TOETSINGSKADER
VOOR DE DOORGIFTE VAN PERSOONSGEGEVENS

SURF Taskforce Beyond Privacy Shield

Inhoudsopgave

Samenvatting

Wat is de achtergrond van het Toetsingskader?

De Algemene verordening gegevensbescherming (AVG) heeft als belangrijk doel het beschermen van persoonsgegevens. Die bescherming geldt niet alleen binnen de landen van de Europese Unie, maar ook als deze gegevens *buiten* de Europese Economische Ruimte (EER)[1] worden gebracht, zoals bijvoorbeeld het hosten van persoonsgegevens in de Verenigde Staten. Het buiten de EER brengen van persoonsgegevens wordt 'doorgifte' genoemd.

Aan doorgifte van persoonsgegevens naar landen buiten de EER stelt de AVG speciale voorwaarden. Deze voorwaarden zijn complex, zeker na de uitspraak van het Europees Hof van Justitie in de zaak Schrems II. Ook de leden van SURF* worstelen met de vraag of, en zo ja onder welke voorwaarden, doorgifte van persoonsgegevens is toegestaan.

Om de leden van SURF bij de beantwoording van deze vragen te ondersteunen, hebben SURF en zijn leden de Taskforce Beyond Privacy Shield ingesteld. De Taskforce bestaat uit deskundigen van SURF en de leden, die veel met het onderwerp van doorgifte te maken hebben. Het betreft privacy officers, privacy juristen, Functionarissen Gegevensbescherming (FG's), inkopers en deskundigen op het gebied van informatiebeveiliging. Het resultaat van de beraadslagingen van de Taskforce is dit Toetsingskader voor doorgifte van persoonsgegevens.

Wat is het doel en wat is de aard van het Toetsingskader?

Het doel van het Toetsingskader is:

1. Voor de leden van SURF inzichtelijk maken welke risico's zijn verbonden aan data doorgifte;
2. Handvatten bieden waarmee een lid van SURF een weloverwogen beslissing kan nemen of doorgifte doorgang kan vinden en zo ja, onder welke voorwaarden.

Als een lid tot het oordeel komt dat doorgifte onder voorwaarden doorgang kan vinden, dan hebben die voorwaarden vooral betrekking op het nemen van aanvullende maatregelen: op contractueel, organisatorisch en technisch

1 De EER bestaat uit de landen van de EU aangevuld met IJsland, Noorwegen en Liechtenstein.

* Via de coöperatie SURF maken de leden gezamenlijk afspraken met ict- en contentleveranciers over de levering en afname van producten en diensten. Zo zorgen de leden gezamenlijk voor schaalgrootte en een efficiënt aanspreekpunt voor leveranciers.

gebied om zo rechtmatig persoonsgegevens te kunnen doorgeven. Het is belangrijk om te benadrukken dat het Toetsingskader zelf geen beslissingen over doorgifte en aanvullende maatregelen voorschrijft. Dat is uitsluitend en volledig aan ieder lid van SURF.

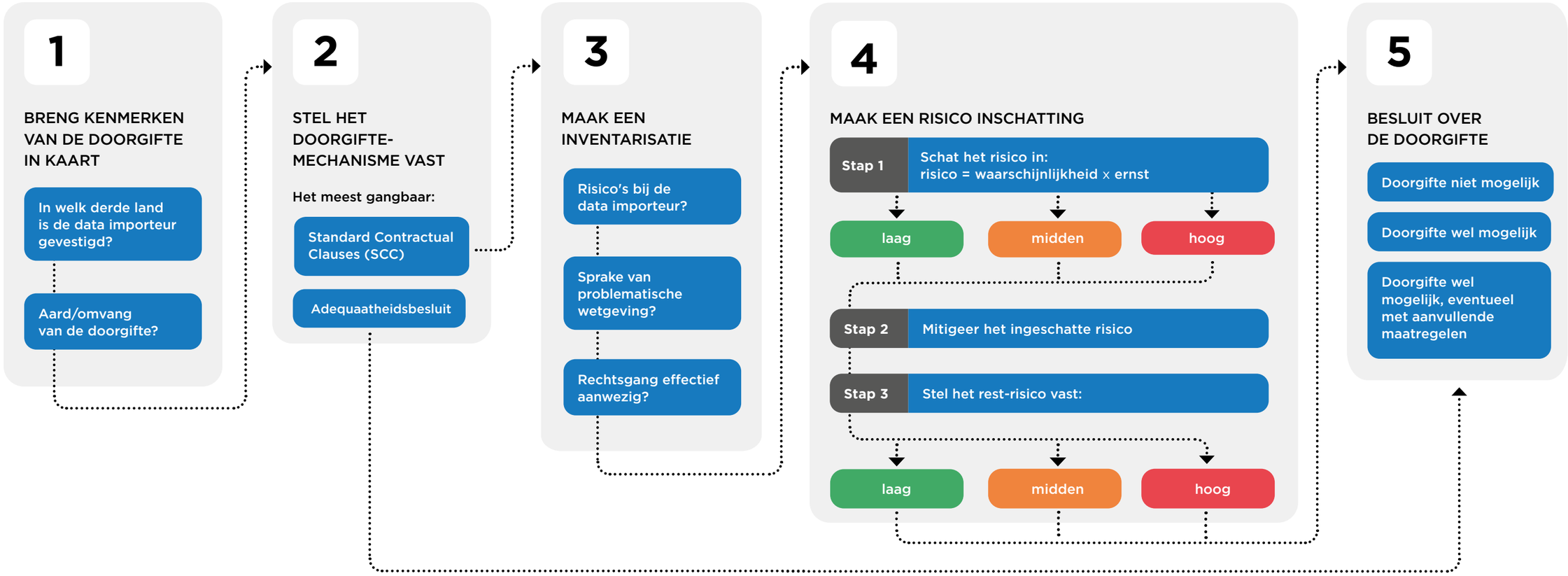
Het Toetsingskader visueel uitgebeeld

In onderstaande visual wordt het Toetsingskader op hoofdlijnen weergegeven, met daarbij een beschrijving van de belangrijkste bevindingen. Voor een toelichting op de verschillende onderdelen wordt in de visual verwezen naar de verschillende hoofdstukken van dit document.

Voor wie is het Toetsingskader bedoeld?

Voor de uitvoering van het Toetsingskader is een belangrijke rol weggelegd voor de partij aan wie de persoonsgegevens worden verstrekt: bijvoorbeeld de leverancier, reseller, verwerker, etc. Dit is bij uitstek de partij om de relevante informatie in het kader van de risico-inschatting te verstrekken.

Daarnaast spelen binnen de leden van SURF ook verschillende afdelingen en functionarissen een belangrijke rol bij de toepassing van dit Toetsingskader. Naast de afdeling, opleiding, etc. die de persoonsgegevens buiten de EER wil brengen, ziet de Taskforce een belangrijke rol voor privacy deskundigen



lees meer in **hoofdstuk 3**

lees meer in **hoofdstuk 4**

lees meer in **hoofdstuk 5**

lees meer in **hoofdstuk 6 & 7**

(bijvoorbeeld privacy officers of de FG), juristen, inkopers en informatie beveiligingsdeskundigen. Zij helpen bij het wegen en beoordelen van de uitkomsten van de inventarisaties, en bij het bepalen of, en zo ja welke, aanvullende maatregelen vereist zijn voor het rechtmatig doorgeven van persoonsgegevens. De precieze invulling van rollen, taken en verantwoordelijkheden is aan ieder lid van SURF zelf en kan inzichtelijk worden gemaakt met bijvoorbeeld een RASCI model[2].

Wat is de status van het Toetsingskader?

De leden van SURF zijn en blijven *zelf* verantwoordelijk voor het voldoen aan alle eisen van de AVG, waaronder de eisen verbonden aan een doorgifte. Het wel of niet (gedeeltelijk) toepassen van het Toetsingskader en de keuze voor het wel of niet doorzetten van een voorgenomen doorgifte is aan de leden zelf. De Taskforce en het Toetsingskader treden niet in die afwegingen en keuzes.

> *Het Toetsingskader kent een dynamisch karakter in die zin dat periodiek dient te worden nagegaan of de voorwaarden en risico's van de bestaande doorgifte zijn gewijzigd.*

Die eigen beoordeling van een lid van SURF kan ertoe leiden dat een voorgenomen doorgifte geen doorgang kan vinden. Bijvoorbeeld omdat deze niet past in de risicobereidheid van het lid, de aanvullende maatregelen te weinig krachtig, haalbaar of effectief zijn of dat zelfs na het treffen van aanvullende maatregelen het restrisico te groot blijft.

Wat zijn verder nog belangrijke overwegingen bij dit Toetsingskader?

Een doorgifte van persoonsgegevens is een verwerking in de zin van de AVG. Dat betekent dat moet zijn voldaan aan onder meer de eisen van de artikelen 5 en 6 van de AVG, het eventueel uitvoeren van een *Data Protection Impact Assessment* (DPIA), het informeren van betrokkenen en het treffen van passende technische en organisatorische beveiligingsmaatregelen.

> *Speciale aandacht in dit verband verdient het vereiste van 'noodzakelijkheid' en meer in het bijzonder de vraag of alternatieve, minder invasieve mogelijkheden voor doorgifte aanwezig zijn. Indien de verwerking mogelijk is binnen de EER, bijvoorbeeld omdat er daadwerkelijk alternatieven zijn (vanuit praktisch-, technisch- en kostenoogpunt) dan kan dat betekenen dat de keuze moet vallen op verwerking binnen de EER, in plaats van op het alternatief buiten de EER.*

Het toepassen van de stappen van het Toetsingskader is een verantwoordelijkheid van elk lid van SURF en elk lid geeft daarmee invulling aan het vereiste van een *Data Transfer Impact Assessment* (DTIA) voor doorgifte van persoonsgegevens. Doorgifte naar derde landen is evenwel mogelijk en wettelijk toegestaan, mits afdoende maatregelen zijn getroffen (en getoetst via een DPIA en DTIA).

In het kader van de verantwoordingsplicht dienen de resultaten van de uitgevoerde toetsing schriftelijk te worden vastgelegd. Bij een positief besluit, dient de doorgifte te worden opgenomen in het register van verwerkingen.

Gaat de Taskforce en/of SURF nog aan de slag met tooling en met een periodieke evaluatie van het Toetsingskader?

De Taskforce is zich bewust van het feit dat het uitvoeren van het Toetsingskader veel van de leden van SURF vraagt. De Taskforce en SURF gaan actief op zoek naar specifieke *tooling*, die de leden van SURF helpen bij het makkelijker, sneller en beter toepassen van het Toetsingskader.

De Taskforce zal daarnaast het Toetsingskader periodiek evalueren en waar nodig herzien op basis van de opgedane ervaringen, *best practices*, ontwikkelingen in wet- en regelgeving (bijvoorbeeld nieuwe/gewijzigde adequaatheidsbesluiten, goedgekeurde certificeringen en gedragscodes of recommendations van de nationale en/of Europese toezichthouders) en nieuwe inzichten binnen SURF rond bijvoorbeeld *Vendor Risk Management* en *cloud-controls*.

Het Toetsingskader is een dynamisch document waarbij de leden van SURF uitdrukkelijk worden uitgenodigd hun ervaring met elkaar en binnen de Taskforce te delen.

2 Het RASCI-model is een matrix die gehanteerd wordt om de rollen en verantwoordelijkheden van de personen betrokken bij een project of taak weer te geven. Het acroniem is als volgt samengesteld: R: Responsible [Verantwoordelijk], A: Accountable [Eindverantwoordelijk], S: Supportive [Ondersteunend], C: Consulted [Geraadpleegd], I: Informed [Geïnformeerd].

1.
Inleiding toetsingskader

Het doorgeven van persoonsgegevens door leden van SURF aan instellingen en organisaties in landen *buiten de EER* roept ook bij de leden van SURF tal van juridische en praktische vragen op. Zeker na de uitspraak van het Europese Hof van Justitie in de zaak Schrems II, worstelen leden van SURF met de vraag welke data doorgiften nog wel mogen en onder welke voorwaarden. De Taskforce Beyond Privacy Shield heeft voor de leden van SURF naast verschillende *use stories*, een Toetsingskader opgesteld dat als hulpmiddel fungeert voor de toetsing van een doorgifte.

Dit Toetsingskader biedt een praktisch stappenplan aan de hand waarvan een instelling een besluit kan nemen over datadoorgifte buiten de EER: of en zo ja onder welke voorwaarden dit plaats kan vinden en wat daarbij de verantwoordelijkheden zijn van de instelling en andere betrokkenen.

De stappen zijn als volgt:

1 Breng de specifieke kenmerken van de voorgenomen doorgifte in kaart

Dit vereist kennis en bekendheid met de voorgenomen doorgifte. Kijk hierbij goed naar:

- Welk derde land ontvangt de persoonsgegevens en wat is de aard en omvang van de persoonsgegevens;
- Welke verdere doorgiften naar welke andere derde landen plaatsvinden.

→ *Gebruik hiervoor de vragenlijst uit hoofdstuk 3.*

2 Stel op basis van de AVG vast wat het juridisch mechanisme is voor de betreffende doorgifte

Er zijn landen buiten de EER waarvoor een zogenaamd adequaatheidsbesluit geldt. Als leden van SURF persoonsgegevens willen doorgeven aan één van deze landen, dan is verder géén actie nodig. Het Toetsingskader hoeft dan niet verder te worden doorlopen. Voor de resterende derde landen zijn de Standard Contractual Clauses (SCC) het meest gangbaar voor use cases binnen de onderwijssector.

→ *Gebruik hiervoor hoofdstuk 4.*

3 Maak een risico-inventarisatie

Wat zijn de verantwoordelijkheden van de instelling en de data importeur in het derde land (passend bij het doorgiftemechanisme) en kunnen beide partijen aantoonbaar of op basis van redelijke verwachtingen aan deze eisen voldoen? Hiervoor is een inventarisatie nodig van:

A. De ontvanger van de persoonsgegevens.

Deze dient te verduidelijken hoe met de (beveiliging van) persoonsgegevens wordt omgegaan. Speciale aandacht is nodig voor:

1. Subverwerkers en het land van vestiging;
2. Welke maatregelen (privacy en security) er getroffen zijn;
3. Dataverstrekking aan autoriteiten.

