aan onder andere: krachtige encryptie voorafgaand aan verzending, bestand zijn tegen crypto-analyse door

overheden (brute force aanvallen), foutloze implementatie van een “end to end” encryptie[2]-algoritme en de sleutels worden uitsluitend beheerd door de verwerkingsverantwoordelijke (of andere partijen, vooropgesteld dat zij zijn gevestigd in de EA of een adequaat derde land).

## Stap 5 Borging van de maatregelen

Zodra de verwerkingsverantwoordelijke heeft vastgesteld welke aanvullende maatregelen noodzakelijk zijn moeten deze procedureel worden verankerd. Verifiëren door de verwerkingsverantwoordelijke van de procedureel beschreven maatregelen tegen de AVG is hierbij noodzakelijk. De uitkomst van de verificatie kan aanleiding vormen voor het laten toetsen van de beschreven maatregelen bij de lokale toezichthoudende instantie.

## Stap 6 Monitoren van de maatregelen

Het is van belang om op regelmatige basis de getroffen maatregelen te evalueren voor wat betreft hun doelmatigheid zoals beschreven in de beoordeling van het derde land. Daarnaast zal tijdens deze evaluatie ook de eventuele toekomstige veranderingen in het derde land, daar waar deze impact hebben op de verwerking van persoonsgegevens, moeten worden meegenomen. Een korte checklist[3] hieronder helpt je met de verdere invulling van maatregelen bij een risicobeoordeling waarbij het derde land als “onveilig” is verklaard. Hierbij gaan wij ervanuit dat geen persoonsgegevens leesbaar[4] worden uitgewisseld met een (sub)verwerker in een onveilig land.

## AVG controlelijst voor verwerking in een onveilig derde land

| Privacy Principe | (sub)Verwerker in “onveilig” derde land bij aanvang verwerking | (sub)verwerker in “onveilig” derde land gedurende verwerking |
|---|---|---|
| 1. Vrije keuze en toestemming | ✓ Extra waarborgen opnemen in de verwerkersovereenkomst over het inzetten van subverwerkers.<br>✓ Binnen de privacyverklaring de verwerking in het betreffende onveilige derde land specifiek maken (Art. 13.1.f) | ✓ Extra waarborgen opnemen in de verwerkersovereenkomst over het inzetten van subverwerkers.<br>✓ Aanpassen privacyverklaring de verwerking in het betreffende onveilige derde land specifiek maken (Art. 13.1.f)<br>✓ Opnieuw toestemming verkrijgen van de gegevenseigenaar voor de werking in het onveilige derde land |
| 2. Wettelijke grondslag, specificatie en beperking | ✓ Opstellen van het verwerkingsregister met doorgiften aan onveilige derde land (Art. 30.1.e) | ✓ Aanpassen van het verwerkingsregister met doorgiften aan onveilige derde land (Art. 30.1.e) |

[2] EDPB stelt uitgebreide eisen aan de mate van encryptie – EDPB 01/2020 casus 1
[3] Met de checklist beogen de auteurs de belangrijkste elementen in te vullen. Een checklist is geen garantie op volledigheid.
[4] EDPB presenteert in haar advies verschillende casussen waarbij wordt geconcludeerd dat het uitwisselen van leesbare persoonsgegevens ook niet door aanvullende maatregelen afdoende kan worden beschermd – EDPB 01/2020

