TOOLKIT

Road Map Data Transfer Impact Assessment

DPO Consultancy
Experts in Data Privacy

April 2026

Wanneer jouw organisatie persoonsgegevens overdraagt naar landen buiten de Europese Economische Ruimte (EER), is het belangrijk om ervoor te zorgen dat hetzelfde beschermingsniveau geldt als in de lidstaten van de EER. Deze landen worden ook wel ‘derde landen’ genoemd. Als je bijvoorbeeld persoonsgegevens van Duitsland naar de Verenigde Staten overdraagt, is het belangrijk dat in de VS hetzelfde niveau van gegevensbescherming van toepassing is.

Een onderdeel van deze wetgeving is dat jouw organisatie altijd beschikt over een rechtsgeldig doorgiftemechanisme voor internationale gegevensoverdrachten. Er zijn verschillende doorgiftemechanismen, zoals adequaatheidsbesluiten, bindende bedrijfsvoorschriften (Binding Corporate Rules) en Standaardcontractbepalingen (Standard Contractual Clauses, SCC’s). In de praktijk zien we dat voor doorgiften naar derde landen de SCC’s het meest gebruikte doorgiftemechanisme zijn. Sinds 27 september 2021 is het bij gebruik van dit mechanisme altijd verplicht om een Data Transfer Impact Assessment (DTIA) uit te voeren voordat de persoonsgegevens de Europese Economische Ruimte mogen verlaten.

Wil je meer weten over internationale gegevensoverdrachten en de AVG?

Check onze blog

Wat is een DTIA?

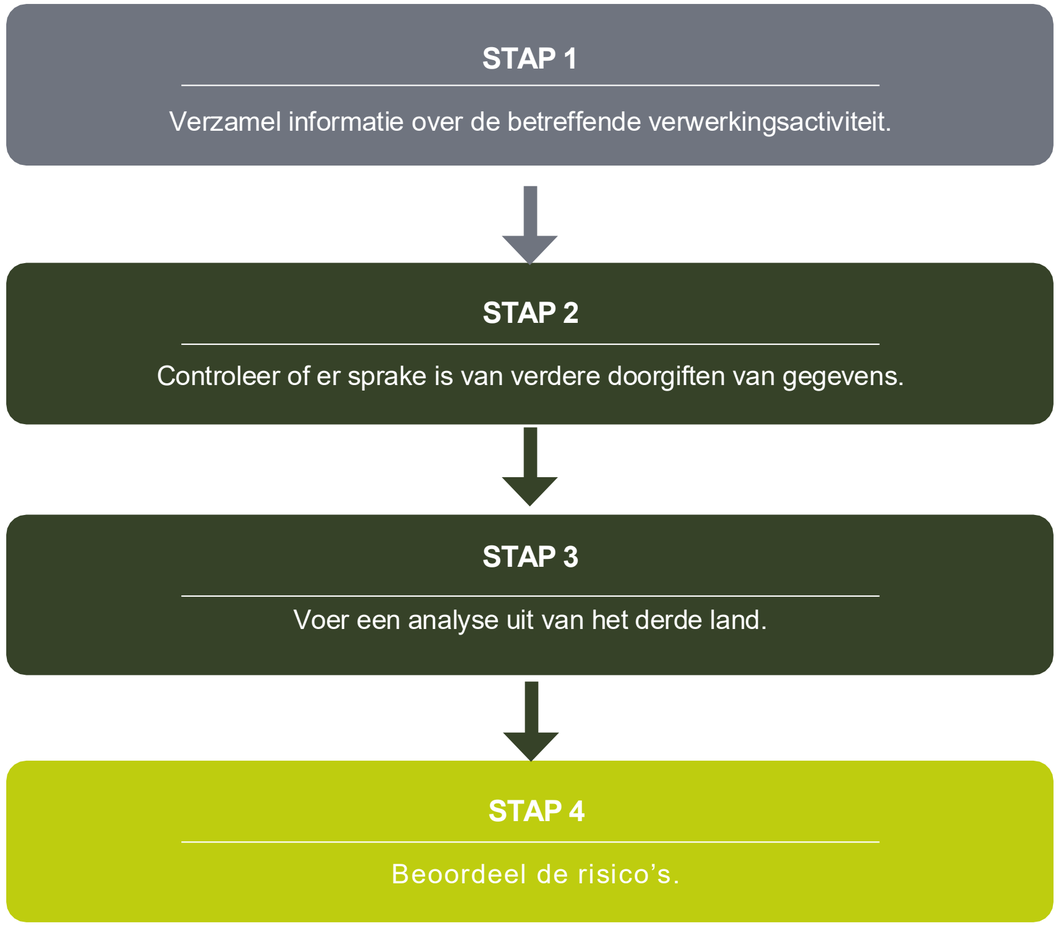
Een Data Transfer Impact Assessment is een instrument waarmee jouw organisatie de risico's kan beoordelen die gepaard gaan met het internationaal overdragen van gegevens.