B. Het land buiten de EER

Is er toepasselijke wet- en regelgeving en zijn er gerelateerde gangbare praktijken m.b.t. bescherming van persoonsgegevens? Conflicteert dit met het niveau van gegevensbescherming zoals geborgd in de AVG? Aandachtspunten hierbij zijn met name inzageverzoeken van overheidsdiensten en de aanwezigheid van effectieve mogelijkheden van rechtsgang (bezwaar en beroep) voor betrokkenen.

→ *Gebruik hiervoor hoofdstuk 5.*

4 Maak een risico-inschatting

> **Door gebruik te maken van de uitkomsten van de risico-inventarisatie en toepassing van 'risico = waarschijnlijkheid x ernst' (ook wel: kans x impact).**

Neem hierin naast standaard maatregelen ook restrisico's, aanvullende contractuele, organisatorische en technische maatregelen mee. Intensiveer deze maatregelen naarmate het risico-niveau stijgt (laag, midden, hoog).

Laag risico:

- zorg voor een passend doorgiftemechanisme;
- basismaatregelen zoals SCC bieden voldoende bescherming.

Midden risico:

- de maatregelen genoemd bij een laag risico, plus de volgende maatregelen:
- tref organisatorische maatregelen, zoals het meenemen van privacyoverwegingen in het inkoopbeleid;
- beoordeel of de verwerking zonder persoonsgegevens kan plaatsvinden, met gepseudonimiseerde gegevens of met een minimale set aan (gepseudonimiseerde) persoonsgegevens;
- maak goede contractuele afspraken;
- tref technische maatregelen, zoals de versleuteling van de persoonsgegevens;
- check de compliance van de ontvanger;
- informeer betrokkenen over doorgifterisico's.

Hoog risico:

- de maatregelen genoemd bij een laag en midden risico, plus de volgende maatregelen:
- tref technische maatregelen, zoals encryptie met sleutel onder eigen beheer;
- beoordeel of de verwerking noodzakelijk is voor de instelling;
- beoordeel of er leveranciers zijn die de verwerking kunnen doen binnen de EER;
- stel vast of er onderhandelingen mogelijk zijn met ontvanger over betere waarborgen.

→ *Gebruik hiervoor hoofdstuk 6 en 7.*

5 Besluit over doorgifte

De instelling neemt een besluit over de doorgifte. De Functionaris Gegevensbescherming dient, zeker bij hoog risico doorgiften, tijdig te worden betrokken voor advies. Dit besluit wordt periodiek herzien op basis van wijzigingen in de doorgifte zelf, bij de data importeur en in de wetten en praktijken van het derde land. Dergelijke wijzigingen kunnen leiden tot een andere (risico-)inschatting van, en dus tot een ander besluit over, de betreffende doorgifte.

1.1
Veelgebruikte termen

Dit Toetsingskader gebruikt een aantal meer algemene AVG begrippen zoals ‘persoonsgegevens’, ‘betrokkene’, ‘(verwerkings)verantwoordelijke’ en ‘verwerker’. De Taskforce veronderstelt dat deze begrippen en hun betekenis bekend zijn bij de lezer[3].

Daarnaast kent het Toetsingskader een aantal meer specifieke en vaak terugkerende termen en begrippen. Voor een helder en eenduidig begrip van het Toetsingskader zijn deze als volgt omschreven:

Doorgifte (doorgeven)
Het ter beschikking stellen door een data exporteur van persoonsgegevens aan een data importeur die zich bevindt in een derde land of aan een internationale organisatie.

Data exporteur
De partij die persoonsgegevens doorgeeft aan een partij in een derde land of aan een internationale organisatie, ongeacht waar deze partij is gevestigd en ongeacht of deze partij zich kwalificeert als (gezamenlijke) verwerkingsverantwoordelijke, verwerker of sub-verwerker.

Data importeur
De partij, gevestigd in een derde land, die persoonsgegevens ontvangt van een data exporteur, ongeacht of deze partij zich kwalificeert als (gezamenlijke) verwerkingsverantwoordelijke, verwerker of sub-verwerker.

Derde Land
Een land dat geen deel uitmaakt van de Europese Economische Ruimte (EER).

Europese Economische Ruimte (EER)
De landen van de Europese Unie en Noorwegen, IJsland en Liechtenstein.

Internationale organisatie
Een organisatie en de daaronder vallende internationaal publiekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst (verdrag) tussen twee of meer landen.

3 Zie voor een omschrijving van de in de AVG gebruikte begrippen artikel 4 van de AVG.

1.2
Taskforce Beyond Privacy Shield en het Toetsingskader

Het uitgangspunt van de AVG is, zoals bekend, het bieden van een hoog beschermingsniveau aan natuurlijke personen op het gebied van persoonsgegevens. Het doorgeven van persoonsgegevens aan partijen in derde landen of aan internationale organisaties mag niet ten koste gaan van dit hoge beschermingsniveau.

Het is om die reden dat de AVG aanvullende verplichtingen in de vorm van doorgiftemechanismen voor doorgiften voorschrijft. Wat deze verplichtingen inhouden, is verduidelijkt en verscherpt in de uitspraak van het Europese Hof van Justitie in de zaak Schrems II[4]. Kort samengevat heeft het Hof geoordeeld dat het *Privacy Shield* als mechanisme voor het doorgeven van persoonsgegevens naar de Verenigde Staten niet rechtsgeldig is. Terwijl een ander doorgiftemechanisme dat op zich wél is (de *SCC)*, maar pas nadat is beoordeeld of er extra maatregelen nodig zijn. Ook de Europese toezichthouders, verenigd in de European Data Protection Board (EDPB), hebben aanbevelingen gepubliceerd over het onderwerp doorgifte[5].

Hoe dan ook, het dossier van doorgifte van persoonsgegevens zit niet bepaald in rustig vaarwater, getuige ook het recente adequaatheidsbesluit voor de Verenigde Staten (EU-US Data Privacy Framework) waarover later meer. Bovendien is het doorgeven van persoonsgegevens voor de leden van SURF geen hypothetisch geval[6]. Door toenemende digitalisering, (internationale) samenwerkingen in onderwijs en onderzoek en door groeiend gebruik van clouddiensten leeft bij veel leden van SURF de prangende vraag wat nu wel en wat niet is toegestaan bij doorgiften.

Het is tegen deze achtergrond dat SURF al snel na de uitspraak van het Europese Hof in de zaak Schrems II, een breed samengestelde expertgroep heeft opgericht: de *Taskforce Beyond Privacy Shield*, om precies die vraag te beantwoorden. De Taskforce is samengesteld door en voor de leden en bestaat uit deskundigen op het gebied van privacyrecht, inkoop en informatiebeveiliging. Ook Functionarissen Gegevensbescherming (FG’s) maken deel uit van de Taskforce.

4 HvJEU 16 juli 2020, C-311/18 (Schrems II).
5 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 november 2020.
6 Nederlandse universiteiten lopen voorop met het cloudgebruik in vergelijking met andere EU lidstaten. Tobias Fiebig, Seda Gürses, Carlos H. Gañán, Erna Kotkamp, Fernando Kuipers, Martina Lindorfer, Menghua Prisse, Taritha Sari, Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds, 27 juli 2021, URL: https://arxiv.org/abs/2104.09462.

Na de afronding van verschillende *use stories* op het gebied van onderwijs(logistiek), onderzoek en bedrijfsvoering, heeft de Taskforce dit Toetsingskader voor de doorgifte van persoonsgegevens ontwikkeld. Hiervoor vonden veel sessies met tal van deskundigen van binnen en buiten de Taskforce plaats. Hoewel de naam van de Taskforce anders doet vermoeden, is het Toetsingskader toepasbaar voor doorgiften naar alle derde landen.

Hoewel de naam van de Taskforce anders doet vermoeden, is het Toetsingskader toepasbaar voor doorgiften naar alle derde landen en niet alleen naar de Verenigde Staten.

1.3
Doel, gebruik en aard van het Toetsingskader

Het Toetsingskader voor doorgifte heeft tot doel de leden van SURF te ondersteunen bij de beoordeling of, en zo ja hoe, zij rechtmatig persoonsgegevens kunnen doorgeven aan derde landen of aan internationale organisaties.

Het zijn de individuele leden van SURF die het Toetsingskader uitvoeren. Dat veronderstelt in de eerste plaats bekendheid met welke (voorgenomen) doorgiften er zijn. Het vereist eveneens de aanwezigheid van voldoende capaciteit voor het goed en volledig uitvoeren van het Toetsingskader. Het is aan ieder lid om zelf te bepalen hoe dit vorm te geven en wie daarbij te betrekken.

Het Toetsingskader als hulpmiddel voor de toetsing van internationale doorgiften impliceert eveneens dat de leden ook zelf de afweging maken (en periodiek blijven maken) of zij een bepaalde doorgifte wel of niet laten doorgaan. Het doorlopen van de stappen helpt bij het maken van die afweging, maar leidt niet tot een vooraf bepaalde uitspraak of een bepaalde doorgifte rechtmatig is (of niet). De kenmerken van de specifieke doorgifte en de risico-afweging van het betreffende lid, zijn en blijven daarvoor doorslaggevend.

1.4
Relatie Toetsingskader en Data Transfer Impact Assessment (DTIA)

Naar aanleiding van de uitspraak in Schrems II, de aanbevelingen van de EDPB en de nieuwe *Standard Contractual Clauses* van de Europese Commissie (EC, waarover later meer) is een specifiek instrument veel belangrijker geworden: de *Data Transfer Impact Assessment* (DTIA).

> ***Het uitvoeren van een DTIA, zelfstandig of als onderdeel van een Data Protection Impact Assessment (DPIA), is verplicht wanneer doorgiften op basis van SCC plaatsvinden.***

Wat is een DTIA? Kort gezegd is het een onderzoek naar een specifieke doorgifte, de daaraan verbonden risico's en de mogelijkheden van beheersing van die risico's. Een DTIA heeft geen door de AVG of rechtspraak vastgelegde vorm of format. Relevant is dat met het toepassen van het Toetsingskader en de vastlegging daarvan, de leden kunnen aantonen dat zij een DTIA hebben uitgevoerd.

1.5
Doorgifte als op zichzelf staande verwerking waarop de AVG van toepassing is

De centrale opdracht en taakomschrijving van de Taskforce hebben betrekking op het vraagstuk van de doorgifte van persoonsgegevens. De uitgewerkte *use stories* en het Toetsingskader zien op doorgifte.

De doorgifte van persoonsgegevens is óók een verwerking van persoonsgegevens in de zin van de AVG (zie de uitspraak van het Europese Hof van Justitie in de zaak Schrems I)[7]. Dat betekent dat die verwerking moet voldoen aan alle eisen die de AVG stelt aan een verwerking van persoonsgegevens. Dus voor een doorgifte geldt eveneens het vereiste van onder andere (i) de aanwezigheid van een rechtsgrondslag voor verwerking, (ii) het toepassen van de beginselen uit artikel 5 AVG, (iii) het treffen van passende beveiligingsmaatregelen en (iv) het informeren van betrokkenen over de verwerking en doorgifte.

7 HvJEU 6 oktober 2015, C-362/14 (Schrems I).

Speciale aandacht verdient het vereiste van noodzakelijkheid, meer in het bijzonder de vraag of alternatieve, minder invasieve mogelijkheden voor doorgifte aanwezig zijn. Indien de verwerking mogelijk is in de EER, bijvoorbeeld omdat er daadwerkelijk alternatieven zijn (vanuit praktisch-, technisch-, en kostenoogpunt) dan kan dat betekenen dat de keuze moet vallen op verwerking binnen de EER in plaats van op het alternatief buiten de EER.

Indien de verwerking mogelijk is in de EER, bijvoorbeeld omdat er daadwerkelijk alternatieven zijn (vanuit praktisch-, technisch-, en kostenoogpunt) dan kan dat betekenen dat de keuze moet vallen op verwerking binnen de EER in plaats van op het alternatief buiten de EER.

1.6
Periodieke evaluatie van het Toetsingskader

In de inleiding is al aangegeven dat er volop discussie is over doorgifte van persoonsgegevens. Ontwikkelingen volgen elkaar snel op door rechterlijke uitspraken, besluiten en *guidance* van nationale en Europese toezichthouders en ook door ontwikkelingen binnen SURF op het gebied van *Vendor Risk Management* en *cloud controls*.

Daar komt bij dat de Taskforce in de komende periode op zoek gaat naar specifieke hulpmiddelen voor de nadere uitwerking van één of meerdere aspecten van het Toetsingskader. Daarbij valt te denken aan *tooling* voor het in kaart brengen en analyseren van wet- en regelgeving in derde landen en aan de ontwikkeling van nieuwe aanvullende maatregelen op vooral technisch gebied, zoals encryptie en sleutelmanagement.

Dit alles betekent dat het voorliggende Toetsingskader geen statisch stuk is, maar een dynamisch document dat door de Taskforce periodiek wordt geëvalueerd en – waar nodig – wordt herzien en aangevuld.

2.
Doorgifte van persoons-gegevens naar derde landen of naar inter-nationale organisaties

Het Toetsingskader kan worden gebruikt als er sprake is van (voorgenomen) doorgifte van persoonsgegevens naar derde landen of internationale organisaties. Dat roept de vraag op wanneer er sprake is van ‘doorgifte’, wat ‘derde landen’ zijn en wat een ‘internationale organisatie’ is.

2.1
Doorgifte

Wat een ‘doorgifte’ is, is in de AVG zelf niet gedefinieerd. In dit Toetsingskader is van doorgifte sprake als een data exporteur persoonsgegevens ter beschikking stelt aan een data importeur.

De begrippen data exporteur en data importeur zijn in onderdeel 1.1 gedefinieerd.

Het ‘ter beschikking stellen’ van persoonsgegevens is een breed begrip en kan onder meer inhouden het (ver)zenden van bestanden, het geven van inzage in onderzoeksresultaten en het opslaan van studentenadministraties in een cloudomgeving.

Voorbeelden van doorgifte

Gelet op het brede bereik van de begrippen ‘verwerking’, ‘data exporteur’ en ’data importeur’ is, ook in gevallen waar dit in eerste instantie niet voor de hand ligt, sprake van doorgifte. Onderstaande voorbeelden maken dit duidelijk.

Een lid van SURF gaat in het kader van de bedrijfsvoering een samenwerking aan met een leverancier in Frankrijk. De leverancier op zijn beurt heeft afspraken gemaakt met een hostingprovider in Duitsland. De Duitse partij host de persoonsgegevens die in deze samenwerking worden verwerkt op servers die fysiek in Duitsland staan.