| Privacy Principe | (sub)Verwerker in "onveilig" derde land bij aanvang verwerking | (sub)verwerker in "onveilig" derde land gedurende verwerking |
|---|---|---|
| 3. Levenscyclus gegevens | ✓ Uitvoerend aanvullend privacy risico assessment gericht op vaststellen wetgeving betreffende land met betrekking tot het opslaan, bewaren en vernietigen van persoonsgegevens (Art. 13.2.a en 14.2.a) | ✓ Uitvoerend aanvullend privacy risico assessment gericht op vaststellen wetgeving betreffende land met betrekking tot het opslaan, bewaren en vernietigen van persoonsgegevens (Art. 13.2.a en 14.2.a) |
| 4. Kwaliteit en Nauwkeurigheid | ✓ Vereist geen additionele maatregelen | ✓ Vereist geen aanpassingen |
| 5. Openheid, transparantie, communicatie | ✓ Binnen de privacyverklaring de verwerking in het betreffende onveilige derde land specifiek maken (Art. 13.1.f) | ✓ Aanpassen privacyverklaring de verwerking in het betreffende onveilige derde land specifiek maken (Art. 13.1.f) |
| 6. Rechten van betrokkene | ✓ Vereist geen additionele maatregelen | ✓ Vereist geen aanpassingen |
| 7. Verantwoordelijkheden | ✓ Vereist geen additionele maatregelen | ✓ Vereist geen aanpassingen |
| 8. Beveiligingsmaatregelen | ✓ Vaststellen dat wordt voldaan aan AVG vereisten van technische en organisatorische maatregelen.<br>✓ Encryptie dient te voldoen aan de zes expliciet gedefinieerde vereisten. | ✓ Vaststellen dat wordt voldaan aan AVG vereisten van technische en organisatorische maatregelen.<br>✓ Encryptie dient te voldoen aan de zes expliciet gedefinieerde vereisten. |
| 9. Meten, monitoren, rapporteren | ✓ Opnemen van het nieuwe privacy risicogebieden binnen de organisatie | ✓ Opnemen van het nieuwe privacy risicogebieden binnen de organisatie |
| 10. Voorkomen van schade | ✓ De (sub)verwerker op de hoogte stellen van potentiële privacy schade aan de gegevenseigenaar bij een exposure | ✓ De (sub)verwerker op de hoogte stellen van potentiële privacyschade aan de gegevenseigenaar bij een exposure |
| 11. Derde partijen | ✓ Opnemen van standaardcontractbepalingen in de verwerkersovereenkomst<br>✓ De (sub)verwerker informeren dat melding van privacyincidenten aan verwerkingsverantwoordelijke verplicht is binnen de wettelijke termijn | ✓ Aanpassen van standaardcontractbepalingen in de verwerkersovereenkomst<br>✓ De (sub)verwerker informeren dat melding van privacyincidenten aan verwerkingsverantwoordelijke verplicht is binnen de wettelijke termijn |
| 12. Inbreuken, incidenten | ✓ Vereist geen additionele maatregelen | ✓ Vereist geen aanpassingen |
| 13. Security & Privacy by design | ✓ Vereist geen additionele maatregelen | ✓ Vereist geen aanpassingen |

| Privacy Principe | (sub)Verwerker in "onveilig" derde land bij aanvang verwerking | (sub)verwerker in "onveilig" derde land gedurende verwerking |
|---|---|---|
| 14. Transport naar Landen & zones | ✓ Raamwerk van interne beveiligingsmaatregelen communiceren aan US verwerker<br>✓ Uitvoeren van privacy risico assessment voor transport buiten EER<br>✓ Uitvoeren van verschil-analyse tussen raamwerk beveiligingsmaatregelen verwerkingsverantwoordelijke en de geldende wetgeving voor verwerker<br>✓ Stel vast dat verwerker conform het raamwerk beveiliging heeft ingericht<br>✓ Zorg voor vastlegging van getransporteerde persoonsgegevens naar verwerker | ✓ Aanpassen van het interne privacymaatregelen raamwerk v.w.b. het onveilige derde land<br>✓ Specifiek binnen het raamwerk op nemen van de uitvoering van een privacy risico assessment voor transport naar het onveilige derde land<br>✓ Opnemen van aanvullende maatregelen ter compensatie van mogelijke risico's verwerking in het onveilige derde land<br>✓ Vaststellen dat de (sub)verwerker de noodzakelijke compenserende maatregelen ook heeft geïmplementeerd<br>✓ Zorgdragen voor de vastlegging van getransporteerde persoonsgegevens |

## Over de auteurs:


- Menno Borst werkzaam bij iRISK cybersecurity (CRISC, CDPSE) - Menno Borst | LinkedIn

  Experienced Information Technology Risk Manager with a demonstrated history of working in retail and finance industry. Skilled in Information Technolgy Process management, Governance by design Cobit 2019, Security management ISO 27001, IT Risk Management, Software development life cycle and privacy compliancy. Strong and pragmatic information technology professional, securing what matters, focused on IT Risk Management, Security and Privacy from ISACA.

- Piet Dekker werkzaam bij Onetrust consulting (CIPP/E) - Piet Dekker | LinkedIn