Een DTIA is vormvrij, hoewel de European Data Protection Board richtlijnen heeft opgesteld over hoe een DTIA moet worden uitgevoerd en welke aanvullende maatregelen kunnen worden genomen om risico's te beperken.
Het is belangrijk om te benadrukken dat wanneer de toezichthoudende autoriteit contact opneemt met de gegevensimporteur of de gegevensexporteur om de uitgevoerde DTIA te beoordelen, deze moet kunnen worden verstrekt. Dit sluit aan bij het verantwoordingsbeginsel (accountability) onder de AVG, dat vereist dat organisaties hun naleving van de AVG documenteren.

Hoe voer je een DTIA uit?

Bij een Data Transfer Impact Assessment is het belangrijk dat jouw organisatie weet welke stappen moeten worden genomen en hoe een DTIA moet worden uitgevoerd. Met dit stappenplan helpen wij jouw organisatie bij het uitvoeren van een Data Transfer Impact Assessment. Zo kun je DTIAs op een duidelijke, efficiënte en verantwoorde manier uitvoeren.

De vier stappen van een Data Transfer Impact Assessment



Stap 1

Verzamel informatie over de betreffende verwerkingsactiviteit

Er zijn veel specifieke elementen die in deze stap moeten worden beoordeeld, maar de kern is dat je de datastroom moet beschrijven om te begrijpen hoe gegevens zich van input naar output verplaatsen. Daarnaast moet je ook de beveiliging van de gegevens beschrijven. Welke maatregelen zijn er om de gegevens te beschermen? Tot slot moet je de volgende zes vragen beantwoorden: wie, wat, wanneer, waar, waarom en hoe? Dit kunnen vragen zijn zoals:

- Wie verzendt de gegevens?
- Welke persoonsgegevens zijn betrokken?
- Wanneer en hoe vaak vindt de overdracht plaats?
- Waar worden de gegevens naartoe gestuurd?
- Waarom is het nodig om de gegevens te verzenden? Wat is het doel?
- Hoe worden de gegevens verzonden? Wat is het gegevensformaat?

De basis voor jouw DTIA is dat je over alle noodzakelijke informatie beschikt over de betreffende verwerkingsactiviteit. Wanneer je kunt terugvallen op gegevens uit bestaande verwerkingsactiviteiten, is de benodigde informatie voor deze stap eenvoudig te vinden.

Zo niet, dan moet je belangrijke informatie over de verwerkingsactiviteit verzamelen. Een andere mogelijkheid is dat er een overeenkomst bestaat die veel informatie bevat die je als bron kunt gebruiken. Voorbeelden hiervan zijn Master Services Agreements, verwerkersovereenkomsten (Data Processing Agreements) en distributieovereenkomsten.

Stap 2

Controleer of er sprake is van verdere doorgiften van gegevens

Nadat je alle informatie over de verwerkingsactiviteit hebt verzameld, is het noodzakelijk om te beoordelen of er verdere doorgiften van gegevens plaatsvinden naar een andere partij of entiteit. Dit is belangrijk, omdat het mogelijk is dat de gegevens naar meerdere derde landen worden verzonden. Je moet ervan bewust zijn dat je als verwerkingsverantwoordelijke voor de verwerkingsactiviteit verantwoordelijk bent om dit te verifiëren met andere partijen of entiteiten.

Daarom is het belangrijk om jezelf, vergelijkbaar met stap 1, de zes vragen te stellen met betrekking tot verdere doorgiften (indien van toepassing): wie, wat, wanneer, waar, waarom en hoe? In deze stap kun je denken aan vragen zoals:

- Welke partijen voeren verdere doorgiften uit?
- Wat zijn de exacte rollen van deze partijen onder de AVG (verwerkingsverantwoordelijke/(sub)verwerker/gezamenlijke verwerkingsverantwoordelijke)?
- Wanneer moet aan deze verplichting worden voldaan? Aangezien je de informatie moet verzamelen vóór de verdere doorgifte van gegevens en voordat de SCC's worden afgesloten.
- Waar worden de gegevens opgeslagen?
- Waarom is het, met inachtneming van gegevensminimalisatie, noodzakelijk dat de betreffende partij of entiteit deze gegevens verwerkt?
- Hoe zijn de contractuele relaties tussen de verschillende partijen ingericht? Zijn er SCC's, aanvullende verwerkersovereenkomsten (Data Processing Agreements), enzovoort afgesloten?