In dit voorbeeld is het Toetsingskader niet van toepassing, want er is geen sprake van doorgifte buiten de Europese Economische Ruimte (EER).
Het Toetsingskader is al wel van toepassing als:

- De Franse en/of de Duitse leverancier onderdeel zijn van een groep van ondernemingen waarvan de moedermaatschappij is gevestigd in een land buiten de EER.
- De Duitse hostingpartij voor verschillende IT-aspecten een overeenkomst heeft gesloten met een IT-dienstverlener die is gevestigd in India. Medewerkers in India hebben in dat kader remote access vanuit India tot de persoonsgegevens die zijn opgeslagen in Duitsland.Hoewel de persoonsgegevens dus fysiek binnen de EER blijven, is toch sprake van doorgifte van persoonsgegevens.

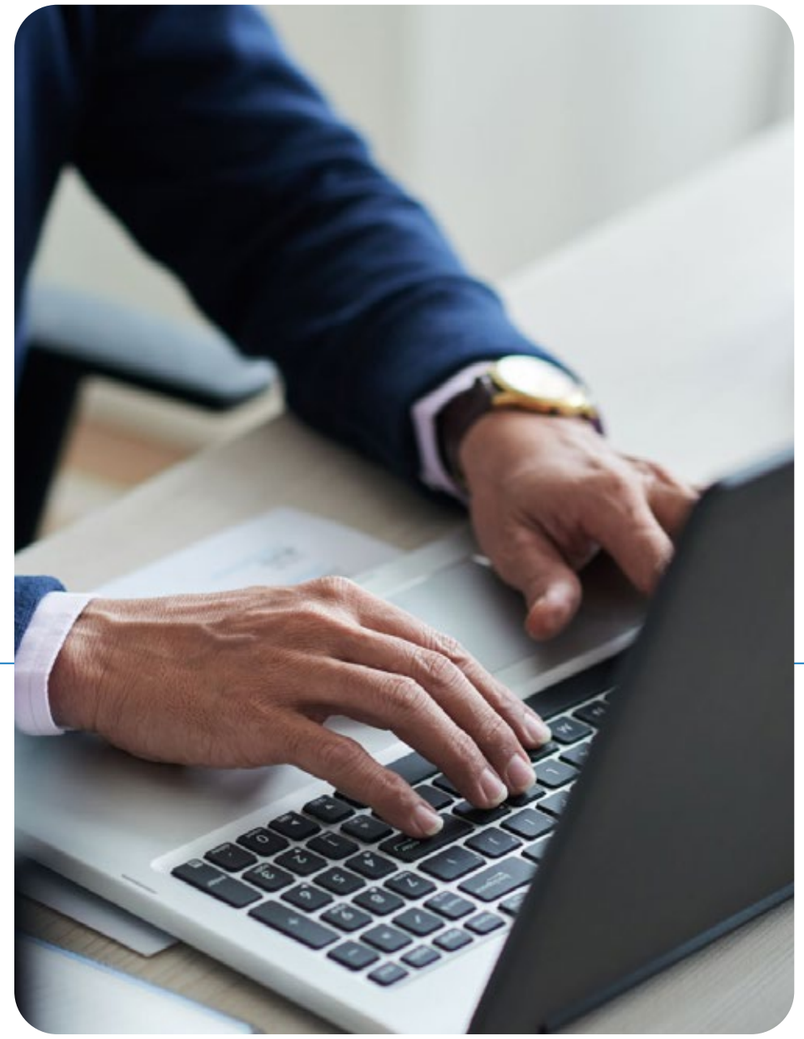
Overigens is eveneens sprake van doorgifte (en is het Toetsingskader van toepassing) als:

- De Duitse hostingpartij gebruikmaakt van diensten van dienstverleners in derde landen, bijvoorbeeld een Content Delivery Network of cloud security-dienst, maar ook voor analytics of voor het verzenden van mailings.

Voor alle duidelijkheid: van doorgifte is geen sprake als de betrokkene *zelf* direct persoonsgegevens ter beschikking stelt aan een partij in een derde land. Van doorgifte is evenmin sprake als een medewerker naar een derde land reist, in dat derde land inlogt op de laptop en vervolgens op afstand toegang (*remote access*) krijgt tot de database met persoonsgegevens van het bedrijf/instelling van de medewerker[8].

2.2
Derde landen en internationale organisaties

Voor doorgifte is verder relevant dat persoonsgegevens worden doorgegeven aan derde landen of internationale organisaties waarbij ‘derde landen’ alle landen buiten de EER zijn. En 'internationale organisaties' zijn organisaties zoals de Verenigde Naties (en de aan haar geaffilieerde organisaties zoals de ILO, de FAO, het IMF, de Wereldbank, Unicef, Unesco, UNHCR, etc.), de WHO, WTO en het Internationaal Strafhof. De organisaties van de Europese Unie worden *niet* gekwalificeerd als internationale organisatie. De leden van SURF geven in beperkte mate persoonsgegevens door aan internationale organisaties.



8 Een aantal verhelderende voorbeelden van wanneer wel en geen sprake is van doorgifte van persoonsgegevens is opgenomen in: Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0, adopted on 14 February 2023.

3.
Inventarisatie: wat zijn de kenmerken van de doorgifte?

Het startpunt van het Toetsingskader is het in kaart brengen van de specifieke kenmerken van de betreffende doorgifte door middel van het beantwoorden van onderstaande vragen (vanuit het perspectief van de data exporteur):

Vragen	Toelichting op de vragen
1e doorgifte	**Een 1e doorgifte heeft betrekking op de doorgifte van leden van SURF (data exporteur) aan een data importeur.**
Welke partij geeft de persoonsgegevens door en in welke hoedanigheid (verantwoordelijke of verwerker)?	Dit betreft voor een eerste doorgifte altijd een lid van SURF.
Welke partij(en) heeft (hebben) toegang tot de persoonsgegevens?	Geef een omschrijving van de (juridische) naam van de ontvangende partij(en).
In welk(e) land(en) is (zijn) deze partij(en) gevestigd?	Indien sprake is van een eerste doorgifte naar meerdere landen, geef alle landen op.
Wat is het doel van de betreffende doorgifte?	Zie de verschillende *use stories* voor onderwijs, onderzoek en bedrijfsvoering op de website van de SURF Taskforce Beyond Privacy Shield. Bijvoorbeeld hosting van administraties, clouddienstverlening, platform voor uitwisseling van onderzoeksdata, uitwisseling van studenten, etc.
Is de doorgifte incidenteel of heeft het een meer structureel/ doorlopend karakter?	Een incidentele doorgifte is bijvoorbeeld het eenmalig doorgeven van persoonsgegevens aan een ontvangende partij. Een voorbeeld is het eenmalig ter beschikking stellen van een specifieke set onderzoeksdata aan een onderzoeker in een derde land. Er is sprake van structurele doorgifte bij opslag van persoonsgegevens in de cloud of langlopende samenwerkingen op het gebied van onderwijs en onderzoek.
Is de ontvangende partij een verantwoordelijke, gezamenlijk verantwoordelijke, een verwerker of sub-verwerker?	Zie de AVG voor een begrip van de rollen in het kader van de AVG en de verplichtingen die uit die rol voortvloeien. **Let op!** Veel internationale clouddienstverleners bieden standaard verwerkersovereenkomsten aan die meestal alleen betrekking hebben op de content data die een instelling zelf aanlevert en niet op alle andere persoonsgegevens over het gebruik van de clouddiensten. Denk bij dat laatste aan: diagnostische gegevens, account-/ contactgegevens, supportgegevens en websitegegevens. Bekijk goed welke rol de ontvangende partij inneemt bij deze persoonsgegevens.
Welke 'normale' persoonsgegevens worden doorgegeven?	Het betreft alle persoonsgegevens die GEEN bijzondere persoonsgegevens zijn. Denk aan: naam, adres, e-mail, log-data, zakelijke telemetriedata, telefoonnummers, leeftijd, etc.
Welke bijzondere persoonsgegevens worden doorgegeven?	Bijzondere persoonsgegevens: Ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.
Welke gegevens van gevoelige aard worden doorgegeven, waarvoor dus extra waarborgen nodig zijn?	Denk aan gegevens over surfgedrag, inhoud van communicatie, zoekindexen, andere inhoudelijke gegevens zoals bestands- of padnamen, locatiegegevens, financiële gegevens zoals inkomen/ salaris en rekeningnummers en gegevens over minderjarigen.

Vragen	Toelichting op de vragen
Wie zijn de (categorieën van) betrokkenen in/bij de doorgifte?	Bijvoorbeeld medewerkers, systeembeheerders, studenten, patienten, onderzoekers, alumni, etc.
In welk(e) land(en) worden de persoonsgegevens opgeslagen?	Vaak is dit het land waar de partij is gevestigd, maar het kan ook een ander land zijn. Een voorbeeld is een afspraak met een partij uit India die de persoonsgegevens host in de Verenigde Staten.
Wat zijn de organisatorische en technische beveiligingsmaatregelen die zien op de doorgifte?	Indien er geen specifieke maatregelen zijn voor alleen de doorgifte, kan worden volstaan met een meer generieke beschrijving van de maatregelen.
Verdere doorgiften	**Het kan voorkomen dat een data importeur bepaalde persoonsgegevens op zijn beurt doorgeeft aan een partij in een ander derde land. De data importeur wordt daarmee data exporteur. Deze doorgiften dienen ook in kaart te worden gebracht.**
Welke partij(en) heeft (hebben) toegang tot de persoonsgegevens?	Dit betreft de partijen die van de eerste data importeur de persoonsgegevens ontvangen.
Welke persoonsgegevens maken deel uit van de verdere doorgifte(n)?	Dit kunnen dezelfde persoonsgegevens zijn die hierboven zijn opgesomd. Het kan ook een kleinere subset betreffen.
Welke derde landen ontvangen de persoonsgegevens?	Hier kan worden volstaan met een opsomming van de derde landen aan wie de data importeur de persoonsgegevens doorgeeft.

Tevens is het in deze inventarisatie nodig om de verdere doorgiften in kaart te brengen: de keten van doorgiften. In sommige gevallen is sprake van doorgifte aan één data importeur. In andere gevallen kan die data importeur bepaalde persoonsgegevens weer doorgeven aan een andere partij in een derde land[9]. Zo kan er sprake kan zijn van een lange keten van doorgiften met persoonsgegevens.

De vraag komt op wie deze inventarisatie dient uit te voeren? Is dat de data exporteur die zich kwalificeert als verwerkingsverantwoordelijke of is dat ook (of juist) de data importeur? En als een rol is weggelegd voor de data importeur, is dat dan ook het geval wanneer deze zich kwalificeert als verwerker of sub-verwerker? Het antwoord op deze vragen is belangrijk, aangezien de leden van SURF als data exporteur niet al deze vragen zelf kunnen beantwoorden, zeker wanneer er sprake is van een uitgebreide keten van doorgiften.

Juridisch kan goed worden betoogd dat de data importeur de inventarisatie dient uit te voeren ongeacht of deze (gezamenlijk) verantwoordelijke of verwerker is. Uitgangspunt bij de toepassing van de inventarisaties van hoofdstukken 3 en 5 is dat de leden van SURF vooral de data importeur moeten betrekken.

In het kader van de verantwoordingsplicht is het raadzaam om de antwoorden op deze vragen schriftelijk vast te leggen.

9 De data importeur wordt voor die doorgifte dan de data exporteur en de ontvangende partij de data importeur.

4.
Keuze: welk doorgifte-mechanisme is mogelijk?

Een specifieke verplichting voor de doorgifte van persoonsgegevens naar een derde land of internationale organisatie is dat *elke* doorgifte alleen mogelijk is via een doorgiftemechanisme. Deze mechanismen, die een zekere hiërarchie kennen, zijn limitatief opgesomd in de AVG en zijn in volgorde van voorkeur:

4.1
Adequaatheidsbesluit

Bovenaan de hiërarchie staat een adequaatheidsbesluit van de Europese Commissie (EC) voor een derde land. Een dergelijk besluit houdt in dat de EC van oordeel is dat de wetten en praktijken van dat derde land op het gebied van privacy en gegevensbescherming een 'passend beschermings-niveau' bieden en waarborgen. Een dergelijk besluit komt tot stand na zeer uitvoerig onderzoek door de EC. Voor de volgende landen heeft de EC een adequaatheidsbesluit genomen.

Landen met een adequaatheidsbesluit (stand van zaken op 14 juli 2023):

- Andorra
- Argentinië
- Canada (enkel ten aanzien van commerciële bedrijven en het geldt niet voor gegevens van werknemers); bekijk hier de toelichting.
- Faeröer eilanden
- Guernsey
- Israël
- Verenigd Koninkrijk en Isle of Man
- Japan
- Jersey
- Nieuw-Zeeland
- Uruguay
- Zwitserland
- Zuid-Korea
- Verenigde Staten (ten aanzien van gecertificeerde organisaties, zie voor meer informatie: www.dataprivacyframework.gov)

Belangrijk: als leden van SURF persoonsgegevens willen doorgeven aan één van deze landen, dan is strikt genomen géén actie nodig. Het Toetsingskader hoeft dan niet verder te worden doorlopen. Dat laat onverlet dat leden van SURF ook bij aanwezigheid van een dergelijk besluit wel degelijk kunnen kiezen voor extra aanvullende maatregelen.

Het is goed om te bedenken dat een adequaatheidsbesluit een beperkte geldigheidsduur heeft (die overigens wel kan worden verlengd). Een bestaand adequaatheidsbesluit kan bovendien door het Europees Hof van Justitie ongeldig worden verklaard. De leden van SURF wordt derhalve geadviseerd:

1. bij aanvang van de doorgifte goed te kijken of het betreffende besluit (nog) geldig is en - dit geldt voor doorgiften aan de VS - of de organisatie aan wie wordt doorgegeven daadwerkelijk is gecertificeerd, en
2. gedurende de doorgifte na te gaan of er iets wijzigt in de status van het adequaatheidsbesluit.

Daarnaast staat het de leden van SURF uiteraard vrij, ook bij het bestaan van een geldig en toepasselijk adequaatheidsbesluit, aanvullende maatregelen te treffen. Bijvoorbeeld vanwege het risico-profiel van de doorgifte zelf, op basis van de analyse bij de data importeur in het betreffende land dan wel de praktijken in het land waarvoor het adequaatheidsbesluit is afgegeven.

4.2.
Passende waarborgen

4.2.1 Inleiding

Als er geen adequaatheidsbesluit is (zoals bijvoorbeeld voor grote landen als India en China), dan biedt de AVG de volgende passende waarborgen op grond waarvan doorgifte kan plaatsvinden:

Passende waarborgen

- Juridisch bindend en afdwingbaar instrument tussen overheidsinstanties of -organen.
- Bindende bedrijfsvoorschriften (Binding Corporate Rules – BCR) die zijn goedgekeurd door de Autoriteit Persoonsgegevens (AP) of door een andere bevoegde EU AVG toezichthouder.
- Modelcontract EC (Standard Contractual Clauses – SCC).
- Modelcontract opgesteld door de AP.
- Een door de AP goedgekeurde gedragscode.
- Een door de AP goedgekeurd certificeringsmechanisme
- Door de AP goedgekeurde contractbepalingen tussen partijen.

Op dit moment komt een aantal van de in de AVG genoemde waarborgen niet voor toepassing in aanmerking.

1. De Autoriteit Persoonsgegevens (AP) heeft voor zover bekend nog geen modelcontracten opgesteld en nog geen gedragscode voor doorgifte goedgekeurd. Er is ook geen sprake van een goedgekeurd certificeringsmechanisme voor partijen waarop de AVG niet van toepassing is. Het Europees Comité voor Gegevensbescherming heeft tot nu toe één algemene gedragscode voor cloudproviders goedgekeurd[10], maar die is uitdrukkelijk niet bedoeld als specifieke gedragscode voor doorgifte.
2. Aangezien de leden van SURF geen onderdeel zijn van een internationale groep van ondernemingen met vestigingen in derde landen, zal ook van de toepassing van BCR meestal geen sprake kunnen zijn.

Een belangrijke uitzondering geldt voor de gevallen waarin een lid van SURF persoonsgegevens doorgeeft aan een data importeur die verwerker is en waarvoor die data importeur – als onderdeel van een groep van ondernemingen – BCR zijn goedgekeurd door de toezichthoudende autoriteit. Een laatste overzicht van de goedgekeurde BCR zijn hier te vinden.

Als een lid van SURF van deze passende waarborg gebruik kan en wil maken, is verdere uitvoering van het Toetsingskader vereist.

3. De Taskforce is niet bekend met de aanwezigheid van bindende en afdwingbare instrumenten tussen overheidsinstanties of -organen, zodat ook deze passende waarborg niet voor toepassing in aanmerking lijkt te komen.

10 EDPB, Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE), 19 May 2021, URL: https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202117_cispecode_en_0.pdf.

Let op!
Op dit moment komt eigenlijk alleen de modelovereenkomst – de versie van juni 2021 - van de EC (de SCC) als passende waarborg voor toepassing in aanmerking. Zoals blijkt uit de door de Taskforce opgestelde use stories, is de huidige praktijk van de leden van SURF ook dat bijna exclusief van dit doorgiftemechanisme gebruik wordt gemaakt. In het vervolg van dit Toetsingskader zal derhalve alleen aan deze passende waarborg aandacht worden besteed.

De huidige SCC zijn niet geschikt als passende waarborg bij doorgiften aan internationale organisaties. De EC is voornemens speciale SCC op te stellen voor deze situatie.

4.2.2 De Standard Contractual Clauses

De SCC vormen een gestandaardiseerd modelcontract dat is opgesteld door de EC. Er zijn twee soorten SCC:

1. een modelverwerkersovereenkomst voor gebruik tussen partijen binnen de EER, en
2. een aparte modelovereenkomst voor doorgifte vanuit de EER naar derde landen[11].

Dit kader gaat alleen over die tweede modelovereenkomst, die door (gezamenlijk) verantwoordelijken en verwerkers in de EER kan worden gebruikt voor doorgifte naar derde landen. In het kort zijn dit de de SCC bepalingen die moeten waarborgen dat in het derde land sprake is van een passend beschermingsniveau voor de doorgegeven persoonsgegevens.

Op 4 juni 2021 heeft de EC nieuwe SCC opgesteld (ter vervanging van de SCC die nog dateerden van voor de AVG), waarbij rekening is gehouden met meerdere doorgiftescenario's. Dit Toetsingskader gaat niet uitvoerig in op de inhoud van de SCC. Vooral relevant in het kader van het Toetsingskader is het volgende:

11 Zie de toelichting van de Europese Commissie op https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf

1. De SCC kent een algemeen deel en een modulaire opbouw waarbij rekening is gehouden met 4 scenario's van data exporteur en data importeur:

   Module 1
   Doorgifte van verantwoordelijke naar een verantwoordelijke buiten de EER.

   Module 2
   Doorgifte van verantwoordelijke naar een verwerker buiten de EER.

   Module 3
   Doorgifte van verwerker naar een sub-verwerker buiten de EER.

   Module 4
   Doorgifte van verwerker naar een verantwoordelijke buiten de EER.

2. De SCC kunnen voor een bepaalde doorgifte worden afgesloten door meerdere data exporteurs en data importeurs. Bovendien bestaat de mogelijkheid dat andere partijen als data exporteur of data importeur op een later tijdstip aansluiten (al dan niet via een andere module), zodat ook zij gebonden zijn aan de SCC. Deze bepaling is vooral relevant als in de keten van doorgiften sprake is van meerdere doorgiften (zie hiervoor).

3. De data exporteur en data importeur mogen de SCC *niet* wijzigen. Alleen het toevoegen van bepalingen die meer bescherming bieden aan betrokkenen is toegestaan, zoals bijvoorbeeld de beschrijving (voorbeeld in de bijlagen van de SCC) van de eventuele *aanvullende* maatregelen die een lid van SURF treft na het doorlopen van het Toetsingskader.

4. De bijlagen bij de SCC moeten volledig worden ingevuld door de data exporteur en/of de data importeur. De inventarisaties van dit Toetsingskader bieden daarvoor belangrijke input.

5. Indien module 2 van toepassing is dan kan hiermee worden volstaan. Strikt genomen is dan een aparte verwerkersovereenkomst naast de SCC niet nodig. Let bij het gebruik van alleen de SCC goed op welke persoonsgegevens onderdeel zijn van de SCC. Zo komt het bij dienstverleners in de Verenigde Staten wel voor dat de SCC zich alleen richten op *customer content data* zoals dit is gedefinieerd door de dienstverlener. Het gevolg is dan dat andere persoonsgegevens niet vallen onder het toepassingsbereik van de SCC.

6. Een belangrijk onderdeel van de nieuwe SCC is artikel 14. Uit dit artikel vloeit onder meer voort dat in ieder geval moet worden onderzocht of het recht van het derde land de data importeur niet belemmert in het (kunnen) voldoen aan de verplichtingen uit de SCC.

4.2.3 Aanvulling(en) op de SCC

In de zaak Schrems II heeft het Europees Hof van Justitie geoordeeld dat het gebruik van de SCC op zichzelf rechtsgeldig is, maar dat de specifieke doorgifte aanleiding kan geven voor het nemen van *aanvullende* maatregelen, om zo een *passend* beschermingsniveau mogelijk te maken.

> *Let wel: in tegenstelling tot adequaatheidsbesluiten, is het bij de SCC dus nog wél van belang dat de leden van SURF goed kijken of de aard van de betreffende doorgifte noopt tot het nemen van aanvullende maatregelen.*

Het Toetsingskader helpt bij het bepalen van de risico-inschatting van de doorgifte en het vervolgens besluiten tot het nemen van aanvullende maatregelen; hoe hoger het risicoprofiel, hoe meer aanvullende maatregelen (van veelal technische aard) nodig zijn.

De inschatting van een SURF-lid kan ook zijn dat de risico's op basis van een risico-inschatting te groot zijn of dat de aanvullende maatregelen te beperkt zijn, waarmee er geen sprake is van een passend beschermingsniveau. In dat geval kan de doorgifte op basis van de SCC geen doorgang vinden.

Aandachtspunten bij het gebruik van SCC

Kies de juiste module van de SCC, op basis van de rollen van data exporteur en importeur, zoals vastgesteld in de inventarisatie van de doorgifte.

Maak van de SCC geen 'papieren tijger'. Ga na of de data importeur feitelijk kan voldoen aan de bepalingen van de SCC. Overigens is dat ook een verplichting die volgt uit artikel 14 van de SCC.

4.3.
Specifieke uitzonderingssituaties

Als er geen adequaatheidsbesluit is en ook de passende waarborgen niet leiden tot een adequaat beschermingsniveau, kan doorgifte alleen plaatsvinden als is voldaan aan één van onderstaande (strenge) uitzonderingsregels. Als één van deze uitzonderingen van toepassing is, is verdere toepassing van het Toetsingskader niet langer nodig.

De specifieke uitzonderingsgevallen zijn:

- Uitdrukkelijke toestemming van betrokkene, waarbij de betrokkene ook goed wordt geïnformeerd over de specifieke risico's die zijn verbonden aan de doorgifte.
- Noodzakelijke doorgifte voor de uitvoering of sluiting van een overeenkomst tussen betrokkene en verwerkingsverantwoordelijke.
- Noodzakelijke doorgifte voor het sluiten of uitvoeren van een overeenkomst in het belang van betrokkenen.
- Noodzakelijke doorgifte wegens gewichtige redenen van algemeen belang.
- Noodzakelijke doorgifte voor de instelling, uitvoering of onderbouwing van een rechtsvordering.
- Noodzakelijke doorgifte voor bescherming vitale belangen betrokkene of van andere personen.
- Doorgifte vanuit een (semi)openbaar register.
- Niet repetitieve doorgifte van gegevens van een beperkt aantal betrokkenen wegens dwingende gerechtvaardigde belangen (restcategorie).

De specifieke uitzonderingsgevallen zijn precies dat; uitzonderingen voor hele specifieke situaties. De uitzonderingen dienen restrictief te worden uitgelegd en toegepast. Dat houdt waarschijnlijk in dat toepassing alleen aan de orde is bij een incidentele doorgifte en als het niet al te veel betrokkenen betreft. Overigens gelden sommige van de uitzonderingen niet voor de leden van SURF die zich kwalificeren als overheidsinstantie en waarbij de doorgifte deel uitmaakt van de uitoefening van openbare bevoegdheden.

De eis van 'noodzakelijkheid' dwingt bovendien alleen al tot de nodige terughoudendheid. Het toepassen van een uitzonderingsgeval, waar mogelijk, betekent ook een zware last op de leden van SURF in het kader van het goed toelichten en onderbouwen van de toepassing van het uitzonderingsgeval[12].

12 Raadpleeg bij twijfel de uitgebreide uitleg van de EDPB in de Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

5.
Inventarisatie: wie is de data importeur?
Wat is de toepasselijke wet- en regelgeving en wat zijn de gangbare praktijken in het derde land?

Het onderzoek naar de data importeur en de toepasselijke wet- en regelgeving (en gangbare praktijken) in het derde land is een wezenlijk onderdeel van het Toetsingskader (en voor het maken van de risico-inschatting).

Zo spreekt het voor zich dat het risico van doorgifte groter wordt naarmate de data importeur niet wil of kan voldoen aan de eisen rond gegevensbescherming. En ook in landen waar opsporingsinstanties veel mogelijkheden hebben voor het opvragen van allerlei persoonsgegevens (waaronder telemetrie en andere metadata) bij data importeurs, is sprake van risico's voor de betrokkenen. En dat geldt evenzeer voor landen waar betrokkenen geen of zeer beperkte mogelijkheden hebben om effectief bezwaar aan te tekenen of naar de rechter te stappen voor een onafhankelijk oordeel.

Kortom, er zijn genoeg redenen deze aspecten te onderzoeken. Vanwege de beschikbare tijd en/of capaciteit bij de leden van SURF is dit geen gemakkelijke opgave.

Los van de (on)mogelijkheden voor de leden van SURF deze vragen te kunnen beantwoorden komt de vraag op wie deze inventarisatie eigenlijk moet doen. Is dat de data exporteur zelf? Kan de data exporteur dit onderzoek laten doen door de data importeur? Of is het juist de data importeur die hiertoe een zelfstandige verplichting heeft?

Let op!
Uitgangspunt van dit Toetsingskader is dat het lid van SURF als data exporteur hier een zelfstandige verantwoordelijkheid heeft, MAAR dat de data importeur actief ondersteuning dient te verlenen, aangezien de data importeur ook de meest aangewezen partij is om deze vragen te beantwoorden. Het verdient aanbeveling dit uitgangspunt in de (privacy)overeenkomst met de data importeur ook contractueel vast te leggen.

Onderstaand zijn de vragen naar de data importeur en wet- en regelgeving (en gangbare praktijken) in het derde land opgenomen.

Vragen	Toelichting op de vragen
Vragen over de data importeur	
Check de website en het privacy statement van de data importeur.	De mate van aanwezigheid en afwezigheid van informatie op de website en/of een privacystatement is een indicatie van het privacybewustzijn van de data importeur. Daarnaast biedt deze informatie, indien aanwezig, ook antwoord op de vraag of de data importeur de persoonsgegevens bijvoorbeeld ook voor eigen doeleinden – statistisch/verbeteren product, etc. – gebruikt.
Wie is de FG of contactpersoon voor vragen rond de doorgifte en privacy?	De aanwezigheid van een contactpersoon – en zeker als dat een FG is - kan een indicatie zijn dat privacy als belangrijk wordt gezien.

Vragen	Toelichting op de vragen
Is de data importeur gecertificeerd?	Indien de data importeur gecertificeerd is, dan is de vraag welke certificering dit betreft, bijvoorbeeld ISO 27001 en/of een SOC-2 audit? Per wanneer en hoe lang is de certificering nog geldig? En wat is de scope van die certificering?
Heeft de data importeur zelf risico-assessments, DPIA, DTIA's en/of audits uitgevoerd?	Grotere data importeurs dan wel de data importeurs die veel zaken doen met Europese partijen zijn de vragen van data exporteurs vaak voor. Zij hebben dan zelf DPIA's, DTIA's en/of audits (SOC-2) uitgevoerd. Deze self assessments geven een inkijk in hoe de data importeur zelf de risico's van verwerkingen en doorgiften inschat en welke (aanvullende) maatregelen zij hebben getroffen. Deze documenten zijn een waardevolle bron van informatie voor de data exporteurs.
Doe een check op de juridische, organisatorische en technische beveiligingsmaatregelen van de data importeur (zoals opgenomen in de SCC). Vraag eventueel documentatie op, waaronder beleidsstukken en bevindingen van audits.	In het kader van SCC zijn partijen verplicht op te nemen welke beveiligingsmaatregelen zijn getroffen voor een veilige doorgifte. In de gevallen waarin de data importeur voorstellen doet, verdient het aanbeveling deze maatregelen te toetsen. Zijn zij voldoende? Zijn deze maatregelen daadwerkelijk geïmplementeerd in de organisatie van de data importeur? Is er zicht op de (goede) werking van die maatregelen?
Check of er de mogelijkheid is om zelf technische testen uit te voeren, waaronder pentesten. Indien dergelijke testen door de data importeur zijn uitgevoerd, vraag dan de resultaten hiervan op.	