Stap 3

Voer een analyse uit van het derde land

Tot slot moet je beoordelen of een autoriteit verzoekt om openbaarmaking van of toegang tot de gegevens bij de gegevensimporteur. Hoe gaat de wetgeving van dit derde land hiermee om? Wij zetten de belangrijkste aandachtspunten voor je op een rij:

- Organisaties vergeten vaak dat het niet alleen om de AVG gaat, maar ook om het recht op privacy: een fundamenteel mensenrecht. Het is daarom ook belangrijk om te beoordelen hoe mensenrechten en fundamentele vrijheden in derde landen worden gerespecteerd.
- Jouw organisatie dient ook te beoordelen welke privacywetgeving van toepassing is. Heeft het land bijvoorbeeld een privacywet? Dit geeft je de nodige inzichten in hoe het land privacyrechten respecteert.
- Beoordeel hoe de rechtsbescherming voor betrokkenen – personen van wie persoonsgegevens worden verwerkt – is geregeld. Als je bijvoorbeeld als individu in de EU woont en juridische stappen wilt ondernemen tegen een organisatie in Brazilië, is het dan mogelijk om naar de rechter te gaan?
- Vergelijk ook de concepten en beginselen van de AVG met de wetgeving van het betreffende derde land. Denk aan AVG-beginselen zoals gegevensminimalisatie, doelbinding of transparantie. Maar ook aan de omgang met rechten van betrokkenen, zoals het recht om vergeten te worden of het recht op inzage.
- Beoordeel hoe eenvoudig het is voor overheidsinstanties om toegang te krijgen tot persoonsgegevens. Moet een overheidsinstantie bijvoorbeeld eerst een gerechtelijk bevel verkrijgen om toegang te krijgen, of kan zij eenvoudig verzoeken of eisen dat de gegevens worden verstrekt?

Wil je gebruikmaken van onze derde-landenanalyse-database (Global Data Transfer Atlas) of DTIA-as-a-service?

Lees meer over onze services

Stap 4

Het beoordelen van de geïdentificeerde risico’s

Een veelgebruikte manier om privacyrisico’s te identificeren is het gebruik van een risicoscoringsmodel. Er zijn verschillende opties als het gaat om risicoscoringsmodellen. Een manier om risico’s te identificeren is door zowel de waarschijnlijkheid als de impact van het risico te scoren op een schaal van 1 tot 5.
Bij de waarschijnlijkheidsscore betekent 1 dat het risico zeer onwaarschijnlijk is en 5 dat het risico zeer waarschijnlijk is. Bij de impactscore wordt de ernst van het risico gemeten, waarbij 1 een geringe impact heeft op de betrokkenen en 5 een zeer ernstige impact heeft op de betrokkenen.

Kans	1	2	3	4	5
De waarschijnlijkheid dat het risico zich voordoet	Zeer onwaarschijnlijk	Gering	Mogelijk	Waarschijnlijk	Zeer waarschijnlijk
Impact	1	2	3	4	5
De impact (gevolgen) van het risico	Geringe impact	Beperkte impact	Aanzienlijke impact	Ernstige impact	Zeer ernstige impact

Vervolgens kun je alle geïdentificeerde privacyrisico's bij de gegevensoverdracht in kaart brengen door de feitelijke omstandigheden die je hebt vastgesteld te beschrijven en vervolgens toe te lichten welke gevolgen dit kan hebben voor de privacy van betrokkenen. Daarna kun je je richten op de aanvullende maatregelen die je kunt nemen om de privacyrisico's te beperken. Aanvullende maatregelen kunnen onder meer het gebruik van anonimisering en pseudonimisering omvatten, waar mogelijk. Dit is aanbevolen door de European Data Protection Board.

Nr.	Risico	Oorsprong	Kans (1-5)
1	Gebaseerd op het feit dat.... (omschrijf het feit), bestaat er een kans dat (omschrijf gevolg)	Artikel 5(1)(b) AVG; Doelbinding	2

Daarnaast moeten aanvullende of mitigerende maatregelen die uw organisatie neemt duidelijk maken of het resterende risico wordt geaccepteerd, wie eigenaar is van dat risico en wanneer de maatregel zal worden afgerond. Tot slot wordt een goedkeuring door de CEO aanbevolen, aangezien dit de verantwoordelijkheid van de verwerkingsverantwoordelijke onderstreept.

Conclusie

Nadat je alle informatie hebt verzameld over de verwerkingsactiviteit, verdere doorgiften en de juridische analyse van het derde land, ben je in staat om privacyrisico's te identificeren. Met een Data Transfer Impact Assessment zorg je ervoor dat hetzelfde beschermingsniveau wordt gewaarborgd wanneer jouw organisatie persoonsgegevens overdraagt naar landen buiten de Europese Economische Ruimte. Op deze manier voldoe je niet alleen aan wet- en regelgeving, maar voorkom je ook dat mogelijke problemen pas achteraf aan het licht komen.

Heb je aanvullende vragen over
de DTIA of andere specifieke onderwerpen?
Contacteer ons via info@dpoconsultancy.nl
of +31 85 0711080

Europalaan 28B
5232 BC 's-Hertogenbosch
The Netherlands

Samenwerkingsstraat 50
2845 Niel
Belgium
www.infosentry.be
www.thesecurityfactory.be

1 Lyric Square London
W6 0NB
England

+31 85 0711080
info@dpoconsultancy.nl
www.dpoconsultancy.com