Vragen	Toelichting op de vragen
Vragen over wet- en regelgeving en gangbare praktijken in het derde land	**Als de data importeur gebruikmaakt van (sub)leveranciers in andere derde landen, dan dienen onderstaande vragen ook voor dat betreffende land te worden beantwoord.**
Is er in het derde land wet- en regelgeving die toeziet op de bescherming van persoonsgegevens?	Geef een korte omschrijving van de algemene wet- en regelgeving, maar ook eventuele specifieke/sectorale wet- en regelgeving.
Is er in het derde land wet- en regelgeving op grond waarvan overheidsorganisaties in dat land de data importeur kunnen dwingen toegang te verlenen tot persoonsgegevens?	Zo ja, geef een korte toelichting welke wet- en regelgeving het betreft en geef ook het volgende aan: - Zijn de wetten en regels duidelijk, toegankelijk en beschikbaar? - Zijn er onafhankelijke toezichtmechanismen? - Is er een doeltreffende rechtsingang, ook voor burgers uit andere landen dan het derde land?
Is de bestaande en relevante wet- en regelgeving ook daadwerkelijk van toepassing op de data importeur?	De mogelijkheid bestaat dat er wet- en regelgeving is, maar dat deze niet van toepassing is op (i) het bedrijf of de organisatie van de data importeur, (ii) het type betrokkenen en/of (iii) de aard van de persoonsgegevens. Dat hangt af van het materiële en/of territoriale toepassingsbereik van die wet- en regelgeving.
Als de relevante wet- en regelgeving van toepassing is, zijn er dan wettelijke mogelijkheden voor de data importeur en/of betrokkene, om effectief bezwaar/beroep aan te tekenen, tegen het verzoek van overheidsorganisaties?	Het al dan niet bestaan van effectieve mogelijkheden tot bezwaar en verzet zijn belangrijke aspecten in het bepalen van het risicoprofiel van een doorgifte.

Vragen	Toelichting op de vragen
Heeft de data importeur toegang tot ongecodeerde persoonsgegevens (clear text)?	Als de data importeur een dergelijke toegang niet heeft, dan bemoeilijkt dat de toegang tot die persoonsgegevens door autoriteiten door derde landen.
Hoe vaak heeft de data importeur in de afgelopen 3 jaar een verzoek ontvangen van overheidsinstanties dat betrekking heeft op de persoonsgegevens van de data exporteur?	De aan- of afwezigheid van verzoeken van nationale overheidsdiensten is een indicatie van het risicoprofiel van de doorgifte. De verzoeken, indien hieraan gehoor wordt gegeven, kunnen ook betrekking hebben op inzage of afgifte van die persoonsgegevens en kunnen zien op totaalaantallen voor Europa in zijn geheel.
Wat is de reactie van de data importeur als een dergelijk verzoek wordt ontvangen?	De data importeur dient duidelijk aan te geven welke acties en maatregelen hij treft, wanneer hij een dergelijk verzoek ontvangt. Denk aan het weigeren te voldoen aan het verzoek, het aantekenen van bezwaar, het informeren van de data exporteur, het tijdelijk stopzetten van (verdere) verwerking, etc.
Is het waarschijnlijk dat de aard van de dienstverlening van de data importeur - en soortgelijke bedrijven of organisaties - zodanig is dat overheidsinstanties interesse hebben in de persoonsgegevens van de data exporteur?	De aard van de diensten en werkzaamheden van de data importeur, al dan niet in combinatie met de aard van de persoonsgegevens en of/betrokkenen, kunnen zodanig zijn dat de overheidsinstanties in het geheel geen of weinig interesse hebben in toegang tot die persoonsgegevens, waardoor de kans op inzage slechts een theoretische kan zijn.

Een actieve inzet van de data importeur blijft nodig[13]. Eén van de beoogde aankomende activiteiten van de SURF Taskforce Beyond Privacy Shield is om na te gaan welke tools beschikbaar zijn voor de check op relevante wet- en regelgeving en gangbare praktijken. Dergelijke instrumenten kunnen de werklast verlichten.

Tot slot volgen hier nog enkele praktische tips voor deze inventarisatie:

1. Voor een beperkte check op de aanwezigheid van privacy wetgeving, zie de landkaart van advocatenkantoor DLA Piper: https://www.dlapiperdataprotection.com
2. Doe een check via internet op (i) het bestaan (en bevoegdheden) van een toezichthoudende autoriteit in het derde land, (ii) de mogelijkheden rechten uit te oefenen en (iii) de aanwezigheid van *transparancy reports*.
3. Uitgangspunt is dat de leden van SURF mogen vertrouwen op de juistheid en volledigheid van de door de data importeurs verstrekte informatie en documentatie. Dat is anders als blijkt dat:
   - de data importeur geen (of heel beperkt) antwoorden geeft;
   - die antwoorden onmiskenbaar onjuist of onvolledig blijken te zijn;
   - er anderszins redenen zijn aan om te nemen dat de data importeur niet te goeder trouw is bij het geven van de gevraagde informatie, en/of;
   - de informatie/antwoorden uit de hiervoor gestelde vragen aanleiding geven tot nader onderzoek of zelfs reden zijn om af te zien van doorgifte naar deze data importeur.

13 Zie ook: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, para. 44.

6.
Risico-inschatting:
wat is de weging van de risico's van de specifieke doorgifte?

Nadat de inventarisatie is afgerond, is de volgende stap in te schatten wat de risico's zijn van de datadoorgifte voor betrokkenen.

6.1.
Handelingsperspectief

De inschatting van dat risico geeft de leden van SURF een handelingsperspectief. Zo kan een inherent hoog risico betekenen dat de instelling niet kan instaan voor het vereiste hoge niveau van bescherming van de doorgegeven persoonsgegevens. In dat geval moet het lid van SURF op zoek gaan naar maatregelen om dat risico te verlagen. Het lid kan, eventueel gezamenlijk met andere leden via SURF, een traject starten met de beoogd data importeur om diens waarborgen te verbeteren, zodat risico's voldoende zijn gemitigeerd. De DPIA trajecten[14] die vanuit SLM Rijk en SURF zijn uitgevoerd zijn voorbeelden van zo'n aanpak. Het lid kan ook besluiten om af te zien van de voorgenomen doorgifte of op zoek te gaan naar een privacy-vriendelijker alternatief bij een andere dienstverlener.

Kortom, de risico-inschatting van de doorgifte is van belang voor het lid van SURF om het eigen handelingsperspectief te identificeren en te bepalen welke (eventuele) extra maatregelen en waarborgen getroffen moeten worden.

6.2.
Risicogebaseerd?

In artikel 24 lid 1 AVG is – kort gezegd - bepaald dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen treft bij verwerkingen van persoonsgegevens.

14 Zie bijvoorbeeld: https://www.surf.nl/uitkomsten-van-data-protection-impact-assessment-dpia-op-microsoft-onedrive-sharepoint-en-teams.

Wat 'passend' is, is afhankelijk van een aantal factoren, waaronder aard, omvang, context en doel van de verwerking maar ook van

> *"(...) de qua **waarschijnlijkheid** en **ernst** uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen (...)".*

Het valt dus onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, ook in de rol van data exporteur, om 'risicogebaseerd'[15] passende waarborgen te nemen voor verwerkingen van persoonsgegevens. Zoals hierboven al is aangegeven, is de doorgifte van persoonsgegevens óók een verwerking[16].

Bij het maken van een risico-inschatting dienen door de leden van SURF (als verwerkingsverantwoordelijke) de *waarschijnlijkheid* en de *ernst* van het betreffende risico afgewogen te worden. Hiermee sluit de AVG aan bij de gangbare interpretatie van een risico als het product van *kans* maal *impact*. Maar wat is dan een doorgifte risico? En waar moet rekening mee worden gehouden?

15 Er bestaat enige discussie over de reikwijdte van het begrip 'risk based' in de AVG, waarbij de EDPB in concrete uitspraken een iets andere interpretatie heeft dan de Europese wetgever. Voor nadere toelichting op dit onderscheid zie: Lokke Moerel, What happened to the Risk Based Approach to Data Transfers? How the EDPB is rewriting the GDPR. Online: https://fpf.org/wp-content/uploads/2022/09/FPF-Guest-Blog-What-Happened-to-the-Risk-Based-Approach-of-Data-Transfers.doc.pdf. Ook Paul Breitbarth analyseert de legitimiteit en de scope van het begrip risk based in zijn artikel: A Risk-Based Approach to International Data Transfers. EDPL, 2021, pp. 539 – 549. Online: https://edpl.lexxion.eu/data/article/17963/pdf/edpl_2021_04-010.pdf. Dit is ook in lijn met de Draft Statement of the Council's reasons (2012/0011 (COD)): "In order to achieve the objectives of the Regulation, the Council Position at first reading strengthens the accountability of controllers (responsible for determining the purposes and the means of the processing of personal data) and processors (responsible for processing personal data on behalf of the controller) so as to promote a real data protection culture. Against that background, throughout the Regulation, a risk-based approach is introduced which allows for the modulation of the obligations of the controller and the processor according to the risk of the data processing they perform." Zie pg 4: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_ADD_1&from=EN De EC bevestigt vervolgens opnieuw de risk-based approach: "Ook handhaaft en ontwikkelt het akkoord de op risico gebaseerde benadering die al in het voorstel van de Commissie was vervat, nl. dat verwerkingsverantwoordelijken, en in bepaalde gevallen de verwerkers, rekening moeten houden met de aard, het toepassingsgebied, de context en de doeleinden van de verwerking en met de waarschijnlijkheid en de ernst van de risico's voor de rechten en vrijheden van degene wiens persoonsgegevens worden verwerkt." Zie pg 4, MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT overeenkomstig artikel 294, lid 6, van het Verdrag betreffende de werking van de Europese Unie over het standpunt van de Raad betreffende de vaststelling van een verordening 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 (algemene verordening gegevensbescherming) en tot intrekking van Richtlijn 95/46/EG: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52016PC0214&from=en. Ook in haar recente (2023) publicatie spreekt de EDPB deze risico gebaseerde benadering niet tegen. Zie: 2022 Coordinated Enforcement Action. Use of cloud-based services by the public sector. Adopted on 17 January 2023. Online: https://edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf.

16 Zie: HvJEU 6 oktober 2015, C-362/14 (Schrems I). EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0. Adopted on 18 June 2021. Online: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf#page=15.

Volgens het Europese Hof van Justitie in de Schrems II uitspraak[17] dient bij die beoordeling in het kader van een doorgifte rekening te worden gehouden met *"(...) de contractuele bepalingen die zijn overeengekomen tussen de in de Europese Unie gevestigde verwerkingsverantwoordelijke of zijn in de Europese Unie gevestigde verwerker en de in het betrokken derde land gevestigde ontvanger van de doorgifte, als, wat een eventuele toegang van de overheidsinstanties van dat derde land tot de doorgegeven persoonsgegevens betreft, de relevante aspecten van het rechtsstelsel van dat derde land (...)."* Het Hof benoemt twee elementen dat, vertaald voor de leden van SURF, het volgende betekent en inhoudt.

1. *De contractuele bepalingen tussen het lid van SURF en de dienstverlenende partij in het derde land*, moeten voldoende (waar)borgen bieden, eventueel met aanvullende maatregelen, zodat het beschermingsniveau van de doorgegeven persoonsgegevens gelijkwaardig (*'essentially equivalent'*[18]) is aan het niveau zoals gesteld in de AVG. Het Hof oordeelt in Schrems II dat die maatregelen toezien op waarborgen voor de betrokkenen. Die waarborgen moeten de naleving van gegevensbeschermingsvereisten en de geldende rechten van de betrokkenen waarborgen. Het betreft dan onder meer, aldus het Hof, de beschikbaarheid van afdwingbare rechten van betrokkenen en van doeltreffende beroepsmogelijkheden in de Europese Unie of in een derde land[19].

In de praktijk betekent dat hoofdzakelijk:

- Toepassing van de juiste modules uit de SCC.
- Het eventueel treffen (en opnemen in de SCC) van aanvullende maatregelen zoals strikte doelbinding voor alle soorten persoonsgegevens in de (verwerkers)overeenkomst, pseudonimisering, versleuteling van de persoonsgegevens, data minimalisatie, verkorte bewaartermijnen, etc.
- Teneinde ervoor te zorgen dat de persoonsgegevens ook na doorgifte beschermd blijven op een adequaat niveau, moet de instelling niet alleen contractuele garanties afdwingen van de data importeur, maar ook technische beschermingsmaatregelen treffen.

17 Zie: ECLI:EU:C:2020:559, para 105 en 203 lid 2. Online: https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=NL.

18 Zie: ECLI :EU :C :2020 :559, para 105. Noot: De Nederlandse vertaling: "in grote lijnen" wijkt teveel af van de Engelse betekenis van "essentially equivalent". De Engelse tekst (en betekenis) prevaleert, omdat procestaal Engels was.

19 Zie : ECLI :EU :C :2020 :559, para 131.

2. *De mate waarin overheidsinstanties van dat derde land toegang hebben tot de doorgegeven persoonsgegevens,* bijvoorbeeld op basis van wat als 'problematische wetgeving' van dat derde land wordt gekarakteriseerd.

Het begrip 'problematische wetgeving' betreft onder meer *massa-surveillance* door bijvoorbeeld Amerikaans overheidsdiensten op basis van Amerikaanse wetgeving. Dit gaat om surveillance die niet is gebaseerd op precieze regels, zonder aantoonbare noodzaak of evenredigheid met een legitiem doel, zonder onafhankelijk toezichtmechanisme en zonder dat betrokkenen toegang hebben tot onafhankelijke rechtspraak[20].

Hoe ver gaat de taak van de data exporteur in dit verband? De EDPB stelt in haar Recommendations (01/2020) met betrekking tot de taak van de data exporteur:

> *You will need to look into the characteristics of each of your transfers and determine whether the domestic legal order and/or practices in force of the country to which data is transferred (or onward transferred) affect your transfers. The scope of your assessment is thus limited to the legislation and practices relevant to the protection of the specific data you transfer, in contrast with the general and wide encompassing adequacy assessments the European Commission carries out in accordance with Article 45 GDPR.*

Met andere woorden, het lid van SURF hoeft niet *alle* aspecten in overweging te nemen, zoals de EC dit dient te doen bij het onderzoek op basis waarvan deze een adequaatheidsbesluit kan toekennen aan een derde land, en zoals bepaald in EU AVG Artikel 45.

In de praktijk betekent dat hoofdzakelijk:

- Vaststellen of er sprake is van 'problematische wetgeving' (wetten en gebruiken) in dat derde land.
- Vaststellen of de kenmerken van de voorgenomen doorgifte binnen de scope van die problematische nationale wetgeving valt.
- Vaststellen of de gegevens dan in leesbare vorm op te vragen zijn door overheidsinstanties in het derde land.

20 De EDPB beschrijft vier essentiële waarborgen waaraan surveillance wetgeving moet voldoen. Zie: EDPB, Aanbevelingen 02/2020 over de Europese essentiële garanties voor surveillancemaatregelen, Vastgesteld op 10 november 2020, URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_nl.pdf.

6.3.
Waarschijnlijkheid en ernst

De vorige paragraaf maakt duidelijk dat een risico-inschatting een inschatting vereist van:
- de ‘waarschijnlijkheid’ (kans) dat het risico optreedt;
- en de ‘ernst’ (impact) wanneer het risico zich daadwerkelijk voordoet.

De leden van SURF kunnen het risico dat verbonden is aan een doorgifte dus verlagen door het treffen van maatregelen die zich richten op zowel de ‘waarschijnlijkheid’ als de ‘ernst’.

Zo kunnen leden van SURF technische maatregelen treffen, zoals de toepassing van encryptie met sleutelmanagement. Daarnaast dient het lid van SURF, in samenwerking met de data importeur, de reële kans in kaart te brengen dat de verschillende soorten persoonsgegevens daadwerkelijk in leesbare vorm worden opgevraagd door derden.

In dat licht kan, met de nodige voorzichtigheid en voorwaarden, eveneens de aanbeveling van de EDPB worden gezien. Namelijk wanneer er gegeven de *practices* geen reden is om aan te nemen dat relevante en *problematische wetgeving* in de praktijk zal worden toegepast op de voorgenomen doorgifte van het lid van SURF[21].

> *Zie in dit verband ook de duiding - in twee stappen - van de analyse van de Amerikaanse CLOUD-Act door het Nationaal Cyber Security Centrum (NCSC). In de NCSC publicatie (augustus 2022): De werking van de CLOUD-Act bij dataopslag in Europa[22] werd geconstateerd dat ook Europese bedrijven met dataverwerkingen in Europa, soms vallen onder de werking van de Amerikaanse CLOUD-Act. Hierdoor kan in Europa opgeslagen data toegankelijk zijn voor de Amerikaanse overheid.*

> *Er is in de VS dus sprake van, vanuit EU perspectief, ‘problematische wetgeving’, vanwege het bestaan van de CLOUD-Act. In het Schrems II arrest heeft het Europese Hof met name gekeken naar twee andere voorbeelden van problematische nationale wetgeving in de VS: FISA[23] en EO12333[24].*

In november 2022 oordeelde het NCSC dat er een “(…) kleine kans (is) dat Amerikaanse overheid toegang krijgt tot Europese gegevens op basis van de CLOUD-Act”[25]. Meer specifiek:

> *Risicomanagement vormt het hart van een adequate beveiliging van (persoons)gegevens. De integrale risicoanalyse die daaraan ten grondslag ligt, vereist een heldere inschatting van de kans en impact van de verschillende risico’s. Hiermee kan onderscheid worden gemaakt tussen de hypothetische risico’s en de daadwerkelijke risico’s. Het onderzoek van Greenberg Traurig laat zien dat het risico dat de Amerikaanse overheid toegang krijgt tot Europese (persoons)gegevens, specifiek op basis van de CLOUD-act, weliswaar voorstelbaar, maar in de praktijk ook (heel) klein is.*

Belangrijk voor de leden van SURF is dat (aanvullende) maatregelen betrekking kunnen hebben op zowel de ‘waarschijnlijkheid’ als de ‘ernst’ van een doorgifte risico.

Inzicht in de ***wetten*** én de ***practices*** (denk aan verzoeken van overheidsinstanties voor daadwerkelijke toegang tot persoonsgegevens) van een derde land, geven een beeld van de ***waarschijnlijkheid* en *de ernst*** van een risico.

In het voorbeeld van de CLOUDAct voor de Verenigde Staten volgt uit de formule van ‘***risico = waarschijnlijkheid** x **ernst***’ dat als de waarschijnlijkheid klein is, dit leidt tot een verlaging van het risico. Hoeveel lager dat risico dan wordt, is afhankelijk van de (potentiële) ernst.

21 Zie: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, para. 47.
22 Zie online: https://www.ncsc.nl/actueel/weblog/weblog/2022/de-werking-van-de-cloud-act-bij-dataopslag-in-europa.

23 Zie: https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf.
24 Zie: https://www.archives.gov/federal-register/codification/executive-order/12333.html.
25 Zie: https://www.ncsc.nl/actueel/weblog/weblog/2022/kleine-kans-dat-amerikaanse-overheid-toegang-krijgt-tot-europese-gegevens-op-basis-van-de-cloud-act. Zie meer specifiek ook het aanvullende rapport van Greenberg Traurig LLP, Number of CLOUD Act requests, d.d. November 17, 2022. Online: https://www.ncsc.nl/documenten/rapporten/2022/november/23/cloud-act-requests.

6.4
Waarschijnlijkheid

Belangrijke vraag is *hoe* de waarschijnlijkheid in te schatten dat overheidsinstanties in een derde land toegang krijgen tot de persoonsgegevens in leesbare vorm? Aangezien de meest gebruikte cloudleveranciers uit de VS komen, wordt de analyse hieronder beperkt tot drie indicatoren die specifiek zijn voor leveranciers uit de VS:

1. Transparantie over aantallen bevragingen.
2. Hoog algemeen beveiligingsniveau: naleving standaarden, certificering en *Zero Trust*.
3. Reikwijdte van de problematische wetgeving.

6.4.1. Indicator 'waarschijnlijkheid': transparency reports

Een transparency report[26] is een regelmatig verschijnend rapport van een leverancier over de aard en omvang van verzoeken van overheidsorganisaties om toegang tot gegevens van (klanten van) dat bedrijf. Vrijwel alle grote Amerikaanse techbedrijven publiceren inmiddels jaarlijkse of halfjaarlijkse transparency reports.

In het hierboven aangehaalde onderzoeksrapport van Greenberg Traurig LLP uit 2021 getiteld: "Number of CLOUD Act requests" is geput uit zogenaamde "transparency reports". Microsoft wordt onder andere uitgelicht:

- *Since the US CLOUD Act became effective in March 2018, Microsoft reported 12 disclosures of non-US based enterprise content data to the US government. Please note that it is uncertain whether any EU resident's personal data was disclosed in relation to these 12 disclosures, since this is not specified in the reports.*
- *In November 2021, Microsoft stated they "never provided access to any personal data of public sector organizations in the EU to any government authority."*

Het feit dat Microsoft in de voorafgaande zin heel specifiek benoemt dat het bedrijf geen toegang heeft verleend tot enige persoonsgegevens van enige Europese publieke organisatie aan enige overheidsorganisatie, is opmerkelijk[27], omdat bedrijven in de regel in hun statistieken een bepaalde bandbreedte aanhouden.

Er is in de praktijk grote variatie in de mate van openheid in deze transparency reports, en daarmee ook in de mate van bruikbaarheid van de informatie uit deze rapportages. De OECD doet aanbevelingen voor het verbeteren van de kwaliteit van die transparantie, binnen de geldende beperkende wettelijke kaders.

De leden van SURF kunnen uit de uitspraak van Microsoft afleiden dat het risico van toegang door opsporingsdiensten uit de VS tot persoonsgegevens van medewerkers en studenten die het lid van SURF heeft doorgegeven aan Microsoft, als 'laag' te kwalificeren is. Dit aangezien – in ieder geval tot november 2021 - sprake is van een onwaarschijnlijkheid van toegang tot die gegevens.

Uiteraard is dit een momentopname en het verdient aanbeveling de inhoud van de transparancy reports goed in de gaten te houden.

6.4.2. Indicator 'waarschijnlijkheid': standaarden, certificering en Zero Trust

De waarschijnlijkheid van mogelijke toegang door overheidsinstanties in derde landen wordt niet alleen beïnvloed door gegevens die de leveranciers bewust verstrekken, maar ook door lekken in de beveiliging van gegevens. Opsporingsdiensten kunnen gebruikmaken van zero day exploits (gebruikmaken van een zwakke plek in software, die nog onbekend is bij de software-ontwikkelaar), medewerkers omkopen of hacken, of binnendringen bij (software van) toeleveranciers. Daarom moeten de leden van SURF ook kijken naar de kwaliteit van de beveiliging van de persoonsgegevens door de data importeur.

26 Zie voor een overzicht van transparency reports van tech bedrijven de Transparency Reporting Index: https://www.accessnow.org/transparency-reporting-index/. Google publiceerde het eerste transparency report, in 2009 over de tweede helft van dat jaar.

27 Hiermee wijkt Microsoft af van beperkingen die bedrijven in de VS wettelijk zijn opgelegd met betrekking tot het verschaffen van enige transparantie . Zie hiertoe ook pg. 20, Transparency Reporting Considerations for the Review of the Privacy Guidelines. OECD Digital Economy Papers. April 2021. No. 309.: "Prior to January 2014, US-based companies were not able to even acknowledge having received national security requests. After a settlement between Facebook, Google, LinkedIn, Microsoft and Yahoo with the US Department of Justice, these companies were allowed to report on these requests under two possible reporting structures. One structure uthorized the reporting on numbers of national security letters (NSLs), Foreign Intelligence Surveillance Act (FISA) orders for content, and FISA orders for non-content in bands of 1 000, whilst under the other structure companies could report numbers in bands of 500 provided that all requests were reported in the aggregate. The passing of the 2015 USA FREEDOM Act relaxed the aforesaid restrictions significantly, making available four alternative reporting structures; however, actual numbers must be still reported in bands (of 1000, 500, 250 or 100, depending on the chosen reporting structure)."

1. Standaarden

Het Nationaal Cyber Security Centrum (NCSC) geeft in haar richtlijn *'(publieke) clouddiensten'*[28] het volgende aan over de beveiliging van cloudomgevingen tegen onbewuste toegang door hacking, omkoping, chantage, etc.:

Voor de beveiliging van cloudomgevingen en het mitigeren van beveiligingsrisico's zijn diverse best practices en sets met control richtlijnen beschikbaar. Bekende voorbeelden hiervan zijn:

- *ISO 27017[29]; een onderdeel van de ISO 27000 familie en specifiek bedoeld voor informatiebeveiliging (27017) en privacy (27018) in cloudomgevingen;*
- *Cloud Controls Matrix[30] van de Cloud Security Alliance (CSA);*
- *Cloud Computing Compliance Criteria Catalogue[31] (C5) van de Duitse BSI. Dit normenkader is mede gebaseerd op de ISO en CSA control sets.*

Inhoudelijk liggen deze standaarden en kaders vrij dicht bij elkaar[32]. Bovenop deze standaarden kan ook de SOC-2 privacy module worden toegevoegd. Deze module onderzoekt of de feitelijke verwerkingen in lijn zijn met het beleid.

2. Certificering

Het NCSC stelt in dezelfde richtlijn (pg. 19 en 20) met betrekking tot *certificering* van cloudomgevingen:

De beveiligingscertificering van clouddiensten helpt inzichtelijk te maken aan gebruikers en afnemers aan welk niveau van beveiliging deze dienstverlening voldoet door middel van een onafhankelijke toetsing. Het doel hiervan is om vertrouwen te creëren in de adequate beveiliging van clouddienstverlening. Internationaal zijn er verschillende cloud-certificeringsschema's. Eén van de meest bekende is de CSA-STAR[33]. Binnen Nederland kennen we daarnaast bijvoorbeeld de Zeker-Online[34] cloudcertificering.

De verschillende certificering- en assurance-schema's voor clouddiensten helpen meer grip op en inzicht te krijgen in de beveiliging van die diensten. Bekende schema's zijn die van CSA, C5, SecNum[35], ENS[36] en FedRamp[37].

Met de introductie van de Europese Cyber Security Act[38] (CSA) in juni 2019 heeft cloudcertificering een aanzienlijke impuls gekregen. In de CSA is opgenomen dat er een Europese cloud- certificeringsschema komt en zijn kaders afgesproken waaraan deze dient te voldoen. Zo krijgt het schema drie assurance niveau's; 'laag', 'midden' en 'hoog'. Gebruikers zullen op basis van een risico-afweging moeten bepalen welk niveau voor hen passend is. De verwachting is dat voor overheidsorganisaties en organisaties in het vitale domein, met name 'hoog' en 'midden'-diensten relevant zijn.

3. Zero Trust

Tenslotte noemt het NCSC in de hierboven aangehaalde richtlijn ook: 'Zero Trust' (pg. 19):

Zero Trust gaat uit van 'never trust, always verify'. Zero Trust stelt je eigen data centraal. Om die data heen wordt, liefst zo fijnmazig mogelijk, beveiliging georganiseerd. Gebruikers of applicaties kunnen alleen toegang krijgen tot die data als zij daar expliciet toe gerechtigd zijn. Belangrijke elementen in een Zero Trust beveiligingsaanpak zijn IAM, RBAC, encryptie, zonering en microsegmentatie.

Sinds President Biden in mei 2021 in de *Executive Order on Improving the Nation's Cybersecurity*[39] de term 'Zero Trust' verankerde in de cyberstrategie van de VS, is wereldwijd een groei waar te nemen van aanbieders van Zero Trust Architectuur. Zero Trust betekent dat een online dienst niemand permanent vertrouwt, en bij ieder gebruik eerst verifieert of een gebruiker of apparaat toegang mag krijgen.

Dit architectuurprincipe is inmiddels ingebakken in veel clouddiensten. De leden van SURF zouden zero trust dus ook als een requirement kunnen hanteren bij de inkoop van (online) diensten uit de Verenigde Staten en andere derde landen.

28 Zie: NCSC, (Publieke) clouddienstverlening. Enkele ervaringen uit onze cloud journey. Richtlijn. 11-06-2020. Online: https://www.ncsc.nl/documenten/rapporten/juni/ervaringsdocument/20/cloud-ervaringsdocument.

29 Zie: https://www.iso.org/standard/43757.html?browse=tc.

30 Zie: https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/.

31 Zie: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.pdf?__blob=publicationFile&v=1.

32 NCSC, (Publieke) clouddienstverlening. Enkele ervaringen uit onze cloud journey. Richtlijn. 11-06-2020, p. 18.

33 Zie: https://cloudsecurityalliance.org/star/.

34 Zie: https://www.zeker-online.nl/.

35 Zie: https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/.

36 Zie: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html.

37 Zie: https://www.fedramp.gov/.

38 Zie: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

39 Zie: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Samenvattend: wat betekenen standaarden, certificeringen en zero trust voor de risico-inschatting van een doorgifte?

- De leden van SURF kunnen in de onderhandeling met de leverancier van diensten en/of producten uit een derde land een aantal requirements opstellen over informatiebeveiliging. De eisen moeten strenger zijn naarmate de risico's van doorgifte voor betrokkenen groter zijn. Als de data importeur adequate beveiligingsmaatregelen hanteert en naleeft, leidt dat tot een relevante verlaging van de waarschijnlijkheid dat het risico zich voordoet.

- Als de organisatie in het derde land, al dan niet na onderhandelingen, zich daadwerkelijk kwalificeert volgens bovengenoemde geaccepteerde standaarden, dan kan dit redelijkerwijs gezien worden als relevante vermindering van de waarschijnlijkheid van het risico verbonden aan een doorgifte. Het verkleinen van de waarschijnlijkheid door toepassing van privacy en security 'by design en by default' via deze standaarden, zijn dus risico mitigerende maatregelen.

- De genoemde standaarden en certificeringen voor informatiebeveiliging zijn indicatoren die de leden van SURF kunnen meewegen in hun risicoafweging. En tevens bewijs van de implementatie van passende waarborgen bij deze cloudomgevingen voor de verwerkingen van de data importeur.

- Het strekt tot aanbeveling bij certificaten altijd de scope (welke activiteiten zijn gecertificeerd) en de geldigheid van het certificaat te verifiëren. In voorkomende gevallen kan een lid van SURF besluiten een aanvullende controle uit te laten voeren, bijvoorbeeld door middel van een pentest, om redenen van betrouwbaarheid betaald door het lid van SURF zelf en uitgevoerd door een derde, onafhankelijke partij.

6.4.3. Indicator 'waarschijnlijkheid': scope of toepassingsbereik van de 'problematische wetgeving'

Het laatste aspect dat inzicht kan geven in de waarschijnlijkheid dat het risico van bijvoorbeeld toegang tot persoonsgegevens door een overheidsdienst in een derde land optreedt, is kennis van de scope of het toepassingsbereik van de 'problematische wetgeving' zelf.

Zo gelden bijvoorbeeld voor FISA (section 702) *Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons*[40] bepaalde beperkingen:

1. VS ingezetenen mogen geen doelwit zijn[41].
2. Op basis van FISA kunnen Amerikaanse aanbieders van elektronische communicatiediensten (electronic communication service providers (ECSPs)) worden gedwongen[42] om informatie te verstrekken om 'foreign intelligence information' te verkrijgen. En al is de definitie van een ECSP in de praktijk breed[43], een universiteit in de VS is *geen* ECSP en valt dus niet binnen de scope van FISA.
3. Voordat surveillance programma's worden goedgekeurd, dienen er op basis van *facts* en *probable cause* zogenaamde *certifications* te worden ingediend door de Attorney General en de Director of National Intelligence bij een rechter, die namens de Foreign Intelligence Surveillance Court[44] (FISC) een toetsing doet op basis waarvan een aanvraag al dan niet wordt gehonoreerd.

Expert opinions, zoals voor de VS van Prof. Stephen I. Vladeck[45], kunnen leden van SURF helpen om een beeld te krijgen van de scope en werking van 'problematische wetgeving' in derde landen.

40 Zie: https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf#page=4.
41 Ibidem; Limitations 1 tot en met 4.
42 In FISA termen: 'assistance' bieden. Zie: sectie 802 Definities.
43 Zie ook: sectie 802 Definities.
44 De FISC publiceert jaarverslagen, die deels gelakt zijn, maar een indruk geven van de uitvoering van de procedures. Zie ook: https://www.fisc.uscourts.gov/.
45 Expert Opinion on the Current State of U.S. Surveillance Law and Authorities from Prof. Stephen I. Vladeck, University of Texas School of Law from 15 November 2021. Online: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

Tenslotte zit er nog een ander aspect aan de scope van ‘problematische wetgeving’ in een derde land. Met weer als voorbeeld de VS. The Guardian publiceerde[46] in 2013 over BoundlessInformant, een tool die de NSA gebruikt voor analyse van de surveillance data. The Guardian publiceerde in dat artikel ook een ‘global heat map’, waarop zichtbaar is in welke mate landen worden getarget door de NSA:

Het kleurverloop (van groen naar oranje en rood) geeft de mate van surveillance aan, waarbij rood aangeeft dat daar veel surveillance plaatsvindt. Dit overzicht maakt duidelijk dat het om een bepaald aantal landen gaat waar veel surveillance plaatsvindt. Het oogmerk van FISA is met name gericht op preventie van terrorisme en wapenhandel. Uit de jaarverslagen van de FISC valt op te maken dat de focus van surveillance, zoals opgenomen in dit overzicht, sinds de inwerkingtreding van FISA niet wezenlijk is veranderd.

46 Zie: The Guardian, Boundless Informant: the NSA's secret tool to track global surveillance data. 11 Jun 2013. Online: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

6.5. Ernst

De vorige alinea's beschreven hoe de leden van SURF de waarschijnlijkheid kunnen bepalen dat het risico op (onrechtmatige) toegang tot de persoonsgegevens in het derde land van de data importeur zich voordoet. Dit onderdeel van het Toetsingskader beschrijft hoe de leden van SURF de impact (oftewel de ernst van een dergelijke toegang voor de betrokkenen) kunnen bepalen. Met het bepalen van de impact kunnen de leden de risico-inschatting voltooien. Risico is immers: waarschijnlijkheid x impact. Die berekening kun je visualiseren in een matrix.

	Impact laag	*Impact midden*	*Impact hoog*
Zeer waarschijnlijk	**Risico laag**	**Risico midden**	**Risico zeer hoog**
Waarschijnlijk	**Risico laag**	**Risico midden**	**Risico hoog**
Onwaarschijnlijk	**Risico laag**	**Risico laag**	**Risico laag**

Om de impact van het risico te bepalen dient het lid van SURF ook het *staartrisico* te bepalen, alsmede de gevoeligheid van de persoonsgegevens die zijn betrokken bij de doorgifte.

> *Een **staartrisico** of **'tail risk'** doet zich voor wanneer een extreem risico zich onverhoopt toch voordoet, terwijl de waarschijnlijkheid laag is, maar de gevolgen zeer groot. Oftewel, een statistisch zeer kleine kans op extreme gebeurtenissen. Denk aan een pandemie (COVID-19) of een oorlog. Is er politieke onrust of instabiliteit in het betreffende derde land, bijvoorbeeld door oorlog, dan wordt deze tijdelijke en uitzonderlijke context meegenomen in de overall appreciatie van het risico van de doorgifte.*

De belangrijkste maatstaf om de impact te kunnen bepalen, is de mate waarin persoonsgegevens informatie onthullen waar betrokkenen bij onrechtmatig gebruik daarvan (bijvoorbeeld onbevoegde toegang) hinder of nadeel (kunnen) ondervinden. Dit gaat bijvoorbeeld om informatie die tegen betrokkenen kan worden gebruikt. Bij bijzondere en vertrouwelijke/gevoelige persoonsgegevens spreekt voor zich dat onrechtmatig gebruik daarvan

tot grote risico's kan leiden, zoals discriminatie of uitsluiting. Denk aan het geval van een student uit Pakistan die een aanvraag doet om atoomwetenschappen te gaan studeren in Nederland, of deel te nemen aan een sociologie vakgroep die grootschalig onderzoek doet naar politieke radicalisering of aan een discussie tussen informatiebeveiligers over mogelijkheden om quantum cryptografie te hacken. Journalist Maurits Martijn noemt een ander voorbeeld, waarbij je zelfs het risico loopt op vrijheidsberoving:

> *"(...) Stel, je wilt als journalist een stuk schrijven over Nederlandse jongeren die in Syrië gaan vechten. Je boekt een enkele reis omdat je nog niet weet wanneer je terug wilt komen. Daar sta je dan: met de contactgegevens van een paar jihadisten in je telefoon, een enkeltje New York op zak en een kersverse levensverzekering afgesloten. Hoeveel alarmbellen gaan er dan af bij, bijvoorbeeld, de Amerikaanse inlichtingendienst NSA?"*[47]

Maar ook 'gewone' persoonsgegevens zoals een huisadres of e-mailadres kunnen zeer gevoelig zijn, afhankelijk van de aard en kwetsbaarheid van de betrokkene. Voorbeelden zijn de huisadressen van politici en journalisten die bewust geheim worden gehouden, maar ook persoonlijke e-mailadressen van systeembeheerders, om deze te beschermen tegen phishing en malware. Denk daarnaast ook aan het geval waarbij leerprestaties worden gekoppeld aan psychologische kwalificaties van de betrokkene.

Voor de vermindering van de impact kunnen de leden van SURF, maar ook de leveranciers allerlei maatregelen treffen om te voorkomen dat ze leesbare persoonsgegevens verwerken. Denk hierbij aan versleuteling van de persoonsgegevens, pseudonimisering van accountgegevens en data-minimalisatie.

Het treffen van maatregelen heeft gevolgen voor de zwaarte van de impact die resulteert in een classificatie van vijf categorieën, in oplopende mate van impact voor de betrokkenen[48]. Het Toetsingskader volgt de classificatie zoals deze in de DPIA's van SURF en SLM Rijk zijn toegepast en onderstaand is opgenomen. Het is een vijfpuntsschaal van impact (ernst) oplopend van *Verwaarloosbaar* tot en met *Zeer hoog*:

Impact (schaal van ernst)	**Kenmerken van de data (bij de doorgifte)**
Verwaarloosbaar	Anonieme of versleutelde data waarbij de sleutel niet gebruikt kan worden door de data importeur.
Laag	Pseudonieme diagnostische data.
Midden	Pseudonieme vertrouwelijke/gevoelige of bijzondere persoonsgegevens.
Hoog	'Gewone' persoonsgegevens die de data importeur leesbaar kan maken en die niet al publiek beschikbaar zijn.
Erg hoog	Vertrouwelijke/gevoelige of bijzondere persoonsgegevens die de data importeur leesbaar kan maken.

Dus de impact van bijvoorbeeld onrechtmatige toegang tot geanonimiseerde data of end-to-end versleutelde gegevens, waarbij het lid van SURF de sleutel beheert, is 'verwaarloosbaar'. Terwijl onrechtmatige toegang tot onversleutelde bijzondere categorieën van persoonsgegevens wordt geclassificeerd als een impact die 'erg hoog' is.

47 Maurits Martijn, Nee, je hebt wél iets te verbergen, URL: https://decorrespondent.nl/209/nee-je-hebt-wel-iets-te-verbergen/4113922560-dfab02e3.

48 Zoals ontwikkeld door Privacy Company.

6.6.
Samenvattend

Bij de risico-inschatting met betrekking tot de doorgifte van persoonsgegevens kunnen leden van SURF de risico-inschatting maken; de inventarisatie van de risico's van doorgifte alsmede de waarschijnlijkheid en impact daarvan met betrekking tot:

- De volwassenheid van de eigen organisatie in termen van geaccepteerde standaarden op het gebied van informatiebeveiliging en gegevensbescherming.
- Kenmerken van 'problematische wetgeving' en de *practices* op basis van die wetgeving in het derde land waar de data importeur is gevestigd (inschatting van *waarschijnlijkheid* en *ernst*).
- Kenmerken van de data importeur (en diens resellers en subverwerkers) aan wie de leden van SURF de persoonsgegevens doorgeven. Die kenmerken hebben betrekking op het (i) bestaan en werking van geaccepteerde standaarden op het gebied van informatiebeveiliging en gegevensbescherming, (ii) relevante certificeringen en (iii) zero trust.
- Kenmerken van de doorgifte (waaronder de vraag of bijzondere categorieën van persoonsgegevens worden doorgegeven) en kenmerken van de personen van wie de persoonsgegevens worden doorgegeven (kwetsbare personen).

Deze risico-inschatting is dynamisch en dient onderdeel te zijn van een Plan-, Do-, Check-, Act-cyclus. Op basis van deze risico-inschatting kunnen de leden van SURF de maatregelen identificeren die ze dienen te nemen in aanvulling op de SCC om het Europese hoge beschermingsniveau te kunnen waarborgen bij doorgifte.

7.
Aanvullende maatregelen: wat zijn de aanvullende maatregelen voor de specifieke doorgifte?

Zoals al aangegeven in dit Toetsingskader zijn op grond van de AVG voor de doorgifte van persoonsgegevens *passende* beveiligingsmaatregelen vereist. Dat betreft organisatorische, contractuele en technische beveiligingsmaatregelen. Welke maatregelen passend zijn is afhankelijk van de specifieke verwerking en doorgifte en is ter beoordeling aan ieder lid van SURF.

> *De bedoeling van het nemen van passende maatregelen is het mitigeren (wegnemen of verkleinen) van de waarschijnlijkheid en/of ernst waardoor het vastgestelde risico er niet langer is of lager wordt. Op deze manier kan een instelling van SURF het aldus overblijvende rest-risico (laag, midden of hoog) vaststellen en hierover een besluit nemen.*

Voor bepaalde doorgiften zijn in hoofdstuk zes al een aantal belangrijke (en aanvullende) risico-mitigerende maatregelen beschreven. Doorgiften waar een lid van SURF tot het oordeel komt dat de risico-inschatting ‘hoog’ of ‘zeer hoog’ is, bijvoorbeeld bij doorgiften waar bijzondere persoonsgegevens, BSN en/of gevoelige persoonsgegevens zijn betrokken, vereisen doorgaans aanvullende maatregelen. Deze aanvullende maatregelen zijn vooral van technische aard en dan liggen encryptie en sleutelmanagement het meest voor de hand voor het mitigeren van de ‘hoog’ of ‘zeer hoge’ risico’s.

In het kader van cloudoplossingen zijn twee soorten encryptie mogelijk:

1. Versleuteling van opgeslagen gegevens waarbij *alleen* de klant toegang heeft tot de sleutel. Denk aan opslag van een archief of verzameling documenten op een VM of in een eigen map bij een cloudprovider. De klant heeft de sleutel op een eigen apparaat (of bij een vertrouwde derde partij, een TTP, in een EU-lidstaat) en versleutelt het gewenste bestand voordat hij het bestand naar de provider uploadt.

2. Versleuteling van dynamische gegevens waarbij de data importeur toegang nodig heeft tot de sleutel, om *live* gegevens voor de klant te kunnen ontsleutelen. Dit is het geval bij databases. Het is niet efficiënt en schaalbaar voor de klant om alle gegevens uit een complexe database eerst te downloaden, uit te pakken met de eigen sleutel, lokaal te doorzoeken op het gewenste informatie, te bewerken, en daarna weer versleuteld te uploaden.

In de nieuwe opinie van de EDPB over certificering als doorgifte waarborg, wordt een nieuwe nuance gegeven over de eerste soort versleuteling. De EDPB schrijft niet meer dat de data importeur geen toegang mag hebben tot de sleutel, maar dat hij niet gedwongen mag worden tot het exporteren van de sleutel. Dat betekent dat veelgebruikte opslagoplossingen op een VM, waarbij de sleutel wordt opgeslagen in een HSM (Hardware Security Module) van de leverancier, mogelijk toch voldoende zijn als waarborg. De leverancier heeft er dan alles aan gedaan om het zichzelf onmogelijk te maken om de sleutel te gebruiken zonder opdracht van de klant. Van de leverancier kan niet de hightech kennis verwacht worden dat die de sleutel uit de HSM kan halen om aan een overheidsinstantie te overhandigen.

Daarnaast kunnen de verschillende strategieën van Privacy by Design zoals geformuleerd in het Blauwe Boekje[49] van Jaap-Henk Hoepman handvatten bieden voor ook het nemen van passende *en* aanvullende contractuele, organisatorische en technische maatregelen in het kader van doorgifte. Hoepman maakt onderscheid tussen *datageoriënteerde strategieën* en *procesgeoriënteerde strategieën*. Zie voor een overzicht bijlage 1. Wat betreft de concrete aanvullende maatregelen, tot slot, geeft de EDPB in haar verschillende aanbevelingen[50] goede opsommingen van aanvullende maatregelen. Deze zijn in te zetten om de geïdentificeerde risico’s te mitigeren en doen dit in essentie door de *waarschijnlijkheid* of de *ernst*, behorend bij het risico, te beïnvloeden. In bijlage 2 zijn en worden aanvullende maatregelen opgenomen.

49 Zie: Jaap-Henk Hoepman, Privacyontwerpstrategieën, 2020. Online: https://www.cs.ru.nl/-jhh/publications/pds-boekje.pdf.

50 Zie: Annex 2 in: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0 Adopted on 18 June 2021. Online: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf en: 2022 Coordinated Enforcement Action. Use of cloud-based services by the public sector. Adopted on 17 January 2023. Online: https://edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf. Dat het hierbij om meer gaat dan alleen versleuteling en bijbehorende sleutelbeheer blijkt uit het laatstgenoemde EDPB document, waarin de volgende benadering beschrijft (pg. 2):

- Carry out a DPIA;
- Ensure that the roles of the involved parties are clearly and unequivocally determined;
- Ensure the CSP acts only on behalf of and according to the documented instructions of the public body and identify any possible processing by the CSP as a controller;
- Ensure that a meaningful way to object to new sub processors is possible;
- Ensure that the personal data are determined in relation to the purposes for which they are processed;
- Promote the DPO’s involvement;
- Cooperate with other public bodies in negotiating with the CSPs;
- Carry out a review to assess if processing is performed in accordance with the DPIA;
- Ensure that the procurement procedure already envisages all the necessary requirements to achieve compliance with the GDPR;

Bijlage 1
Privacy By Design Strategieën

(Ontleend aan: Jaap-Henk Hoepman, Privacyontwerpstrategieën, 2020)

1	**Datageoriënteerde strategieën**				
1.1	**Minimaliseer**	Beperk zoveel mogelijk de verwerking van persoonsgegevens.	**1.1.1**	*Selecteer*	Selecteer alleen relevante personen of gegevens. Bepaal van tevoren welke personen of gegevens relevant zijn en verzamel enkel die gegevens. Bewaar binnenkomende gegevens alleen als ze aan het selectiecriterium voldoen. Wees conservatief in je selectiecriteria: selecteer alleen dat wat strikt noodzakelijk is. Gebruik een whitelist.
			1.1.2	*Sluit uit*	Sluit op voorhand bepaalde personen of gegevens uit. Bepaal van tevoren welke personen of gegevens niet relevant zijn en verzamel die gegevens niet of gooi ze meteen weg als ze onverhoopt toch binnenkomen. Wees ruim in je uitsluitingsgronden: sluit zo veel mogelijk gegevens uit, tenzij je zeker weet, en kunt verantwoorden, dat je ze nodig hebt. Gebruik een blacklist.
			1.1.3	*Verwijder*	Verwijder (deel)gegevens die niet langer nodig zijn. Bepaal van tevoren hoe lang gegevens nodig zijn en zorg dat ze automatisch na die tijd verwijderd worden. Als het een specifiek veld uit een record betreft, dat verder nog wel bewaard moet worden, zet dat veld dan op een default waarde. Veranderingen in de organisatie, het dienstportfolio of een wijziging in een proces kunnen er ook toe leiden dat gegevens niet langer relevant zijn.
			1.1.4	*Vernietig*	Verwijder volledige persoonsgegevens zodra ze niet langer nodig zijn. Zorg dat de gegevens ook echt niet meer beschikbaar zijn. Dat wil zeggen: verwijder gegevens ook van eventuele back-ups, en wis data op harde schijven en andere opslagmedia op een veilige manier.
1.2	**Scheid**	Scheid de verwerking van persoonsgegevens zoveel mogelijk van elkaar.	**1.2.1**	*Isoleer*	Verzamel of verwerk persoonsgegevens in verschillende, logisch gescheiden databases of systemen.
			1.2.2	*Distribueer*	Distribueer de verwerking over verschillende fysieke locaties. Doe zoveel mogelijk in de apparatuur (PC, smartphone) van de eindgebruiker en maak zo weinig mogelijk gebruik van centrale componenten. Maak gebruik van decentrale of zelfs gedistribueerde systemen in plaats van gecentraliseerde architecturen.
1.3	**Abstraheer**	Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.	**1.3.1**	*Groepeer*	Aggregeer informatie over categorieën personen in plaats van ieder individu. Stel een groepsprofiel op (met de gemiddelde waarde van de gegevens van alle mensen van een bepaalde leeftijd of een bepaald postcodegebied).
			1.3.2	*Vat samen, generaliseer*	Vat gedetailleerde informatie samen in meer algemene gegevens. Registreer bijvoorbeeld een leeftijdscategorie in plaats van een geboortedatum of een woonplaats in plaats van het precieze adres.

			1.3.3	*Ruis toevoegen, verstoren*	Gebruik niet de precieze waarde van een gegeven. Gebruik een benadering van de waarde of pas de waarde aan met een kleine hoeveelheid ruis.
1.4	**Verberg**	Bescherm persoons-gegevens, of maak ze onherleidbaar of onobser-veerbaar. Voorkom dat persoons-gegevens openbaar worden.	**1.4.1**	*Beperk toegang*	Beperk toegang tot persoonsgegevens. Zorg dat de informatiebeveiliging op orde is. Stel strikte maatregelen op voor toegangscontrole. Geef personen alleen toegang tot persoonsgegevens die ze strikt gesproken nodig hebben (‘need to know’). Maak het moeilijk om met opzet of per ongeluk data te delen met onbe-voegden.
			1.4.2	*Maak onbe-grijpbaar*	Maak data onbegrijpbaar voor derden. Versleutel data zodat ze onleesbaar wor-den zonder de sleutel. Hash persoonsge-gevens, bijvoorbeeld door er pseudonie-men van te maken.
			1.4.3	*Verbreek link*	Verbreek de link en de correlatie tussen gebeurtenissen, personen en gegevens. Verwijder direct identificerende gege-vens.
			1.4.4	*Meng*	Maak data of gebeurtenissen onherleid-baar, bijvoorbeeld door deze met elkaar te mengen of door deze te anonimiseren. Verberg gegevens in een ‘wolk’ van wil-lekeurige andere gegevens. Verbreek de correlatie tussen twee gebeurtenissen, bijvoorbeeld door niet meteen te reage-ren. Verzamel eerst een aantal gebeur-tenissen of gegevens over een aantal personen en verwerk deze dan in bulk.

2	**Procesgeoriënteerde strategieën**				
2.1	**Infor-meer**	Informeer gebruikers over de ver-werking van hun persoons-gegevens.	**2.1.1**	*Informeer*	Vertel welke persoonsgegevens worden verwerkt, op welke manier deze worden verwerkt en waarom. Geef aan hoelang persoonsgegevens worden bewaard en hoe ze verwijderd worden. Geef aan met wie persoonsgegevens worden gedeeld, welke afspraken daar over zijn gemaakt en hoe je die afspraken controleert. Zet een link naar je privacybeleid op je home-page en in je app. Geef duidelijk aan hoe mensen contact op kunnen nemen.
			2.1.2	*Leg uit*	Leg uit welke persoonsgegevens worden verwerkt en waarom. Beargumenteer waarom dit nodig is. Doe dit op een dui-delijke en voor leken begrijpbare manier. Structureer je informatievoorziening en richt deze op verschillende doelgroepen: leken, experts, autoriteiten. Maak de informatie ‘gelaagd’: geef een overzicht en ga in aparte pagina’s in op details.
			2.1.3	*Waarschuw*	Waarschuw gebruikers als hun persoons-gegevens gebruikt worden, met derden gedeeld worden of als deze gelekt zijn. Leg procedures hiervoor van tevoren vast. Maak waarschuwingen kort maar informatief. Waarschuw niet te vaak. Geef gebruikers de mogelijkheid in te stellen welke waarschuwingen ze willen ontvangen.
2.2	**Geef controle**		**2.2.1**	*Vraag toe-stemming*	Vraag gebruikers toestemming voor de verwerking van hun persoonsgegevens. Informeer ze hierbij vooraf over welke ge-gevens worden verwerkt, hoe die worden verwerkt en met welk doel (‘informed consent’, zie ook de informeer strategie). Toestemming moet ingetrokken kunnen worden.

		2.2.2	*Geef keuze*	Geef gebruikers een reële keuze over de verwerking van hun persoonsgegevens. Basisfunctionaliteit moet beschikbaar zijn zonder verwerking van persoonsgegevens. Bied een (betaald) alternatief aan.
		2.2.3	*Corrigeer*	Geef gebruikers de mogelijkheid om persoonsgegevens te corrigeren. Het ligt voor de hand dit te combineren met de mogelijkheid die gegevens in te zien (via een privacy dashboard).
		2.2.4	*Verwijder*	Geef gebruikers de mogelijkheid om persoonsgegevens te (laten) verwijderen. Ook dit kan gedaan worden via een privacy dashboard.
2.3	**Dwing af**	**2.3.1**	*Stel vast*	Committeer je als organisatie aan privacy. Neem je verantwoordelijkheid. Stel een privacybeleid op. Stel resources beschikbaar om het beleid uit te voeren. Bepaal per verwerking het doel en de (juridische) grondslag: is er een gerechtvaardigd belang of moet er om toestemming gevraagd worden? Wees duidelijk over het verdienmodel.
		2.3.2	*Dwing af*	Dwing het beleid af met alle noodzakelijke technische en organisatorische maatregelen. Implementeer deze maatregelen. Beleg verantwoordelijkheden. Stel een opleidingsprogramma en awarenesscampagne op. Zorg dat derden (de zogenaamde ‘verwerkers’) ook aan de eisen voldoen.
		2.3.3	*Beheer*	Omstandigheden veranderen. Controleer het privacybeleid, en de implementatie daarvan, regelmatig en pas het waar nodig aan. Stel vooraf eisen op en toets hieraan.
2.4	**Toon aan**	**2.4.1**	*Leg vast*	Documenteer alle (belangrijke) stappen die je neemt. Leg beslissingen vast en motiveer deze. Verzamel logs (en kom in actie bij anomalieën).
		2.4.2	*Audit*	Voer regelmatig audits uit op de verzamelde logs, maar ook meer in het algemeen op de manier van werken in de organisatie en op de manier van verwerken van persoonsgegevens.
		2.4.3	*Rapporteer*	Rapporteer de resultaten van de audits aan de toezichthouder of bewaar deze voor latere inzage. Overleg, waar mogelijk, regelmatig met de toezichthouder.

Bijlage 2
Maatregelen

De volgende bepalingen kunnen in de (verwerkers)overeenkomst worden opgenomen:

1. De leverancier/verwerker verifieert de rechtsgeldigheid van het verzoek tot inzage van een overheidsinstantie.
2. De leverancier/verwerker informeert het lid van SURF over verzoeken en leidt het rechtsgeldige verzoek door naar het lid van SURF.
3. Alleen als het wettelijk verboden is het verzoek door te leiden naar het lid van SURF en/of het lid van SURF te informeren, behandelt de leverancier/verwerker het verzoek zelf.
4. De leverancier/verwerker verzet zich juridisch waar mogelijk tegen elke vordering tot inzage.
5. Als de leverancier/verwerker toch gedwongen is de persoonsgegevens te verstrekken, informeert hij het lid van SURF dat hij niet langer kan voldoen aan artikel 14e en 16a van de SCC.

Coöperatie SURF

Samen aanjagen van vernieuwing

In de coöperatie SURF werken universiteiten, hogescholen, mbo-scholen, umc's en onderzoeksinstellingen samen aan de beste ict voor onderwijs en onderzoek. We ontwikkelen en leveren betrouwbare, state of the art ict-diensten, of kopen die centraal en tegen gunstige voorwaarden in. We werken samen aan nieuwe, innovatieve toepassingen van ict in onderwijs en onderzoek. En we komen bij elkaar om kennis, visie en expertise uit te wisselen. Zo blijft het Nederlandse onderwijs en onderzoek behoren tot de top van de wereld.

SURF Utrecht
Kantoren Hoog Overborch
(Hoog Catharijne)
Moreelsepark 48
3511 EP Utrecht
088 - 787 30 00

SURF Amsterdam
Science Park 140
1098 XG Amsterdam
088 - 787 30 00

info@surf.nl